S3-040223

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

COM 17 – LS 31 – E

English only

Original: English

Question(s):	L/17	Geneva, 10-19 March 2004

Ref. : TD 2397 Rev. 1

Source:	ITU-T Study Group 17, Geneva, 10-19 March 2004
Title:	Information of new ITU-T Recommendations for secure mobile end-to-end data communication, X.1121 and X.1122

LIAISON STATEMENT

To:	3GPP, 3GPP2
Approval:	Agreed to at ITU-T SG 17 meeting
For:	Information

Contact: Dr. Heungyoul Youm
Rapporteur Q.L/17

Tel: +82 41 530 1328
Fax: +82 41 530 1494
Email: hyyoum@sch.ac.kr

Study Group 17 is pleased to inform 3GPP and 3GPP2 that new Recommendations X.1121 and X.1122 have been consented at this SG 17 meeting.

X.1121 (formerly X.msec-1) describes the framework of security technologies for mobile end-to-end data communication. It contains descriptions of security threats, security requirements and security functions.

X.1122 (formerly X.msec-2) is a guideline for implementing secure mobile systems based on PKI and describes models of secure mobile systems, usage models and considerations for secure mobile systems based on PKI.

ITU-T Question L/17 will welcome your comments on our current or future work in mobile security area.

Attached documents are consented Recommendations X.1121 and X.1122.

_____

New ITU-T Recommendation X.1121 (Formerly X.msec-1)

Framework of security technologies for mobile end-to-end data communications

Summary

This Recommendation describes security threat for mobile end-to-end data communication and security requirements from the point of view of mobile user and application service provider (ASP). In addition, this Recommendation shows that where the security technologies which realize certain security function appear in the models of mobile end-to-end data communication.

Framework of security technologies for mobile end-to-end data communications

1 Scope

This Recommendation provides security requirements, which are from the point of view of mobile user and application service provider in upper layer in OSI Reference Model, for mobile end-to-end data communication between mobile terminal in mobile network and application server in open network.

This Recommendation provides a framework of security technologies for mobile end-to-end data communication.

This Recommendation does not provide the details of mobile network except for that provides wireless network access to mobile terminal and is connected to open network.

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 X.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications.*

– ITU-T Recommendation X.803 (1994), *Information Technology – Open Systems Interconnection – Upper Layers Security.*

– ITU-T Recommendation X.810 (1995), *Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview.*

– 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*

3 Definitions

3.1 OSI Reference Model security architecture definitions

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

a) access control;

b) authentication;

c) authentication information;

d) authentication exchange;

e) authorization;

f) availability;

g) confidentiality;

h) cryptography;

i) data integrity;

j) data origin authentication;

k) encipherment;

l) integrity;

m) key;

n) key exchange;

o) key management;

p) non-repudiation;

q) notarization;

r) password;

s) privacy

3.2 Additional definitions

For the purposes of this recommendation, the following definitions apply:

3.2.1 anonymity

Ability to allow anonymous access to services, which avoid tracking of user's personal information and user behavior such as user location, frequency of a service usage, and so on

3.2.2 shoulder surfing

A kind of security threats which collects information in busy places by watching keystroke, reading mobile terminal's screen, or listening to sound from mobile terminal

3.2.3 mobile terminal

An entity that has wireless network access function and connects mobile network for data communication with application servers or other mobile terminals.

3.2.4 mobile network

A network that provides wireless network access points to mobile terminals

3.2.5 mobile user

An entity (person) that uses and operates the mobile terminal for receiving various services from application service providers

3.2.6 application service

A service like mobile banking, mobile commerce, and so on.

3.2.6 application server

An entity that connects to open network for data communication with mobile terminals

3.2.7 application service provider

An entity (person or group) which provides application service(s) to mobile users through application server

3.2.8 mobile security gateway

An entity which relays data communication between mobile terminal and application server, changes security parameter or communication protocol from mobile network to open network or vice versa and can perform security policy management function for mobile end-to-end data communication

3.2.9 security policy management

A function to manage or negotiate a set of rules to provide classified security services. And it can be implemented on the mobile security gateway or other sever

4 Abbreviations

For the purposes of this recommendation, the following abbreviations apply:

ASP	Application Service Provider
DoS	Denial of Service
IMT-2000	International Mobile Telecommunications-2000
LAN	Local Area Network
OSI	Open systems Interconnection
PC	Personal Computer
PDA	Personal Data Assistant
PIN	personal identification number

5 Overview

Mobile terminals with capability of data communications (like IMT-2000 mobile phone, laptop PC or a PDA with a radio-card) have been widely distributed and it becomes to provide various application services (ex. mobile commerce) for mobile terminals through the mobile network. In the e-commerce business, security is necessary and indispensable.

There are many security investigations from mobile operator's point of view (ex. security architecture on IMT-2000 mobile phone network). However, it is also important to investigate from mobile user's point of view and ASP's point of view as well.

When investigating the security for mobile communication from mobile user's point of view or ASP's point of view, security for mobile end-to-end data communication between mobile terminal and application server is one of the most important issues.

In addition, for the mobile system that connects mobile network to open network, security investigation in the upper layers (applications, presentation and session layers) of the OSI Reference Model is needed because there are various implementations of mobile network (for example, IMT-2000 mobile phone network, wireless LAN, Bluetooth and so on) or open network.

This recommendation describes security threats for mobile end-to-end data communication and security requirements from the point of view of mobile user and ASP. In addition, this recommendation shows that where the security technologies which realize certain security function appear in the models of mobile end-to-end data communication.

6 Models of mobile end-to-end data communication

Before describing secure mobile technologies, models of mobile end-to-end data communication should be defined. Models of mobile end-to-end data communication will clarify the relationship between entities in models and the points to which the secure mobile technologies should be adapted.

6.1 General model of mobile end-to-end data communication between mobile user and ASP

General model of mobile end-to-end data communication between mobile user and ASP shows below.

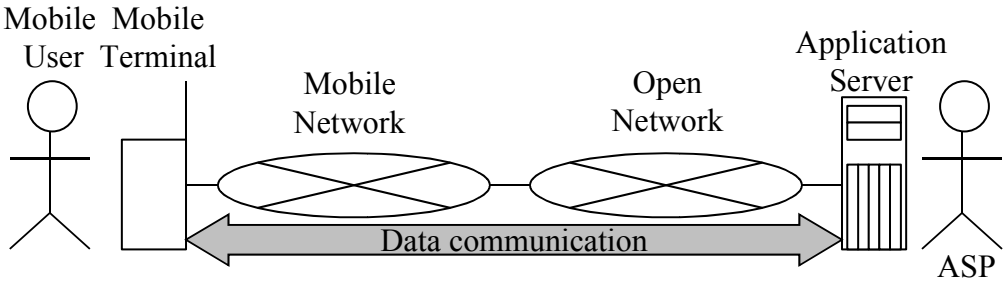

Figure 1 – General model of mobile end-to-end data communication between mobile user and ASP

There are six entities in this model: mobile user, mobile terminal, mobile network, open network, application server and ASP.

And there are five relationships in this model: relation between mobile user and mobile terminal, relation between mobile terminal and mobile network, relation between mobile network and open network, relation between open network and application server, and relation between mobile terminal and application server.

6.2 Gateway model of mobile end-to-end data communication between mobile user and ASP

Another model (Gateway model) of mobile end-to-end data communication between mobile user and ASP shows below.

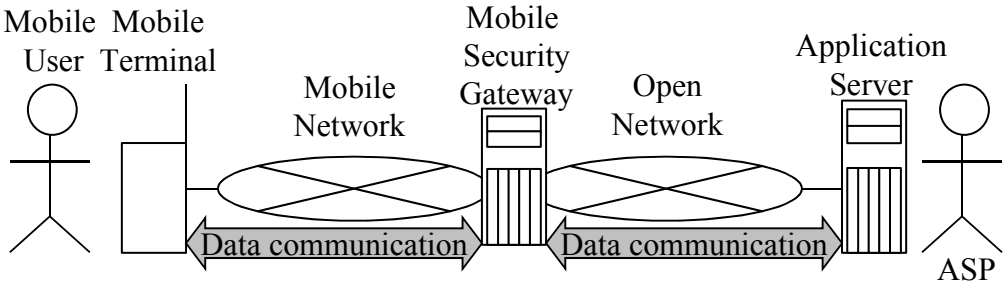

Figure 2 – Gateway model of mobile end-to-end data communication between mobile user and ASP

There are seven entities in this model: mobile user, mobile terminal, mobile network, open network, application server, ASP and mobile security gateway.

And there are seven relationships in this model: relation between mobile user and mobile terminal, relation between mobile terminal and mobile network, relation between mobile network and mobile security gateway, relation between mobile security gateway and open network, relation between open network and application server, relation between mobile terminal and mobile security gateway, and relation between mobile security gateway and application server.

