

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1123

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Differentiated security service for secure mobile end-to-end data communication

Recommendation ITU-T X.1123

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

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.379
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.889
Generic applications of ASN.1	X.890–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.

Recommendation ITU-T X.1123

Differentiated security service for secure mobile end-to-end data communication

Summary

Recommendation ITU-T X.1123 describes the differentiated security service for secure mobile communication. The investigation of differentiated security service is important for both service providers and users. The service providers can use the differentiated security service to overcome the rigorous circumstances of wireless access networks and satisfy various users and services with different levels of security. The differentiated security service is realized by security policy with three layers. One layer is super security policy used as a value-added service that safeguards mobile communication with sensitive information. The second layer is baseline security policy used as the prevalent service that satisfies mobile communication without sensitive information. The last layer is no security policy, defined as the policy under which no security function is configured during communication.

Source

Recommendation ITU-T X.1123 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

Keywords

Differentiated, security dimension, security level, security policy, security service.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

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	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Network model for differentiated security service	3
7	Differentiated security service	4
7.1	Types of assets in the mobile environment	4
7.2	Framework of differentiated security service.....	5
8	Security policy.....	8
8.1	Framework of security policy.....	9
8.2	Configuration of security policy.....	10
9	Negotiation process	10
9.1	Negotiation process of security policy	11
9.2	Negotiation process between terminal and SGW	12
9.3	Negotiation process between SGWs	13
9.4	Negotiation process between SGW and terminal.....	13
10	Billing of security service.....	13
11	Triggering of security resources	14
	Annex A – Functions of the network model for differentiated security service.....	15
A.1	Functions of the network model	15
A.2	Depiction of functions	15
A.3	Protocols between functions.....	18
	Appendix I – Example of security mechanism in line with subgroup of security policy	19
	Bibliography.....	21

Copyright International Telecommunication Union/ITU Telecommunication Sector

Introduction

It is necessary to establish a differentiated security service in secure mobile communication. The reasons are described as follows:

- *Rigorous mobile environment*

The number of types of services that are provided through mobile networks is increasing quickly. Moreover, the number of mobile users also grows remarkably all around the world. Similar to wired networks, mobile networks are also threatened by various attacks. In addition, the mobile environment has many limitations such as limited computing power in mobile terminals, inadequate memory space and low network bandwidth at the air interface. Therefore, the running of applications is more difficult in mobile networks than that in wired networks. Since the purpose of a security service is to organize various security technologies together to achieve a certain level of security for various applications, a differentiated security service mechanism is necessary for applications in the rigorous mobile environment.

- *Additional investment for security*

Compared with unsecured networks, secure networks require additional investment from the service provider's point of view. Moreover, there is no absolute network security. The investment in security strongly relies on the level of security the network can provide. The additional investment at least includes network management of security, security devices, additional consumption on bandwidth and computing power, training for security managers and users, etc.

When telecommunication networks evolve from circuit switched to packet switched, multimedia communication develops fast. The data volume of multimedia communication is much larger than that of audio communication. Data protection with a unique high security level becomes impossible because of the large, real-time data flow. For example, in second generation mobile networks, such as the GSM network, we can encrypt all the data flow at the air interface since the audio communication has a much smaller data flow compared with multimedia communication. However, in third generation mobile networks, when multimedia communication is popular, we need differentiated security levels to protect data flow and save resources.

Since next generation networks are based on package networks, the open characteristics of package networks will cause many new security threats. The intelligence of mobile terminals also induces various threats from viruses. Thus, simple management is necessary to integrate the essential configuration of security for users.

Evidently, security is a kind of service that needs a large amount of investment. Thus, it is impossible to provide the total security service without any charging. Service providers should find efficient methods to present strong security service as value-added service.

- *Various secure algorithms and protocols in different types of terminals*

A variety of security algorithms and protocols exists in different types of terminals. A rigorous problem is how to organize them to provide not only enough security, but also full interoperability among different types of mobile terminals. The problem cannot be solved without an effective security policy. Since a general mobile network includes various types of terminals, it is necessary to develop a security policy at both the terminal and network ends that can satisfy the security requirements effectively.

