



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1121

(04/2004)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS

Telecommunication security

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

ITU-T Recommendation X.1121

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.1121

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

Summary

This Recommendation describes the security threats to mobile end-to-end data communications and the security requirements from the point of view of the mobile users and application service providers (ASP). In addition, this Recommendation shows where the security technologies which realize certain security function appear in the models of mobile end-to-end data communications.

Source

ITU-T Recommendation X.1121 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	Definitions	1
3.1	OSI Reference Model security architecture definitions	1
3.2	Additional definitions	2
4	Abbreviations.....	3
5	Overview	3
6	Models of mobile end-to-end data communications	3
6.1	General model of mobile end-to-end data communication between the mobile user and the ASP	3
6.2	Gateway model of mobile end-to-end data communication between the mobile user and the ASP	4
7	Characteristics of mobile end-to-end data communication	4
8	Security threats to the mobile environment	5
8.1	General security threats	5
8.2	Mobile-oriented security threats.....	6
8.3	Relationship of security threats to end-to-end communication models	7
9	Security requirements for mobile end-to-end data communications	8
9.1	Security requirements from the mobile user's point of view	8
9.2	Security requirements for ASP's point of view	11
9.3	Relationship between security requirements and security threats	14
10	Security functions for satisfying mobile security requirements	15
11	Security technologies for mobile end-to-end data communication	18

ITU-T Recommendation X.1121

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

1 Scope

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

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

This Recommendation does not provide the details of mobile network components except for wireless network access to a mobile terminal when connected to an 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 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.800 (1991), *Security Architecture for Open Systems Interconnection for CCITT applications*.
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

3 Definitions

3.1 OSI Reference Model security architecture definitions

The following terms are defined in ITU-T Rec. X.800:

- 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

This Recommendation defines the following terms:

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

3.2.2 shoulder surfing: A security threat which collects information in busy places by watching keystroke, reading mobile terminal's screen, or listening to sound from a mobile terminal.

3.2.3 mobile terminal: An entity that has wireless network access function and connects a 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.

3.2.7 application server: An entity that connects to an open network for data communication with mobile terminals.

3.2.8 Application Service Provider (ASP): An entity (person or group) which provides application service(s) to mobile users through an application server.

3.2.9 mobile security gateway: An entity which relays data communication between a mobile terminal and an application server, changes security parameters or communication protocol from a mobile network to an open network, or vice versa, and can perform security policy management functions for mobile end-to-end data communication.

3.2.10 security policy management: A function to manage or negotiate a set of rules to provide classified security services which can be implemented on the mobile security gateway or other server.

4 Abbreviations

This Recommendation uses the following abbreviations:

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 data communication capabilities (like IMT-2000 mobile phone, laptop PC or a PDA with a radio-card) have been widely distributed and various application services (e.g., mobile commerce) for mobile terminals are provided through the mobile network. In the e-commerce application, security is necessary and indispensable.

There are many areas under investigation from a mobile operator's point of view (e.g., security architecture on IMT-2000 mobile telephone network). However, it is also important to investigate from the mobile user's point of view and the ASP's point of view.

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

In addition, for the mobile system that connects a mobile network to an 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) or open network.

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

6 Models of mobile end-to-end data communications

Before describing secure mobile technologies, models of mobile end-to-end data communication should be defined. Models of mobile end-to-end data communication 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 the mobile user and the ASP

A general model of mobile end-to-end data communication between a mobile user and an ASP is shown in Figure 1.