7 Characteristics of mobile end-to-end data communication

Mobile end-to-end data communication has various characteristics compared to general end-to-end data communication in the open network. These characteristics show below.

Mobile communication is based on wireless communication

Because mobile end-to-end data communication is based on wireless communication, it is more instable than wired end-to-end data communication in the open network. In addition, because mobile user can move around during mobile end-to-end data communication, it is more instable.

And wireless communication could be based on broadcast communication between mobile terminal and mobile network.

Mobile terminals are small terminals in general

In general, mobile terminals that are used for mobile end-to-end data communication are smaller than existing typical terminals (e.g. desktop PC) that are used for end-to-end data communication in open network. It may causes following characteristics:

- Difficulty of data input or output

  It is difficult to enter data through keyboard or keypad and to see many data through its screen because of limited space of screen (especially, in the case of a small-sized hand-held terminal)
- Lower processing performance than desktop PC
- Limitation on corresponding application capacity (memory size, supply of power, etc.)

Mobile terminals are carried around by mobile users

8 Security threats in mobile environment

There are two types of security threats. One is general security threats that might exist in open network also. And another is mobile-oriented security threats that might exist by characteristics of mobile communication.

8.1 General security threats

As a kind of end-to-end data communication, mobile end-to-end data communications are also vulnerable to general security threats that are present in the open networks.

8.1.1 Eavesdropping

The most widely known problem in open network is susceptible to eavesdropping by anonymous attacks. The anonymous attackers can actively intercept the transmitted data. This can cause the leakage of communication data.

8.1.2 Communication jamming

This takes place when an intentional or unintentional interference overpowers the sender or receiver of a communications link, thereby effectively rendering the communications link useless. This can cause DoS attack.

8.1.3 Injection and modification of data

This occurs when unauthorized entity insert, change or delete information transmitted between mobile terminal and application server. The unauthorized entity could be a person, a program, or a computer. These attacks occur when attacker adds data to an existing connection in order to hijack the connection or maliciously send data. This can cause DoS attack or man-in-the-middle attack.

8.1.4 Interruption

This attack causes a destruction of an asset of mobile terminal and network element. This takes place when destruction of a piece of hardware, such as a hard disk, the cutting the communication line physically, or the disabling of the file management system in the mobile terminal or network element of infrastructure.

8.1.5 Unauthorized access

Access control is the ability to limit and control the access to application server, via a communication links. This takes place when the illegal entity could gain access to application server by pretending a mobile user's identity. The entity trying to gain an unauthorized access must be identified, or authenticated.

8.1.6 Repudiation

This attack takes place when a sender or receiver denies the fact that they have transmitted or received message, respectively.

8.2 Mobile oriented security threats

There are mobile-oriented security threats caused by characteristics of mobile communication, especially mobile communication is wireless communication and broadcast communication between mobile terminal and mobile network. The most widely known problem in wireless network is that it is susceptible to anonymous attackers.

Mobile oriented security threats shows below.

8.2.1 Eavesdropping

In mobile communication, this can be made more easily by actively intercepting radio signals and decode the data being transmitted. And this can cause the leakage of communication data.

8.2.2 Communication jamming

In mobile communication, this can be made more easily between mobile terminal and mobile network. There are two types of attacks, such as jamming against mobile terminal and jamming against network element. The former is give a chance to impersonate the legal mobile terminal to rogue mobile terminal, the latter is to give a chance to impersonate the legitimate network element interfacing the mobile terminal through the wireless interface.

8.2.3 Shoulder surfing

This takes place when an attacker collects information in busy places by watching keystroke, reading mobile terminal's screen, or listening to sound from mobile terminal. This causes the leakage of information.

8.2.4 Lost mobile terminal

This is a security threat caused by carrying around mobile terminal by mobile user. And this can cause the lost or destruction of information stored in mobile terminal.

8.2.5 Stolen mobile terminal

This is also caused by carrying around mobile terminal by mobile user. This can cause the leakage of information stored in mobile terminal, data deletion by unauthorized access from stolen mobile terminal in addition to the lost of information stored in mobile terminal.

8.2.6 Unprepared communication shutdown

This is a security threat caused by instable communication or limitation of supply of power. And this can cause the data deletion.

8.2.7 Misreading

This is a security threat caused by small display of mobile terminal. And this can cause the data deletion by masquerading of ASP.

8.2.8 Input error

This is a security threat caused by difficulty of data input through small keyboard or keypad of mobile terminal. And this can cause the failure of user authentication.

8.3 Relationship of security threats and models

These security threats appear in particular places of models. The relationship of security threats and models shows below (Table 1 and 2).

These tables show that there are same security threats in application server and mobile security gateway. And also these show that there are same security threats in the relation between mobile terminal and application server, the relation between mobile terminal and mobile security gateway, the relation between application server and mobile security gateway.

Table 1 - Relationship of general security threats and models

Threats / Entities, Relations	Eavesdropping	Communication jamming	Injection/ Modification	Interruption	Unauthorized access	Repudiation
Mobile terminal				X	X	
Application server		X		X	X	
Relation between mobile user and mobile terminal						
Relation between mobile terminal and application server	X	X	X	X		X
Mobile security gateway				X	X	
Relation between mobile terminal and mobile security gateway	X	X	X	X		X
Relation between application server and mobile security gateway	X	X	X	X		X

Table 2 - Relationship of mobile-oriented security threats and models

Threats / Entities, Relations	Eavesdropping	Communication jamming	Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading/ Input error
Mobile terminal		X		X		
Application server						
Relation between mobile user and mobile terminal			X			X
Relation between mobile terminal and application server	X	X			X	
Mobile security gateway		X				
Relation between mobile terminal and mobile security gateway	X	X			X	
Relation between application server and mobile security gateway	X	X			X	

9 Security requirements for mobile end-to-end data communication

There are two types of security requirements for mobile end-to-end data communication. One is from mobile user's point of view. Another is from ASP's point of view.

9.1 Security requirements for mobile user's point of view

There are many different user expectations and needs when it comes to applications. What is common to most mobile users is their simple expectation that the application works and is easy to use. Most people expect the applications and service providers to handle their personal data in a secure and privacy respecting way. To give a proper way, mobile user has the following information security requirements.

- Identity management
- Data confidentiality
- Data integrity
- Authentication
- Access control
- Non-repudiation
- Anonymity
- Privacy
- Usability
- Availability

9.1.1 Identity management

Identity management is typically related to protect from revealing information about the user identity. Therefore, identity management is very important aspects of user privacy. Pseudonym can be used during communication. Mobile user's identity management requirement is to generate (or request to generate), maintain, delete (or request to delete), and apply of keys in accordance with mobile user's security policy.

9.1.2 Data confidentiality

Mobile user's data confidentiality requirement consist of following requirements:

Communication data confidentiality between mobile terminal and application server

This is to provide the confidentiality of all or sensitive data transmitted between mobile terminal and application server.

Stored data confidentiality on mobile terminal

This is to provide the confidentiality of all or sensitive data stored in mobile terminal.

Stored data confidentiality on application server

This is to provide the confidentiality of all or sensitive data in application server that are associated with mobile user.

In "Gateway model", mobile user's data confidentiality requirements includes additional requirements as follows:

Communication data confidentiality between mobile terminal and mobile security gateway

This is to provide the confidentiality of all or sensitive data transmitted between mobile terminal and mobile security gateway.

Communication data confidentiality between application server and mobile security gateway

This is to provide the confidentiality of all or sensitive data transmitted between application server and mobile security gateway.

Stored data confidentiality on mobile security gateway

This is to provide the confidentiality of all or sensitive data stored in mobile security gateway.

9.1.3 Data integrity

Mobile user's data integrity requirement consists of following requirements:

Communication data integrity between mobile terminal and application server

This is to provide the integrity of all communication data between mobile terminal and application server.

Stored data integrity on mobile terminal

This is to provide the integrity of all data stored in mobile terminal.

Stored data integrity on application server

This is to provide the integrity of all data stored in application server that are associated with mobile user (for example, mobile user's personal information).

In "Gateway model", mobile user's data integrity requirements includes additional requirements as follows:

Communication data integrity between mobile terminal and mobile security gateway

This is to provide the integrity of all data transmitted between mobile terminal and mobile security gateway.

Communication data integrity between application server and mobile security gateway

This is to provide the integrity of all data transmitted between application server and mobile security gateway.

Stored data integrity on mobile security gateway

This is to provide the integrity of all data stored in mobile security gateway that is associated with mobile user.

