

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1156

(06/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Non-repudiation framework based on a one-time password

Recommendation ITU-T X.1156



International
Telecommunication
Union

Documents
Document Sharing Hub

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
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

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

Recommendation ITU-T X.1156

Non-repudiation framework based on a one-time password

Summary

Recommendation ITU-T X.1156 provides a non-repudiation framework based on a one-time password (OTP) to enhance trust between transaction entities. In addition, this Recommendation describes the security requirements of OTP-based non-repudiation services, as well as the mechanisms for generating non-repudiation tokens. The originator of the transactions may request the trusted third party (TTP) to generate the non-repudiation token and the recipient may request the TTP to generate the non-repudiation of delivery token. Both the originator and the recipient may request TTP to verify the non-repudiation tokens.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1156	2013-06-13	17

Keywords

Non-repudiation framework, one-time password, trusted third party.

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 2013

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.....	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Overview of non-repudiation framework based on a one-time password.....	3
	6.1 Introduction	3
	6.2 Entities and keys.....	3
	6.3 Secure envelope.....	4
7	Security requirements for an OTP-based non-repudiation service.....	5
8	Non-repudiation tokens	6
	8.1 OTP-based non-repudiation of origin token (NROT)	6
	8.2 OTP-based non-repudiation of delivery token (NRDT).....	6
9	Non-repudiation processes	7
	9.1 Process of OTP-based non-repudiation of origin (NRO)	7
	9.2 Process of OTP-based non-repudiation of delivery (NRD)	8
10	Non-repudiation service models	9
	10.1 Overview of the communication models.....	9
	10.2 Service model for indirect NROT and indirect NRDT	10
	10.3 Service model for indirect NROT and direct NRDT.....	12
	10.4 Service model for direct NROT and indirect NRDT.....	13
	10.5 Service model for direct NROT and direct NRDT.....	14
	Bibliography.....	16

Recommendation ITU-T X.1156

Non-repudiation framework based on a one-time password

1 Scope

Recommendation ITU-T X.1156 provides a non-repudiation framework based on a one-time password (OTP) to provide trust mechanisms between transaction entities. Also, this Recommendation describes the security requirements of a one-time password based on a non-repudiation service, as well as the mechanisms for generating non-repudiation tokens.

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.813] Recommendation ITU-T X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[ITU-T X.1153] Recommendation ITU-T X.1153 (2011), *Management framework of a one time password-based authentication service*.

[ISO/IEC 13888-2] ISO/IEC 13888-2:2010, *Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication framework [ITU-T X.1153]: A general framework for the provision of authentication service; two party and (trusted) third party authentication frameworks (based on [b-ITU-T X.811]).

3.1.2 one-time password (OTP) [ITU-T X.1153]: A password that can be used only once as it is changed every time an OTP user logs into the computer system and network. It is secure against the passive attacks allowed by the replaying of captured reusable passwords such as traditional fixed passwords (based on [b-IETF RFC 2289]).

3.1.3 OTP service provider [ITU-T X.1153]: The provider(s) of the OTP validation service offering multi-factor authentication services to other service providers, e.g., Internet service provider or application/contents service provider. A trusted third party would be a good example for an OTP service provider to perform OTP validation more efficiently. The OTP service provider does not necessarily have the role of identity provider as defined in [b-ITU-T X.1141].

3.1.4 OTP token [ITU-T X.1153]: A physical device that generates an OTP, wherein a token means that the OTP user possesses and controls a key or password used to authenticate the OTP user's identity. Such a physical device embeds the display showing an OTP and the numeric keypad optionally.

3.1.5 OTP token identifier [ITU-T X.1153]: A unique identifier assigned to each OTP token for distinguishing it from other OTP tokens. It may consist of alphanumeric characters.

3.1.6 trusted third party [b-ITU-T X.810]: A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy).

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 non-repudiation token: This token is the unforgeable evidence for the non-repudiation service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

HMAC	Hash-based Message Authentication Code
MAC	Message Authentication Code
NRD	Non-Repudiation of Delivery
NRDT	Non-Repudiation of Delivery Token
NRO	Non-Repudiation of Origin
NROT	Non-Repudiation of Origin Token
NRT	Non-Repudiation Token
OSP	OTP Service Provider
OTP	One-Time Password
PON	Positive Or Negative
SENV	Secure Envelope
SEVM	Secure Envelope using MAC
SEVO	Secure Envelope using OTP
TSA	Time Stamping Authority
TTP	Trusted Third Party

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.