

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.1163

(05/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Peer-to-peer security

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

Recommendation ITU-T X.1163

ITU-T

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

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1163

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

Summary

Because of the obvious merits of peer-to-peer (P2P) networks (such as lower cost, scalability and fault tolerance), some operators began to consider the possibility of constructing the next-generation kernel network based on P2P. In order to implement an operable and manageable P2P-based telecommunication network, the security solution must be a critical part of it.

The distributed service network (DSN) defined in Recommendations ITU-T Y.2206 and ITU-T Y.2080 is designed as a telecommunication network based on P2P. The capability requirements and the functional architecture are defined in Recommendations ITU-T Y.2206 and ITU-T Y.2080, respectively; however, the security aspects are not addressed in either of these two Recommendations. The security requirements and mechanisms defined in Recommendation ITU-T X.1163 complement the DSN-related work.

Recommendation ITU-T X.1163 provides a security guideline for a telecommunication network based on P2P technology. It briefly introduces the characteristics of the network, it also analyses the security requirements of the network and the services, and it specifies the security mechanisms to fulfil these requirements.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1163	2015-05-29	17	11.1002/1000/12476

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 2015

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

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	1
5	Conventions	3
6	Architecture of telecommunication network based on P2P.....	3
7	Security requirements analysis	4
	7.1 Authentication and authorization	5
	7.2 Trust management	5
	7.3 Confidentiality	5
	7.4 Integrity	5
	7.5 Digital rights management	5
8	Security mechanisms	6
	8.1 Authentication and authorization mechanism	6
	8.2 Trust management mechanism	8
	8.3 Confidentiality and integrity mechanisms	10
	8.4 Digital rights management mechanism in streaming services	12
	Appendix I – Relationship of Recommendation ITU-T X.1163 and DSN-related Recommendations.....	14
	I.1 Comparison between this Recommendation and [b-ITU-T Y.2206] and [ITU-T Y.2080]	14
	I.2 Mapping with DSN functional architecture in [ITU-T Y.2080]	14
	Bibliography.....	17

Downloaded from <https://www.itu.int/ITU-T/standards/itu-t-x-1163-2015>

Recommendation ITU-T X.1163

Security requirements and mechanisms of peer-to-peer-based telecommunication networks

1 Scope

This Recommendation provides a security guideline for a telecommunication network based on peer-to-peer (P2P) technology, including the network characteristics, the security requirements of the network and the services, as well as security mechanisms to fulfil these requirements.

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 Y.2080] Recommendation ITU-T Y.2080 (2012), *Functional architecture for distributed service networking*.

[3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2006), *3G Security; Security architecture*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 ContentID: An identity number which is the same in different content fragments to identify the fragments of the same content file.

3.2.2 copyright problem: Legal issue resulting from spreading copies without the permission and authorization of the owner.

3.2.3 privacy problem: Attackers steal private information without the permission of or authorization by the owner.

3.2.4 KeyID: An identity number to identify a key in the security algorithms.

3.2.5 KeySeed: A random number based on a key which will be produced in the security algorithms.

3.2.6 trust: The relationship between two entities where each one is certain that the other will behave exactly as it expects.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AF Application Function

Document Sharing Hub

AKA	Authentication and Key Agreement
AUTN	Authentication Token
AV	Authentication Vector
CDF	Content Delivery Function
CK	Confidentiality Key
C/S	Client/Server
CS	Content Server
CSAF	Content Service Application Function
DHT	Distributed Hash Table
DoS	Denial of Service
DRM	Digital Rights Management
DSN	Distributed Service Network
EF	End-user Function
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
ICT	Information and Communication Technology
ID	Identity
IK	Integrity Key
IP	Internet Protocol
MF	Management Function
NAT	Network Address Translation
NEF	Node Enrolment Function
NGN	Next-Generation Network
P2P	Peer-to-Peer
PC	Personal Computer
QoS	Quality of Service
RAND	Random number (used for authentication)
RES	Response
RF	Relay Function
RLF	Resource Location Function
SCF	Service Control Function
SP	Streaming Packer
SS	Streaming Server
TOCF	Traffic Optimization Control Function
UE	User Equipment
USIM	Universal Subscriber Identity Module