9.1.4 Authentication

There are two kinds of authentication: entity authentication and message authentication. The entity authentication is for one entity to prove its identity to corresponding entity. The message authentication is to prove the origin of data or receipt of data. Mobile user's authentication requirement consists of following requirements:

ASP authentication

This is a kind of entity authentication and to confirm the identities of ASP to provide to confidence that ASP is not attempting a masquerade or unauthorized replay of a previous connection.

Mobile user authentication

This is a kind of entity authentication and to prove the identity of user to mobile terminal using various user authentication schemes such as finger printing, password, or PIN to provide protection against unauthorized access from lost or stolen mobile terminal.

Received data authentication

This is a kind of message authentication and to the corroboration of the source of a communication data. This does not request to provide protection against duplication or modification of data.

9.1.5 Access control

Mobile user's access control requirement consists of following requirements:

Access control on mobile terminal

This is to provide protection against unauthorized access to or unauthorized use of mobile terminal.

The control of access will be in accordance with mobile user's security policies.

Access control on application server

This is to provide protection on application server against unauthorized access to data sent by mobile user like mobile user's personal information.

The control of access will be in accordance with mobile user's security policies.

In "Gateway model", mobile user's privacy requirements includes additional requirements as follows:

Access control on mobile security gateway

This is to provide protection on mobile security gateway against unauthorized access to data sent by mobile user like mobile user's personal information.

The control of access will be in accordance with mobile user's security policies.

9.1.6 Non-repudiation

This is one or both of two forms as follows:

Non-repudiation with proof of origin

This is to provide that the origin of received data is particular ASP. This is required to protect against any attempt by the ASP to falsely deny sending the data.

Non-repudiation with proof of delivery

This is to provide the proof of delivery of data to ASP. This is required to protect against any subsequent attempt by the ASP to falsely deny receiving the data.

Non-repudiation requirements will have relation to following requirements: communication data confidentiality between mobile terminal and application server, communication data integrity between mobile terminal and application server, stored data integrity on mobile terminal, mobile user authentication and access control on mobile terminal.

In "Gateway model", this will also have relation to following requirements: communication data confidentiality between mobile terminal and mobile security gateway, communication data confidentiality between mobile security gateway and application server, communication data integrity between mobile terminal and mobile security gateway, communication data integrity between mobile security gateway and application server, stored data integrity on mobile security gateway.

9.1.6 Anonymity

This is to provide an ability to send a message so that ASP cannot find out the identity of mobile user (and mobile terminal).

9.1.7 Privacy

This is to avoid leakage of information and to prevent unauthorized person from getting the information.

Privacy requirements will have relation to following requirements: communication data confidentiality between mobile terminal and application server, stored data confidentiality on mobile terminal, stored data confidentiality on application server, access control on mobile terminal and access control on application server.

In "Gateway model", will also have relation to following requirements: communication data confidentiality between mobile terminal and mobile security gateway, communication data confidentiality between mobile security gateway and application server, stored data confidentiality on mobile security gateway and access control on mobile security gateway.

9.1.8 Usability

This is to provide easy use of application and to avoid misreading or input error.

9.1.9 Availability

This is for mobile user to provide an ability to receive application service anywhere and anytime.

9.2 Security requirements for ASP's point of view

Businesses, which offer their services to mobile users, have to protect their systems against fraud. Because of the specialty of mobile equipment, subscriber authentication and payment mechanism should be managed carefully. Furthermore, if service is given to the mobile users, non-repudiation and traceability for the service cannot be avoidable. Therefore, ASP has the following requirements:

- Data confidentiality
- Data integrity
- Authentication
- Access control
- Non-repudiation
- Availability

9.2.1 Data confidentiality

ASP's data confidentiality requirement consist of following requirements:

Communication data confidentiality between mobile terminal and application server

This is to provide the confidentiality of all or sensitive data transmitted between mobile terminal and application server.

Stored data confidentiality on mobile terminal

This is to provide the confidentiality of all or sensitive data or contents that are sent by ASP and stored in mobile terminal.

Stored data confidentiality on application server

This is to provide the confidentiality of all data stored in application server.

In "Gateway model", mobile user's data confidentiality requirements includes additional requirements as follows:

Communication data confidentiality between mobile terminal and mobile security gateway

This is to provide the confidentiality of all or sensitive data transmitted between mobile terminal and mobile security gateway.

Communication data confidentiality between application server and mobile security gateway

This is to provide the confidentiality of all or sensitive data transmitted between application server and mobile security gateway.

Stored data confidentiality on mobile security gateway

This is to provide the confidentiality of all or sensitive data (or contents) that are sent by ASP and stored in mobile security gateway.

9.2.2 Data integrity

ASP's data integrity requirement consists of following requirements:

Communication data integrity between mobile terminal and application server

This is to provide the integrity of all communication data between mobile terminal and application server.

Stored data integrity on mobile terminal

This is to provide the integrity of all data or contents that are sent by ASP and stored in mobile terminal.

Stored data integrity on application server

This is to provide the integrity of all data stored in application server.

In "Gateway model", mobile user's data integrity requirements includes additional requirements as follows:

Communication data integrity between mobile terminal and mobile security gateway

This is to provide the integrity of all (or part of) data transmitted between mobile terminal and mobile security gateway.

Communication data integrity between application server and mobile security gateway

This is to provide the integrity of all data transmitted between application server and mobile security gateway.

Stored data integrity on mobile security gateway

This is to provide the integrity of all data or contents that are sent by ASP and stored in mobile security gateway.

9.2.3 Authentication

ASP's authentication requirement also consists of entity authentication (mobile user authentication and mobile terminal authentication) and message authentication (received data authentication).

Mobile user authentication

This is a kind of entity authentication and to confirm the identities of mobile user to provide to confidence that mobile user is not attempting a masquerade or unauthorized replay of a previous connection.

Mobile terminal authentication

This is a kind of entity authentication and to confirm the identities of mobile terminal to ensure that mobile terminal equips the functionality to provide application service.

Received data authentication

This is a kind of message authentication to confirm the corroboration of the source of a communication data. It is not a request to provide protection against duplication or modification of data.

9.2.4 Access control

ASP's access control requirement consists of access control on application server and access control on mobile terminal.

Access control on application server

This is to provide protection against unauthorized access to or unauthorized use of application server.

The control of access will be in accordance with ASP's security policies.

Access control on mobile terminal

This to provide protection on mobile terminal against unauthorized access to data or contents sent by ASP.

The control of access will be in accordance with ASP's security policies.

In "Gateway model", ASP's access control requirements includes additional requirements as follows:

Access control on mobile security gateway

This to provide protection on mobile security gateway against unauthorized access to data or contents sent by ASP.

The control of access will be in accordance with ASP's security policies.

9.2.5 Non-repudiation

This is one or both of two forms as follows:

Non-repudiation with proof of origin

This is to prove that the origin of received data is particular mobile user. This is also request to protect against any attempt by the mobile user to falsely deny sending the data or its contents.

Non-repudiation with proof of delivery

This is to provide the proof of delivery of data to mobile user. This is also request to protect against any subsequent attempt by the mobile user to falsely deny receiving the data or its contents.

ASP's Non-repudiation requirements will have relation to following requirements: communication data confidentiality between mobile terminal and application server, communication data integrity between mobile terminal and application server, stored data integrity on mobile terminal, mobile user authentication and access control on mobile terminal.

In "Gateway model", this will also have relation to following requirements: communication data confidentiality between mobile terminal and mobile security gateway, communication data confidentiality between mobile security gateway and application server, communication data integrity between mobile terminal and mobile security gateway, communication data integrity

between mobile security gateway and application server, stored data integrity on mobile security gateway.

9.2.6 Availability

This is for authorized mobile user to provide an ability to receive application service anywhere and anytime.

9.3 Relationship of security requirements and security threats

Each security requirements are countermeasures against certain security threats. The relationship of security requirements and security threats shows below (Table 3 and 4).

Table 3 - Relationship of security requirements and general security threats

Threats / Requirements	Eavesdropping	Communication jamming	Injection/ Modification	Interruption	Unauthorized access	Repudiation
Identity management	X				X	X
Communication data confidentiality	X					
Stored data confidentiality					X	
Communication data integrity			X			
Stored data integrity					X	
Entity authentication			X		X	X
Message authentication			X			
Access control			X		X	
Non-repudiation						X
Anonymity					X	
Privacy	X				X	
Usability						
Availability		X		X		

Table 4 - Relationship of security requirements and mobile-oriented security threats

Threats / Requirements	Eavesdropping	Communication jamming	Shoulder surfing	Lost/Stolen terminal	Unprepared shutdown	Misreading/ Input error
Identity management	X					
Communication data confidentiality	X					
Stored data confidentiality				X		
Communication data integrity						
Stored data integrity				X		
Entity authentication				X		
Message authentication						
Access control				X		
Non-repudiation						
Anonymity				X		
Privacy	X		X	X		
Usability						X
Availability		X			X	

10 Security functions for satisfying mobile security requirements

To satisfy security requirements for mobile end-to-end data communication, there are several security functions as follows:

- Encipherment
- Key exchange
- Digital signature
- Access control
- Data integrity
- Authentication exchange
- Notarization

Encipherment

Encipherment function can provide confidentiality of either communication data or stored data.

Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithm:

a) Symmetric (i.e. secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice versa; and

b) Asymmetric (e.g. public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret.

Because of low processing capability or small memory size of mobile terminal, there are some difficulties to use existing encipherment function, especially asymmetric algorithm, used in existing open network. In the case that it continues to use existing encipherment function on the server in the open network, gateway model is often used.

Key exchange

Key exchange function can share a key for some of encipherment function, especially symmetric encipherment algorithm, to encipher data.

Digital signature

The digital signature function define two procedures:

a) Signing a data, and

b) Verifying a signed data.

The first process uses information that is private (i.e. unique and confidential) to the signer. The second process uses procedures and information which are publicly available but from which the signer's private information cannot be deduced.

The signing process involves either an encipherment of the data or the production of a cryptographic check value of the data, using the signer's private information as a private key.

The verification process involves using the public procedures and information to determine whether the signature was produced correctly with the signer's private information.

The essential characteristic of the signature function is that the signature can only be produced using the signer's private information. Thus when the signature is verified, it can subsequently be

proven to a third party (e.g. a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

Same as encipherment function, due to low processing performance or small memory size of mobile terminal, there are some difficulty to use existing digital signature function used in existing open network.

Access control

Access control function may use the authenticated identity of an entity or information about the entity (such as membership in a known set of entities) or capabilities of the entity, in order to determine and enforce the access rights of the entity. If the entity attempts to use an unauthorized resource, or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail.

Access control function may be based on use of following items:

a) Access control information bases, where the access rights of peer entities are maintained in a database.

b) Authentication information such as passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization;

c) Capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability.

d) Security labels, which when associated with an entity may be used to grant or deny access, usually according to a security policy.

e) Time of attempted access.

f) Route of attempted access,

g) Duration of access, and

h) Physical location of attempted access

Access control function may be applied at either peer entity of a communications association and/or at mobile security gateway.

Access controls involved at the origin or mobile security gateway are used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communications resources.

Data integrity

Two aspects of data integrity are: the integrity of a single data unit or field and the integrity of a stream of data units or fields. In general, different technologies are used to provide these two types of integrity function, although provision of the second without the first is not practical.

Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends to data a quantity that is a function of the data itself. This quantity may be supplementary information such as a block check code or a cryptographic check value and may it be enciphered. The receiving entity generates a corresponding quantity and compares it with the received quantity to determine whether the data has been modified in transit. This alone will not protect against the replay of a single data unit.

Protecting the integrity of a sequence of data units (i.e. protecting against disordering, losing, replaying and inserting or modifying data) requires additionally some form of explicit ordering such as sequence numbering, time stamping, or cryptographic chaining.

Authentication exchange

Some of security technologies that may be applied to authentication exchanges are:

a) Use of authentication information, such as passwords supplied by a sending entity and checked by the receiving entity;

b) Cryptographic technologies; and

c) Use of characteristics and/or possessions of the entity.

Authentication exchange function may be incorporated in order to provide peer entity authentication. If the function does not succeed in authenticating the entity, this will result in rejection or termination of the connection and may cause an entry in the security audit trail and/or a report to a security management centre.

When cryptographic techniques are used, they may be combined with "handshaking" protocols to protect against replay (i.e. to ensure liveness).

The choices of security technologies, which realize authentication exchange, will depend upon the circumstances in which they will need to be used with:

a) Time stamping and synchronized clocks;

b) Two and three way handshakes (for unilateral and mutual authentication respectively); and

c) Non-repudiation functions achieved by digital signature and/or notarization mechanisms.

Notarization

Properties about the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization function. The assurance is provided by a third party notary, which is trusted by the communicating entities, and which holds the necessary information to provide the required assurance in a verifiable manner. Each instance of communication may use digital signature, encipherment, and integrity functions as appropriate to the service being provided by the notary. When such a notarization function is invoked, the data is communicated between the communicating entities via the protected instances of communication and the notary.

These security functions are used to satisfy some of security requirements. Which functions satisfy which security requirements shows below (Table 5).

Table 5 - Illustration of relationship of security requirements and functions

Functions / Requirements	Encipherment	Key exchange	Digital signature	Access control	Data integrity	Authentication exchange	Notarization
Identity management	X	X	X			X	
Communication data confidentiality	X	X		X		X	
Stored data confidentiality	X			X			
Communication data integrity	X	X	X	X	X	X	
Stored data integrity	X		X	X	X		
Entity authentication	X		X			X	
Message authentication	X	X	X		X	X	
Access control				X		X	
Non-repudiation			X			X	X
Anonymity	X						
Usability				X			
Privacy	X			X		X	
Availability				X		X	

11 Security technologies for mobile end-to-end data communication

To realize security function described in above section, various security technologies for mobile end-to-end data communication (i.e. secure mobile technologies) are used. These secure mobile technologies are categorized by security functions realized by the security technology and places to which the security technology applies. Because a security technology applies to an entity or a relation between entities in models of mobile end-to-end data communication, the places to which the security technology is applied denote entities or relations between entities. Table 1 and 2 show where security threats appear in models of mobile end-to-end data communication. Table 3 and 4 which security functions are taken to make countermeasures to particular security threats and Table 5 shows the security functions to satisfy the security requirements. Therefore, the relationship between security functions and places to apply these security functions in models can be shown as Table 6. In other words, Table 6 shows where mobile security technologies, which realize certain security function, are applied to in models.

Particular mobile security technology may realize only a part of security functions or be applied to particular place. For example, elliptic curve cryptographic algorithm can be used to realize Key Exchange function in the relation between user and mobile terminal. Biometrics authentication technology can be used to realize Authentication Exchange function in the relation between user and mobile terminal. PKI technology can be used to realize all security functions in the relation between mobile terminal and server, the relation between mobile terminal and mobile security gateway, and the relation between server and mobile security gateway.

Table 6 – Relationship of secure mobile technologies and models

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	X	X	X
Key Exchange				X
Digital Signature	X	X		X
Access Control	X	X	X	X
Data Integrity	X	X		X
Authentication Exchange	X	X	X	X
Notarization				X

New ITU-T Recommendation X.1122 (Formerly X.msec-2)

Guideline for implementing secure mobile systems based on PKI

Summary

Although 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 communication, 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 shows the guideline when constructing secure mobile systems based on PKI technology.

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 X.msec-1 (2004), *Framework of security technologies for mobile end-to-end data communications*

– ITU-T Recommendation X.509 | ISO/IEC 9594-8 (2000), *Public-key and attribute certificate frameworks*

– ITU-T Recommendation X.800 | ISO/IEC 7498-2 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*

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

– ITU-T Recommendation F.160 (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*

3 Terms and Definitions

For the purposes of this Recommendation, the following definitions apply

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 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 terms are 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 terms are defined in ITU-T Rec. F.160:

a) User Identity Module;

3.5 Additional definitions

The following terms are defined in this Recommendation:

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 is reliable or is not revoked. It also verifies if a Certificate has been revoked.

4 Abbreviations

For the purposes of this Recommendation, the following abbreviations apply.

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 belongs

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

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

(1) Encipherment

(2) Key Exchange

(3) Digital Signature

(4) Access Control

(5) Data Integrity

(6) Authentication Exchange

(7) Notarization

Table 1 – 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 open network to realize above 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

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

General model of secure mobile systems based on PKI for communication between mobile user and ASP shows below.

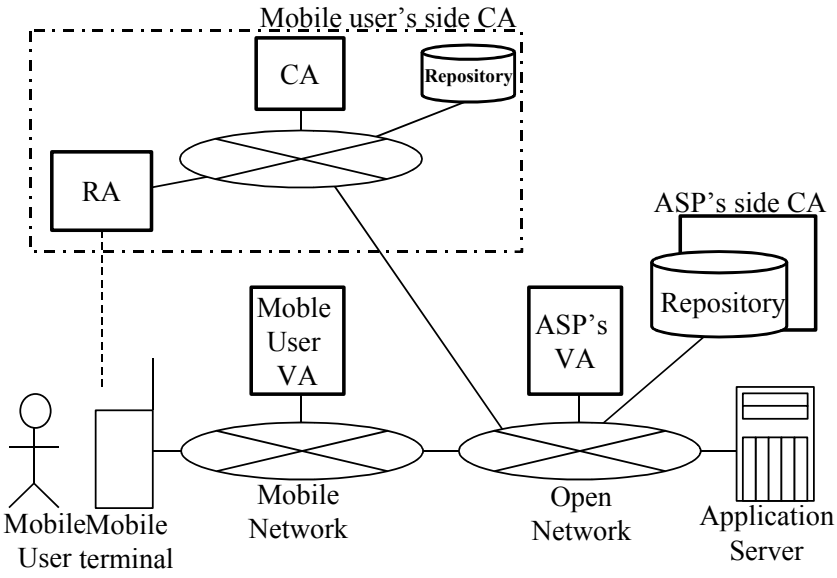

Figure 1 – General model of secure mobile systems based on PKI

This model contains additional entities than general model of mobile end-to-end data communication between mobile user and ASP; 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

Mobile user's side CA issues and manages mobile user's Certificate or mobile terminal's Certificate. This contains RA that is responsible for identification and authentication of mobile user and Repository that stores mobile user's Certificate and CRL.

