

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1162

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Security architecture and operations for peer-to-peer networks

Recommendation ITU-T X.1162



International
Telecommunication
Union

Documents
Document Sharing Hub

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.1162

Security architecture and operations for peer-to-peer networks

Summary

Recommendation ITU-T X.1162 describes a general security-related architectural model which can be applied in various peer-to-peer (P2P) networks. Based on the architectural model, this Recommendation identifies primitive operations for generic P2P networks. Non-generic and application-dependent operations are not described in this Recommendation. For each primitive operation, the relationship between the security requirements and operations is described. In addition, the relationship between the security functions and operations is described.

Source

Recommendation ITU-T X.1162 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 procedure.

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 2008

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	2
5	Conventions	3
6	Conceptual architecture of overlay network.....	3
7	Security architecture of the peer-to-peer network	4
7.1	Peer-to-peer architectural reference model	4
7.2	Relationship between the P2P overlay stratum and transportation stratum ...	5
8	Primitive operations of the peer-to-peer network.....	6
8.1	Join	6
8.2	Leave	6
8.3	Search	6
8.4	Chat.....	6
8.5	Routing	6
8.6	Insertion and Retrieval	7
8.7	Update and Delete	7
8.8	Multicasting.....	7
8.9	Relationship between security requirements and operations.....	7
8.10	Relationship between security functions and operations.....	12
Annex A	Structures of peer-to-peer networks	13
A.1	Centralized peer-to-peer networks	13
A.2	Pure (distributed) peer-to-peer networks.....	14
A.3	Hybrid peer-to-peer networks.....	14
A.4	DHT (distributed hash table)-based peer-to-peer networks [b-ES05].....	14
Bibliography		15

Document Sharing Hub



Documents

Document Sharing Hub

Rec. ITU-T X.1162 (05/2008)

iii

Recommendation ITU-T X.1162

Security architecture and operations for peer-to-peer networks

1 Scope

This Recommendation describes a general and common security-related architectural model and operations that can be applied to various peer-to-peer (P2P) networks, and only covers the generic security issues that are common to most P2P networks. The security issues are described on the basis of the operations. The complete set of security requirements is defined in [ITU-T X.1161]. According to the requirements, the peer-to-peer architectural reference model and primitive operations are proposed. For each primitive operation, the relations among the security requirements, security functions, and operations are described for the development guidelines.

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.1161] Recommendation ITU-T X.1161 (2008), *Framework for secure peer-to-peer communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [b-ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ITU-T X.800]: See data origin authentication defined in clause 3.1.8, and peer entity authentication defined in clause 3.1.12.

3.1.3 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

3.1.7 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.9 integrity [b-ITU-T X.800]: See data integrity.

3.1.10 key [b-ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.11 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

3.1.12 peer entity authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.13 privacy [b-ITU-T X.800]: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.14 peer [ITU-T X.1161]: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

3.1.15 repudiation [b-ITU-T X.800]: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 overlay network: An overlay network is a virtual network that runs on top of another network. Like any other network, the overlay network comprises a set of nodes and links between them. Because the links are logical ones, they may correspond to many physical links of the underlying network.

3.2.2 peer user: A peer user is one who uses a computer system to access the P2P network. A peer user in a P2P network is similar to a user in the Internet, with slight differences. Specifically, peer users in the P2P network have a different operational context including personal interests, resource plans, security considerations, etc.

3.2.3 security domain administrator: A security domain administrator is a party with the authority to manage a specific P2P network. An administrative body may have a security policy and the appropriate enforcement mechanism to ensure the security of the P2P network under its management. Such policy and enforcement mechanism are completely application-dependent.

3.2.4 super-peer: A super-peer is a node in a P2P network to help routing and connectivity of nodes distributed in the Internet. The super-peer is less powerful than ordinary servers, but it is strong enough (in terms of, for example, computing power and storage) to act as a server of route resolution and connection request.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DHT	Distributed Hash Table
DoS	Denial of Service
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
ID	Identifier
P2P	Peer-to-Peer
QoS	Quality of Service