- *Different security requirements for various users and applications*

Although secure communication is important in many applications, such as e-commerce, etc., many other applications require just a low level of security, such as accessing the Internet for open information. In this case, the unidirectional authentication from network to user may be enough. Therefore, security requirements vary among different users and

services. Service providers should provide differentiated security services to users. The structure of security policy is necessary to provide the differentiated security. By this means, it is important to study the differentiated security service that is driven by security policy.

- *Simple and effective security services for users*

Security management is of critical importance in network security. For example, a network is totally unsecured without effective security management even though it deploys many advantageous security entities and implements perfect security solutions. A secure network not only requires professional security managers at the network end, but also mobile users who can take charge of security management at the terminal end. If security management fails at either end, communication is unsecure. As we know, it is impossible to require that all users have enough security management ability. Thus, for better services, it is necessary to develop an effective security policy that is as simple as possible at the terminal end, and in which most policy decisions are executed in the network. For some services, all of the security policies may be determined at the (network) server end, such as e-banking services, etc.

Copyright International Telecommunication Union/ITU Telecommunication Sector

Downloaded from https://www.ava.com

Recommendation ITU-T X.1123

Differentiated security service for secure mobile end-to-end data communication

1 Scope

This Recommendation provides a specification of differentiated security services for secure mobile end-to-end data communication, which includes a series of security policies, security levels and negotiation of security levels between security domains.

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 X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.803] Recommendation ITU-T X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 **access control:** [ITU-T X.800].
- 3.1.2 **anonymity:** [ITU-T X.1121].
- 3.1.3 **application server:** [ITU-T X.1121].
- 3.1.4 **application service:** [ITU-T X.1121].
- 3.1.5 **application service provider (ASP):** [ITU-T X.1121].
- 3.1.6 **authentication:** [ITU-T X.800].
- 3.1.7 **authentication exchange:** [ITU-T X.800].
- 3.1.8 **authorization:** [ITU-T X.800].
- 3.1.9 **availability:** [ITU-T X.800].

- 3.1.10 **confidentiality:** [ITU-T X.800].
- 3.1.11 **data integrity:** [ITU-T X.800].
- 3.1.12 **encipherment:** [ITU-T X.800].
- 3.1.13 **identity management:** [ITU-T X.1121].
- 3.1.14 **integrity:** [ITU-T X.800].
- 3.1.15 **key:** [ITU-T X.800].
- 3.1.16 **mobile network:** [ITU-T X.1121].
- 3.1.17 **mobile terminal:** [ITU-T X.1121].
- 3.1.18 **mobile user:** [ITU-T X.1121].
- 3.1.19 **non-repudiation:** [ITU-T X.800].
- 3.1.20 **password:** [ITU-T X.800].
- 3.1.21 **privacy:** [ITU-T X.800].
- 3.1.22 **security dimension:** [ITU-T X.805].
- 3.1.23 **security policy:** [ITU-T X.800].
- 3.1.24 **usability:** [ITU-T X.1121].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security level: Security level is the application of a network system to process information with different sensitivities and to permit simultaneous access by users with different security clearances and needs-to-know.

3.2.2 security policy server: A security policy server is an entity that connects to a security gateway. It manages security policy and uses the security policy to control the negotiation of security levels among network security domains.

3.2.3 service provider: A service provider is a business that provides service to customers over a network; it includes not only network service providers but also application service providers.

3.2.4 assets: Assets are valuable properties to be protected by the mobile terminal or service provider. Assets are divided into three kinds: information, service, and system assets.

3.2.5 security manager: A security manager is a person or entity that determines the security service level, manages the configuration of security policy, and performs security policy-related tasks at the mobile terminal or service provider.

3.2.6 security service: A security service is a service provided by the service provider to ensure adequate security of the systems or of data transfers. It includes not only eight security dimensions, but also online virus scanning and content filtering.

3.2.7 differentiated security service: A differentiated security service is a security service with a security policy that classifies different security levels.

3.2.8 security gateway: A security gateway is an entity which relays data traffic between security domains, configures security parameters or communication protocols and can perform a security policy management function.

3.2.9 user security agent: A user security agent is an entity embedded in mobile terminals to collect the security-related environmental information and to communicate with the security gateway in the mobile network for the execution of the security policy.