– Mobile user's VA

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

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

– ASP's VA

ASP's VA provides an online service of verification of validity of Certificate received by ASP.

6.2 Gateway model of secure mobile systems based on PKI

Gateway model of secure mobile systems based on PKI for communication between mobile user and ASP shows below.

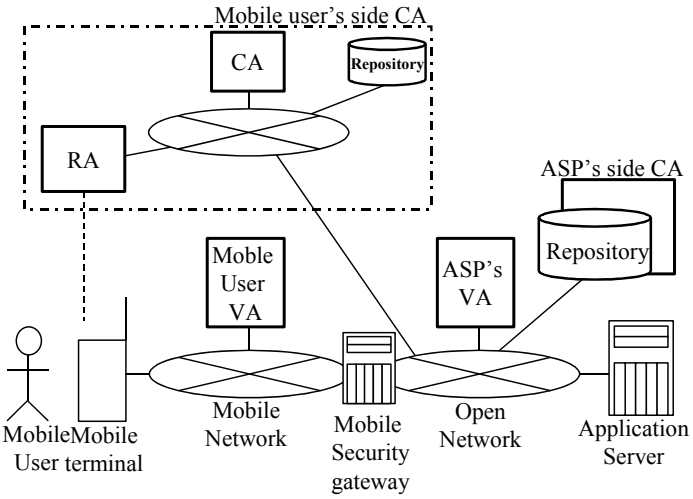

Figure 2 – Gateway model of secure mobile systems based on PKI

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

(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 key and public key

For the generation of a pair of private key and public key, 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 in the security point of view, there can be a model in which the CA generates the keys instead of 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 that the user purchases the device in which the keys are installed. (The device might be a mobile terminal itself or 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 to the device.

7.1.2 Application for and 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 utilisation of the Certificate and so on.

Furthermore, in the mobile environment, the models are differently depending on the relationship between the timings 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 timings 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 timings 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 to provide 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 needed:

(1) Verification of the validity of the Certificate

This is to verify the authenticity of the Certificate of the signer. Concretely, discover an authentication path of the Certificate and verify 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 on-line, 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 at each time of verifying the Certificate).

(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 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 can be 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 (the information of) the existing Certificate is used in the application for the new Certificate.

8 The usage model in the telecommunications services

This section 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). And the application layer usage model is a model that provides the functions of integrity and confidentiality on the application layer.

Many of existing implementations of the over-the-session-layer usage model (TLS is famous 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 can be also 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 very important roles for 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 section 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 the Certificate of the application server 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.

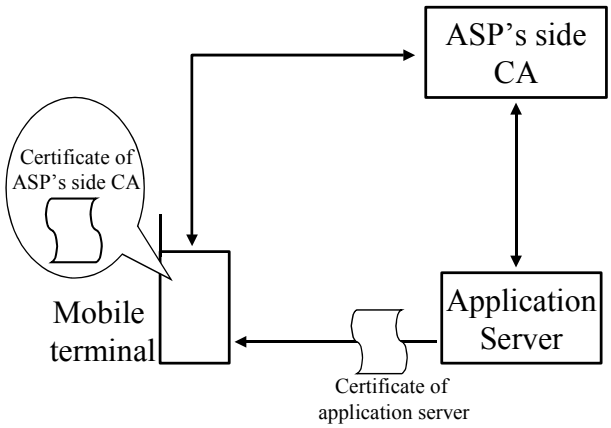

Figure 3 –Server authentication in the general model

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:

- At first, a protected session is established between the mobile terminal and the mobile security gateway by using 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.

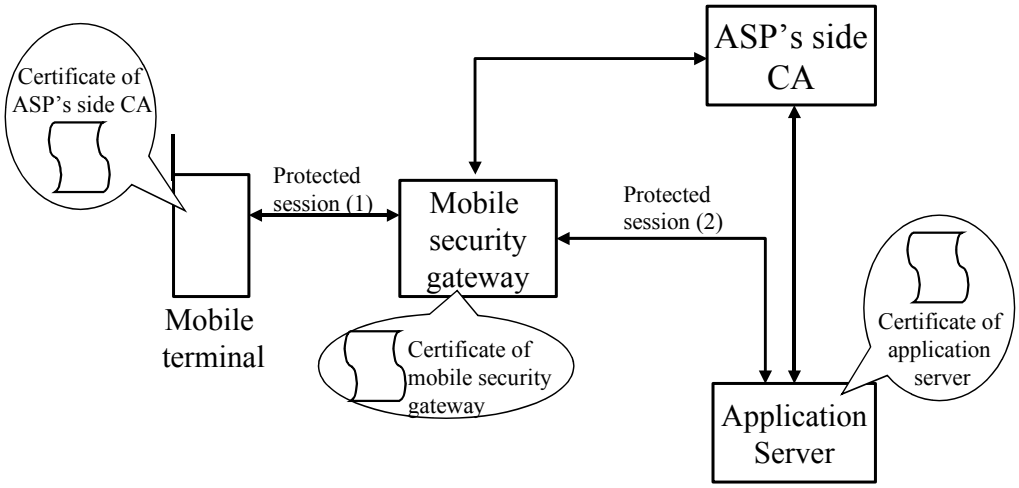

Figure 4 –Server authentication in the gateway model

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.

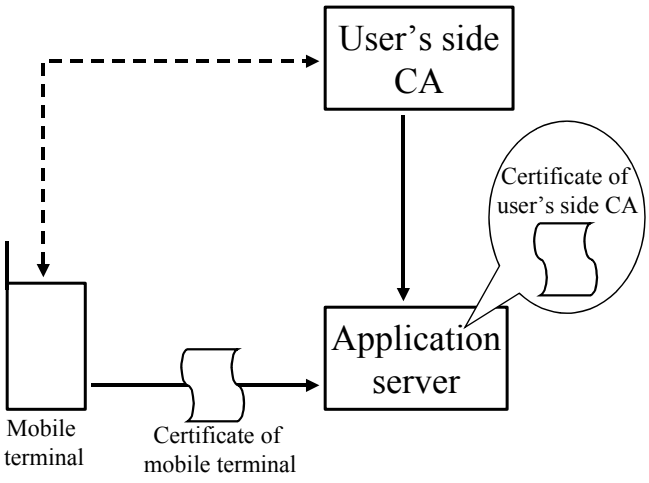

Figure 5 –Client authentication in the over-the-session-layer usage model

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 of the mobile terminal 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 mobile terminal from the repository using the location information of the Certificate.
- The application server verifies the validity of the Certificate of mobile terminal (if needed), verifies the signature with its public key in the Certificate of mobile terminal and the application server authenticates the mobile terminal by using the Certificate of mobile terminal.
- A protected session is established between the mobile terminal and the application server.

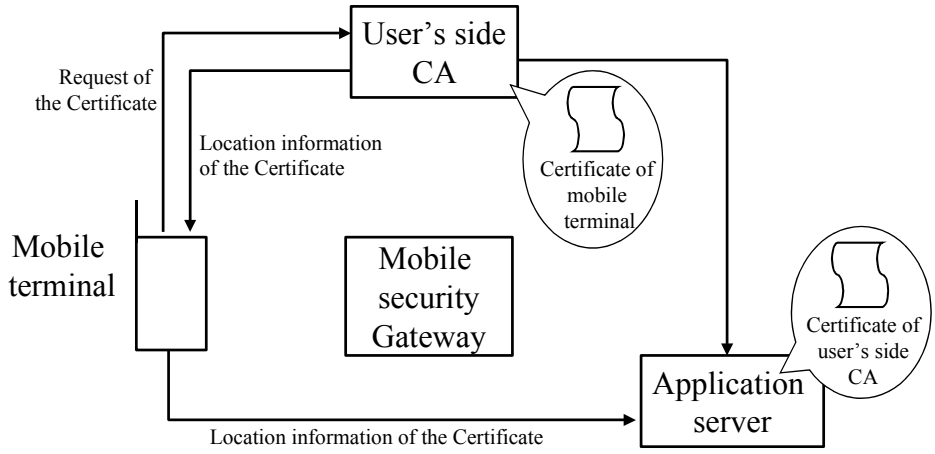

Figure 6 –Client authentication in the over-the-session-layer usage model

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 seed of session key and encrypts it with the public key of the applications server in the Certificate of the application server, in the case of RSA key exchange method, and sends to the application server the encrypted seed of session key. Both the application server and the mobile terminal can make the common session key for subsequent communication from the seed.
- The encrypted communications are started.

