



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1122

(04/2004)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS

Telecommunication security

Guideline for implementing secure mobile systems based on PKI

ITU-T Recommendation X.1122

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

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

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

ITU-T Recommendation X.1122

Guideline for implementing secure mobile systems based on PKI

Summary

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

Source

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2004

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

		Page
1	Scope	1
2	References.....	1
3	Terms and definitions	2
3.1	Public-key and attribute certificate framework definitions	2
3.2	OSI Reference Model security architecture definitions	2
3.3	Guidelines for the use and management of trusted third party services definitions	2
3.4	Service features and operational provisions in IMT-2000 definitions	2
3.5	Additional definitions	2
4	Abbreviations.....	3
5	Categories to which PKI technologies belong.....	3
6	Models of secure mobile systems based on PKI	4
6.1	General model of secure mobile systems based on PKI.....	4
6.2	Gateway model of secure mobile systems based on PKI	5
7	PKI operations for mobile end-to-end data communication.....	6
7.1	PKI operations related to the life cycle of the certificate	6
8	The usage model in telecommunication services	9
8.1	Functions to be realized in the over-the-session-layer usage model	9
8.2	Usage model on the application level.....	13
9	System configuration examples.....	14
9.1	Configuration examples of a certificate management system.....	14
9.2	An example of an authentication model based on the certificate	18
10	Considerations of PKI for mobile end-to-end data communication.....	21
10.1	Considerations of interoperability with an existing system	21
10.2	Considerations for the use of PKI in the mobile environment	21
10.3	Considerations concerning the PKI in general	23
Appendix I – Examples of service models.....		24
I.1	Certificate management service models.....	24

ITU-T Recommendation X.1122

Guideline for implementing secure mobile systems based on PKI

1 Scope

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

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

2 References

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

- ITU-T Recommendation F.116 (2000), *Service features and operational provisions in IMT-2000*.
- ITU-T Recommendation Q.814 (2000), *Specification of an electronic data interchange interactive agent*.
- ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks*.
- ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000*.
- ITU-T Recommendation Q.1761 (2004), *Principles and requirements for convergence of fixed and existing IMT-2000 systems*.
- ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.
- ITU-T Recommendation X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Terms and definitions

3.1 Public-key and attribute certificate framework definitions

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

- a) Attribute Authority;
- b) Attribute Certificate;
- c) Certification Authority (CA);
- d) Certificate Revocation List (CRL);
- e) Public-key;
- f) Public-key certificate (Certificate);
- g) Public Key Infrastructure (PKI).

3.2 OSI Reference Model security architecture definitions

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

- a) authentication information;
- b) confidentiality;
- c) cryptography;
- d) key;
- e) password.

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

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

- a) Registration Authority.

3.4 Service features and operational provisions in IMT-2000 definitions

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

- a) User Identity Module.

3.5 Additional definitions

This Recommendation defines the following terms:

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

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

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

4 Abbreviations

This Recommendation uses the following abbreviations:

AA	Attribute Authority
ASP	Application Service Provider
CA	Certification Authority
CMC	Certificate Management over CMS
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
ID	Identifier
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
POP	Proof Of Possession
RA	Registration Authority
RSA	RSA public key algorithm
TLS	Transport Layer Security
UIM	User Identity Module
VA	Validation Authority

5 Categories to which PKI technologies belong

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

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

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

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

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

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

6 Models of secure mobile systems based on PKI

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

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

6.1 General model of secure mobile systems based on PKI

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

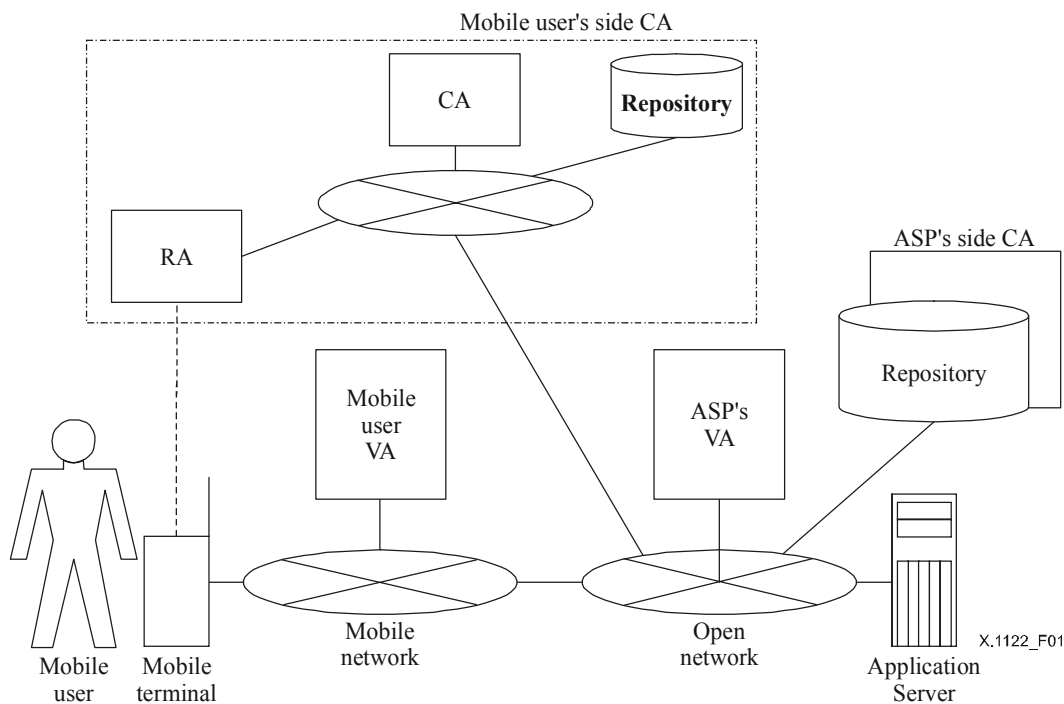


Figure 1/X.1122 – General model of secure mobile systems based on PKI

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

– *Mobile user's CA*

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

– *Mobile user's VA*

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

– *ASP's side CA*

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

– *ASP's VA*

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

6.2 Gateway model of secure mobile systems based on PKI

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