

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1159

(11/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Delegated non-repudiation architecture based on ITU-T X.813

Recommendation ITU-T X.1159

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
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.1159

Delegated non-repudiation architecture based on ITU-T X.813

Summary

Non-repudiation is the ability to prevent entities from denying that they have sent or received electronic transaction data in a telecommunication network. Recommendation ITU-T X.1159 provides a delegated non-repudiation architecture based on Recommendation ITU-T X.813 to generate non-repudiation evidence by a trusted third party (TTP) instead of a user.

Recommendation ITU-T X.813 defines six non-repudiation mechanisms: a TTP security token, security tokens and tamper-resistant modules, a digital signature, time stamping, an in-line TTP and a notary. This Recommendation complies with these six mechanisms, and the non-repudiation service can use a combination of these mechanisms to satisfy the security requirements of the application service.

In this Recommendation, a right and/or user's signing key for a non-repudiation generation delegates to a TTP, which is a central signing authority, and the central signing authority generates and verifies non-repudiation evidence using the delegated user's signing/validation key or the central signing authority's secret key/validation key. The delegated non-repudiation model in this Recommendation is capable of responding to key loss and theft, is safe in an open network, such as a mobile and cloud network, and provides convenient non-repudiation service.

This Recommendation describes the delegated non-repudiation service models and operations for each of the service models. The architecture also defines the security requirements of the delegated non-repudiation service. In this delegated non-repudiation service model, there are two types of service models that use the central signing authority's secret key and the delegated signing key.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1159	2014-11-13	17	11.1002/1000/12342

Keywords

Central signing authority, delegated non-repudiation service, non-repudiation architecture.

* 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.....	2
4	Abbreviations and acronyms	2
5	Conventions	2
6	Delegated non-repudiation architecture.....	3
	6.1 Introduction	3
	6.2 Entities.....	4
	6.3 Operations of the delegated non-repudiation service	5
7	Requirements for a delegated non-repudiation service	7
	7.1 Unforgeability.....	7
	7.2 Prevention of misuse	7
	7.3 Verifiability	7
	7.4 Identifiability	7
8	Delegated non-repudiation service models.....	7
	8.1 Delegated non-repudiation service model using a central signing authority's secret key	7
	8.2 Delegated non-repudiation service model using delegated signing key	10
	8.3 Security considerations for delegated non-repudiation service models	13
	Bibliography.....	15

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T X.1159

Delegated non-repudiation architecture based on ITU-T X.813

1 Scope

This Recommendation provides an enhanced non-repudiation model based on [ITU-T X.813] in support of application services. The user can authenticate and generate non-repudiation evidence for the transaction of data by a trusted third party (TTP), which is the central signing authority. The recommended architecture provides an integration of the authentication token to access the central signing authority. The architecture also integrates multiple service providers to provide a non-repudiation service for a single authenticated device. The model will provide non-repudiation services for any type of device including the mobile device. Although this architecture requires the use of strong authentication, this is out of the scope of this Recommendation. Furthermore, issuing and managing a signing key are out of the scope of this Recommendation.

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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication token [b-ITU-T X.509]: Information conveyed during a strong authentication exchange, which can be used to authenticate its sender.

3.1.2 evidence [ITU-T X.813]: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.1.3 evidence subject [ITU-T X.813]: The entity whose involvement in an event or action is established by evidence.

3.1.4 evidence verifier [ITU-T X.813]: An entity that verifies non-repudiation evidence.

3.1.5 in-line TTP [b-ITU-T X.842]: A TTP positioned directly in the communication path between the entities that can facilitate secure exchanges between these entities.

3.1.6 non-repudiation token [b-ITU-T X.1156]: This token is the unforgeable evidence for the non-repudiation service.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 authentication service provider: The entity is a trusted third party (TTP) that issues the authentication device and/or user's signing key and verifies the transaction-based authentication information.

3.2.2 central signing authority: The entity is a trusted third party (TTP) that stores and manages the user's delegated signing key and generates the non-repudiation evidence on behalf of the user.

3.2.3 delegated signing key: The signing key that is used in generating non-repudiation evidence by a trusted third party (TTP).

3.2.4 delegation information: The information that is derived by the user's signing key for a delegated non-repudiation service.

3.2.5 delegation warrant: The information that assumes that the user gave the central signing authority the authority to generate a non-repudiation evidence.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP	Authentication Service Provider
DB	DataBase
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
NRD	Non-Repudiation of Delivery
NRE	Non-Repudiation Evidence
NRO	Non-Repudiation of Origin
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKI	Public Key Infrastructure
RET	REsult
SM	Service Model
SP	Service Provider
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 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.