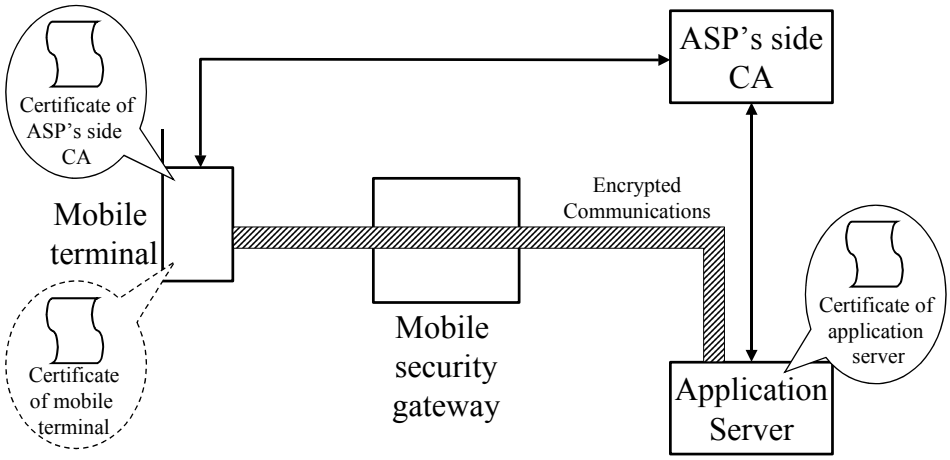

Figure 7 –Communication path encryption in the over-the-session-layer usage model

8.2 Usage model on the application level

PKI can be utilized for an application specific encryption function, a digital signature function, and combination of the both, which necessitate 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 Function of signing at the application level

This function guarantees the integrity of the data and creates a digital signature to guarantee that the data has been originated from the signing person on the hashed value of data transmitted from the mobile terminal. 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 function of signing 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 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 Function of encryption at the application level

This is to provide an encryption function at the application level to allow 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 Certificate Management System

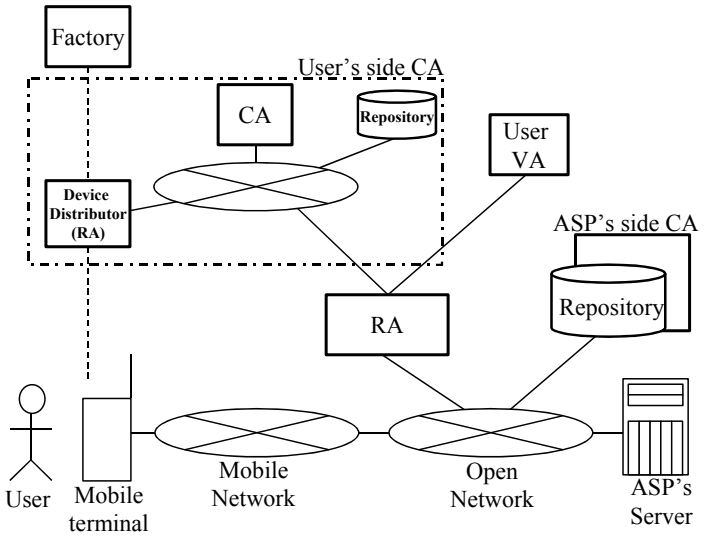

Figure 8 – Example of a system in which the communication carrier issues a Certificate for its user

This is 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.

9.1.1 Example of Certificate issuance

There are two examples to issue 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 ~~(POP).~~ The POP (proof of possession) 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 upon the type of key for which a certificate is requested.

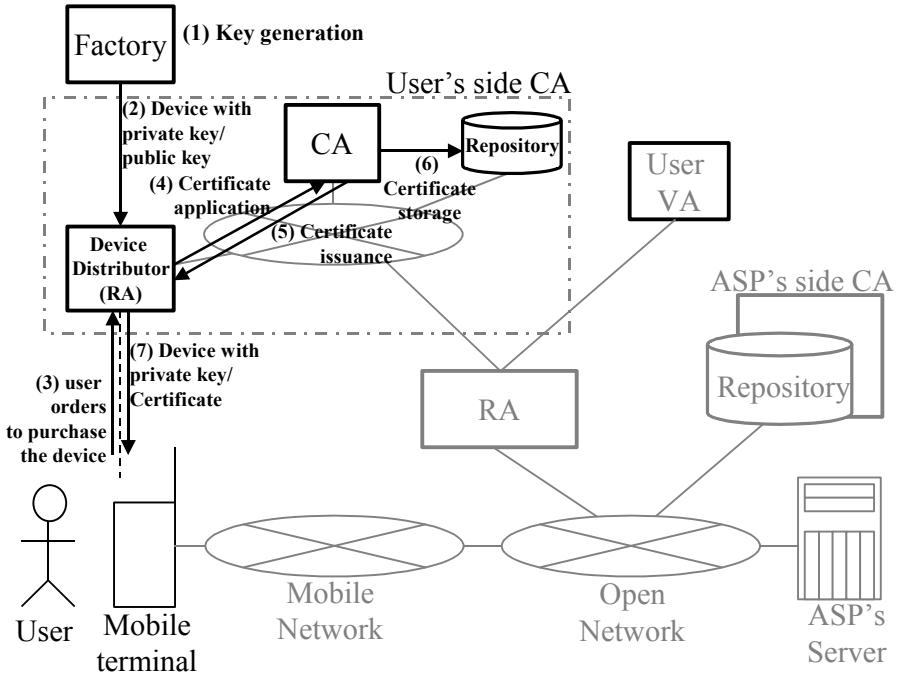

Figure 9 – Example of Certificate issue (1)

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 is installed by the distributor. This is when POP is carried out.

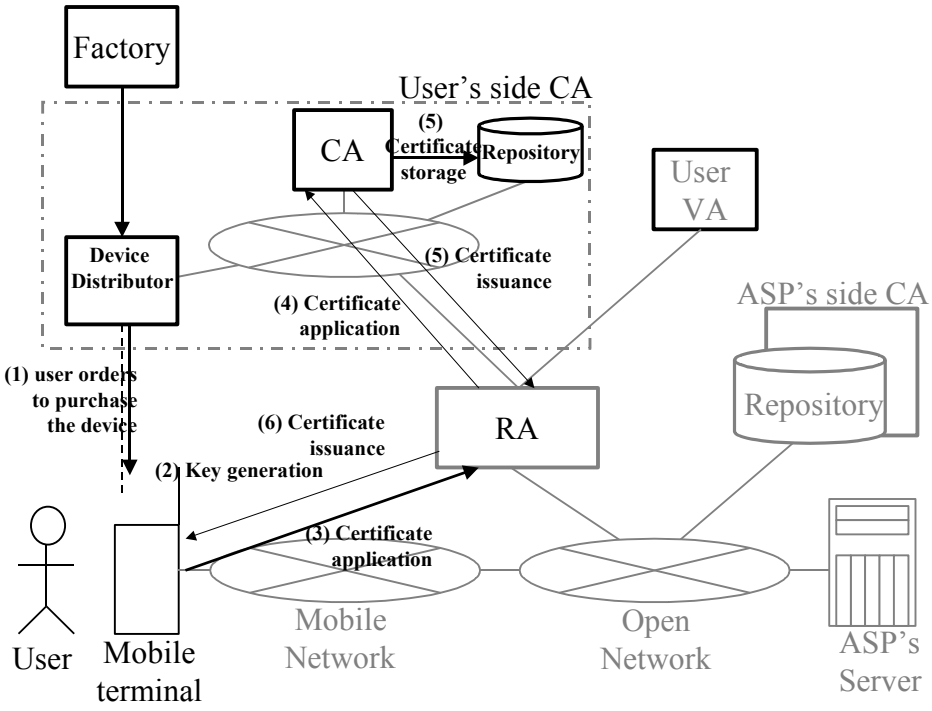

Figure 10 – Example of Certificate issue (2)

Figure 10 shows an example of a system in which the client generates a key and issues a request of Certificate itself. The Certificate is applied for when the user want to receive it from CA and the private key could be kept secret in the mobile terminal. Before 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 private key of mobile terminal.

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 the example of online certificate verification.

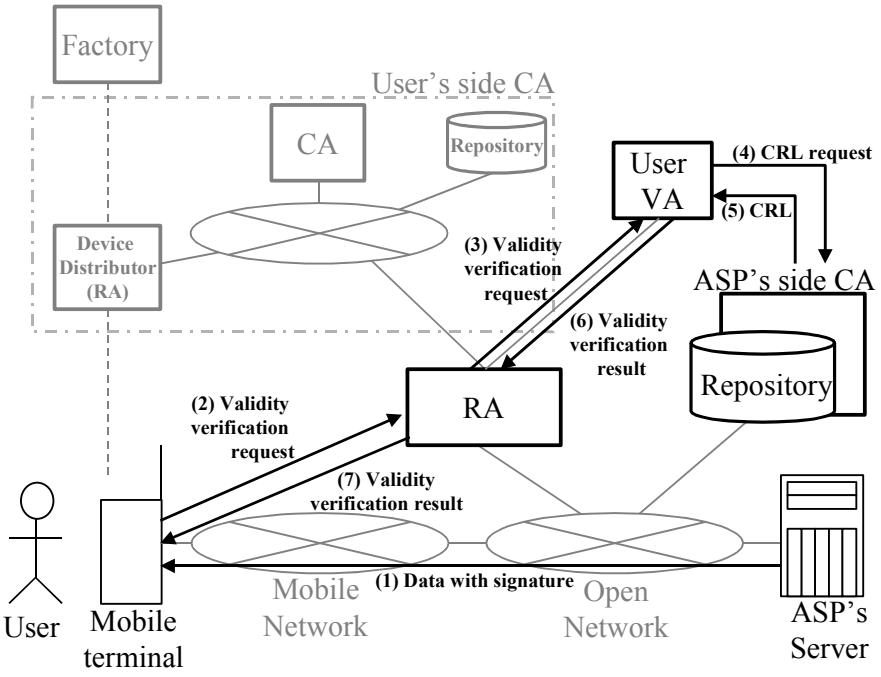

Figure 11 – Example of Certificate verification

To verify the data received from an ASP, the user inquires to a VA if the Certificate of 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 the section 10.2.3.2)

9.1.3 Example of Certificate revocation

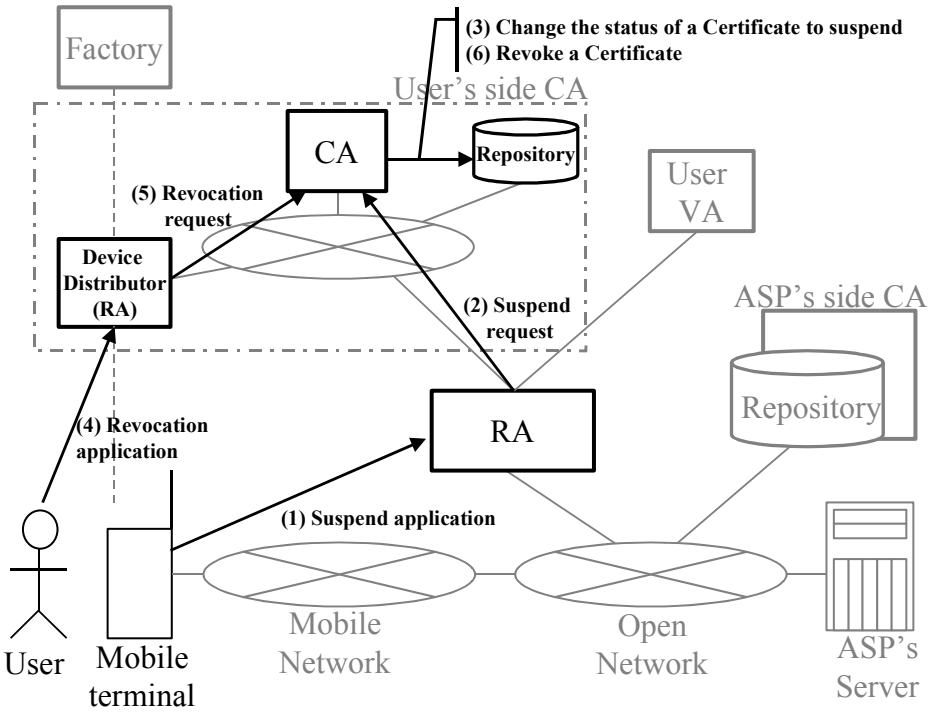

Figure 12 – Example of Certificate revocation

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, submit the application to the CA through the RA. The revocation could complete by submitting the signed application to CA through RA. For the case of lost or stolen of the mobile terminal, the alternatives to suspend the validity should be needed. For example, the user can suspend by calling to device distributor to make a request for suspending.

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 among a user, a carrier and an application service provider (ASP)

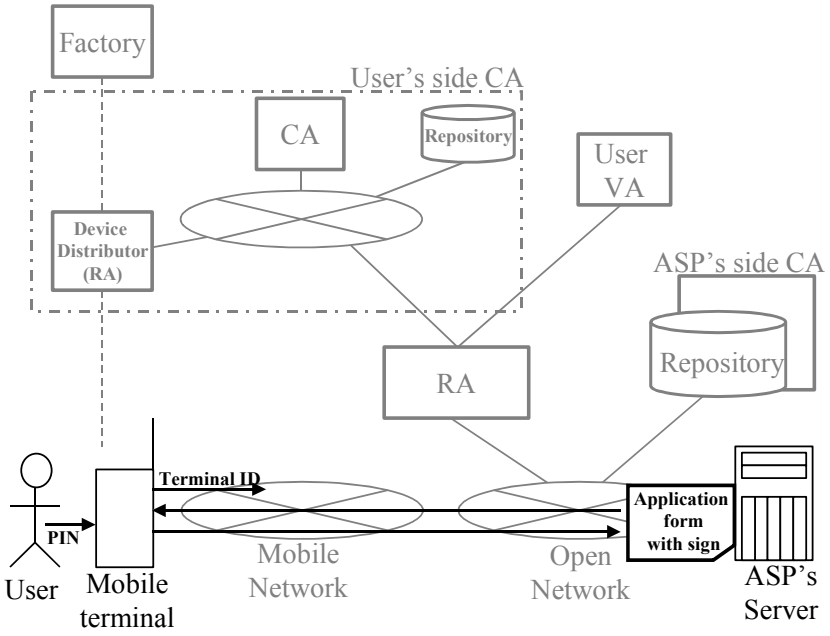

Figure 13 – Example of an authentication model among a user, a carrier and an ASP

9.2.1.1 Authentication of mobile terminal user by 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 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 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 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. Other 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 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 mobile user) itself and the relevant authentication data such as digital signature, message authentication code, and the encrypted data using the private key of 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 authentication model utilizing financial institution

An authentication model utilizing credit card information or other existing infrastructures is also possible.

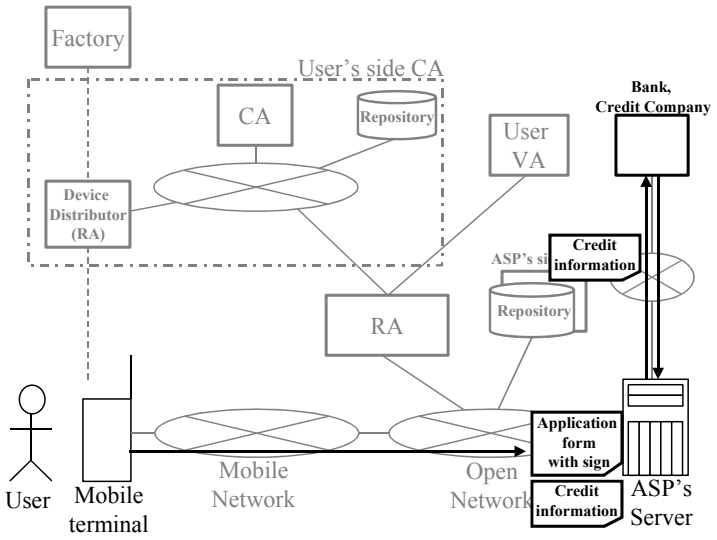

Figure 14 – Example of authentication model utilizing financial institution

9.2.2.1 User authentication by 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 PIN should be needed when this information is used in the mobile terminal in order to identify the legal user that has an access right to them.

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 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 bank, can be used to certify an authorised distributor.

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

10.1 Considerations of interoperability with existing system

When adapting the existing system based on PKI already developed with the open network into a mobile environment, the Certificates for 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 ASP's Certificate format because of constraints of throughput capacity or memory capacity, 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 cannot have enough space to store his/her/its Certificate, the mobile terminal may keep the Certificate URL instead of Certificate itself, and it sends to ASP the Certificate URL. 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 of existing systems using the PKI, RSA cryptographic algorithm is widely used as a signature algorithm. However, the RSA cryptographic algorithm may need more processing powers than that 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 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 approach to resolve the above is introducing the VA with the function to verify a signature, another consideration exists on 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, it technically has no problem even if it is adopted for the mobile terminal.

In addition, as SSL/TLS interchange their Certificates at the initialization stage, this may needs more storage area than that 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 higher layer may be needed.

10.2 Considerations of PKI Use 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 take out 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 to 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, user's public key (Certificate) and the Certificate of root CA are stored 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 preinstalled in the device

For models in which the mobile user purchases the device with the Certificate preinstalled, it is difficult to update the key and the Certificate.

In addition, in the case that 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 preinstalled 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 TLS, the method of attaching the Certificates (all Certificates from the root CA Certificate to signer's Certificate) to the message is adopted as the method to associate the root CA Certificate with 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 verify the signature

Models where Certificate validity is verified by the verifier by 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 section 9.1.2, the mobile terminal accesses the VA through the RA. In this case, the mobile terminal requires a function to recognise 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. For the RA, it needs a function to know the VA which the mobile terminal relies on and requires a function to certify that the VA is valid while communicating with the VA.

10.2.4 Considerations with CA

For existing systems using the PKI, they establish reliable relationships between different certification domains 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 of PKI general

10.3.1 Considerations with key generation

10.3.1.1 Key generator

For models where the user generates the keys, it may be possible that someone may search other'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, some schemes may be required to prevent Certificates of others from being easily acquired.

10.3.2 Considerations with Certificate application/issuance/activation

10.3.2.1 When Certificate activation procedure is required

When the user explicitly follows the Certificate activation procedure, the mechanism to ensure that the procedure 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 utilised.

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 with Certificate revocation

To adopt a model with online revocation, the mechanism to verify that the applicant is the user is required. Especially, to revoke a Certificate because of the loss of a private key, applicant identification with a digital signature cannot be used. So, another method (such as PIN) must be provided.

To adopt a model with offline revocation, the provision of the mechanism to “suspend” a Certificate online may be required for emergency.

10.3.4 Considerations with renewing Certificate

In addition to the considerations on 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 annex describes the service models of the mobile PKI.

I.1 Certificate Management Service Models

In section 9, an example of offline use of the system is provided in which a communication carrier issues Certificates. This section provides other service models of Certificate management.

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

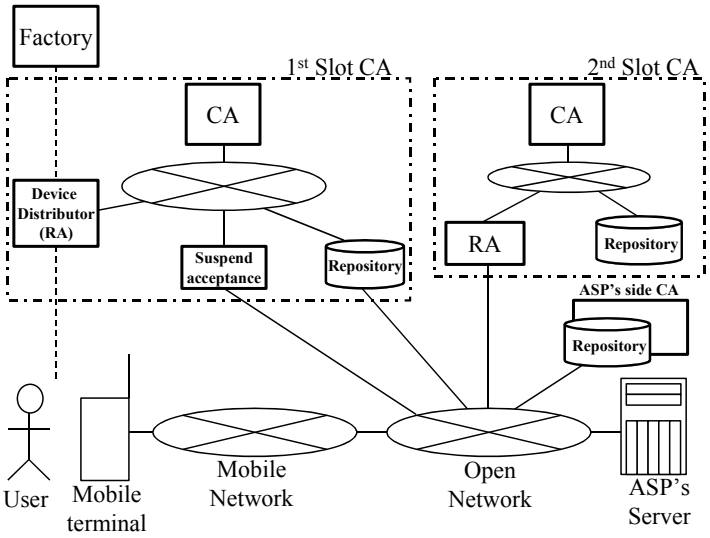

Figure I.2 – Example of a system in which an ASP issues Certificates

In this example, there are two kinds of Certificate; first Certificate is provided by 1st Slot CA which is a CA of carrier to provide the Certificate to mobile terminal to be used in secure session transport second Certificate is provided by 2nd Slot CA which is a CA of ASP to provide the Certificate to 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) use 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.

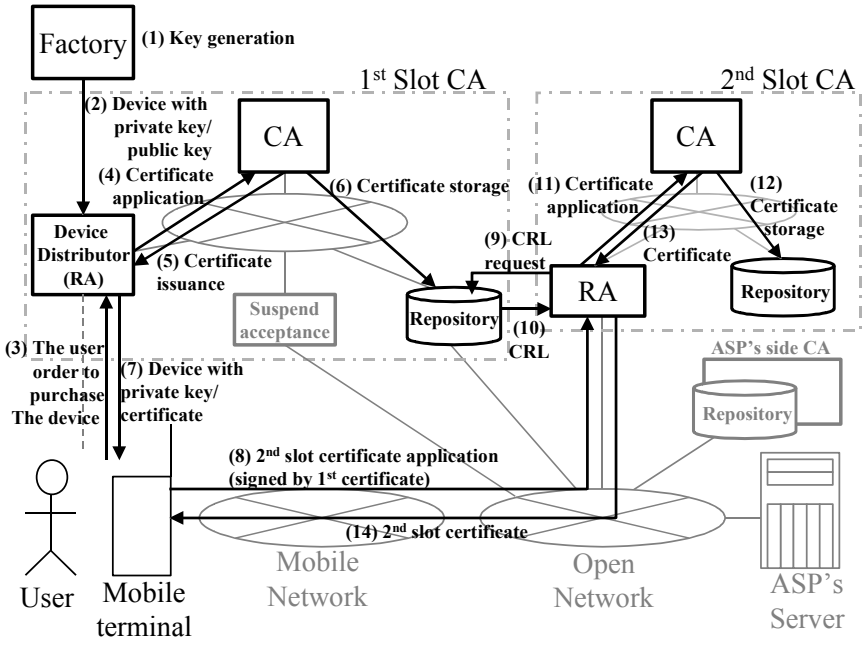

Figure I.3 – Example of 2nd slot Certificates issuance

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

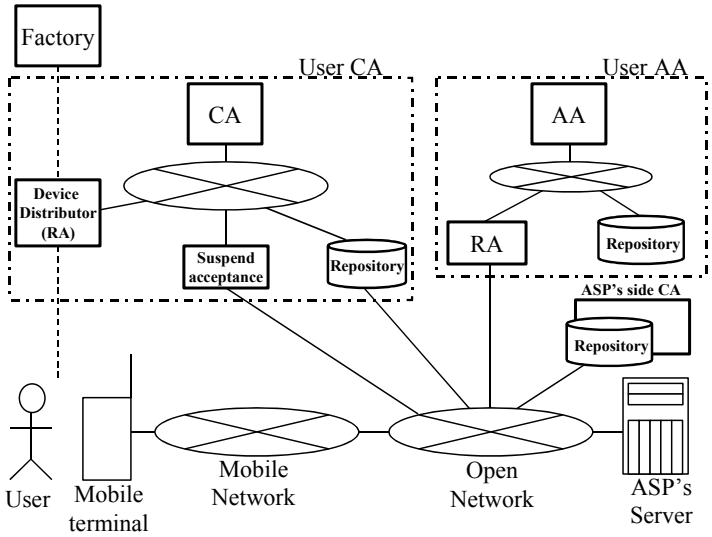

Figure I.4 – Example of a system in which an attribute certificate is utilized

This example assumes the ASP which 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 user, an user CA is used to issue an Certificate to user.

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.)

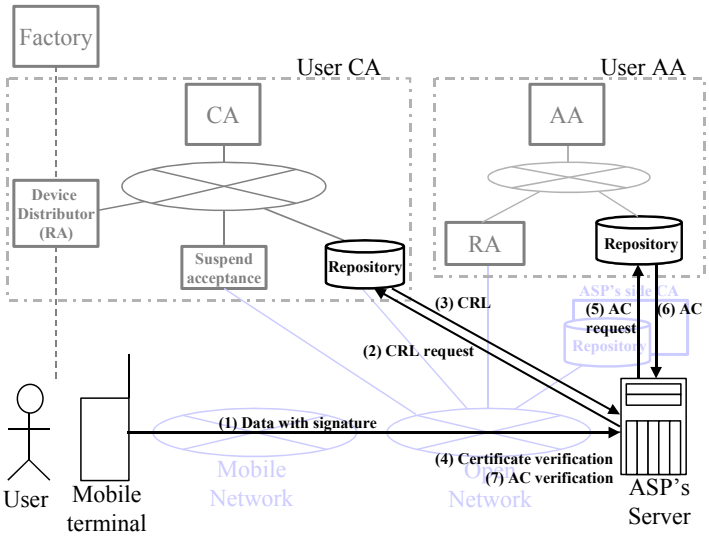

Figure I.5 – Example of authentication model using attribute certificate

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.