

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1404

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Distributed ledger
technology security

Security assurance for distributed ledger technology

Recommendation ITU-T X.1404



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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1404

Security assurance for distributed ledger technology

Summary

Recommendation ITU-T X.1404 defines three levels of security assurance for the distributed ledger technology (DLT) in order to facilitate design and development of security assurance mechanisms. It further defines ten security assurance components encompassing the security assurance and specifies criteria and guidelines for achieving each of the three levels of a security assurance component. Finally, it also provides a mapping between specific threats and security assurance components and a mapping between specific security capabilities and security assurance components.

Distributed ledger technology (DLT) is defined as a shared digital ledger, which is a continually updated list of all transactions. The assurance of DLT is defined as the degree of confidence that the process or deliverable meets defined characteristics or objectives. An assurance level could be considered as a quantitative expression of assurance agreed among the relevant parties.

There is a need for specifying criteria and guidelines for achieving each of the three levels of a security assurance component: data integrity, data confidentiality, credential management, identity proofing of users, entity authentication, authorization, data obfuscation, consensus mechanism strength, smart contract and personally identifiable information (PII) data protection. To facilitate the design and development of security assurance mechanisms, this Recommendation is based on three levels of security assurance.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1404	2020-10-29	17	11.1002/1000/14450

Keywords

Consensus mechanism, distributed ledger technology, integrity, proof of work, security assurance.

* 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 2021

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.....	3
4 Abbreviations and acronyms	3
5 Conventions	4
6 Overview of security assurance for DLT.....	4
6.1 Level of security assurance	4
6.2 Selecting the appropriate level of security assurance.....	5
7 DLT actors.....	5
8 Security assurance for DLT	6
8.1 Data integrity	6
8.2 Data confidentiality	7
8.3 Credential management	8
8.4 Identity proofing of user	9
8.5 Entity authentication.....	9
8.6 Access control	10
8.7 Data obfuscation.....	10
8.8 Consensus mechanism.....	11
8.9 Smart contract.....	12
8.10 Personally identifiable information (PII) data protections	13
9 Threats and capabilities related to DLT security assurance	14
Annex A – Mapping between threat items and security assurance components	15
Bibliography.....	17

Recommendation ITU-T X.1404

Security assurance for distributed ledger technology

1 Scope

This Recommendation defines three levels of security assurance for the distributed ledger technology (DLT). It further defines ten security assurance components encompassing security assurance and specifies criteria and guidelines for achieving each of the three levels of a security assurance component. Finally, it also provides a mapping between specific threats and security assurance components and a mapping between specific security capabilities and security assurance components.

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.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

[ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

[ISO/IEC 27034-3] ISO/IEC 27034-3:2018, *Information technology – Application security – Part 3: Application security management process*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 block [b-ITU-T X.1400]: Individual data unit of a blockchain (see clause 3.1.2), composed of a collection of transactions and a block header.

3.1.2 blockchain [b-ITU-T X.1400]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.3 Byzantine fault tolerance [b-ITU-T X.1400]: Property that enables a system to continue operating properly even if some of its components fail or existence of intentional bad actors.

3.1.4 consensus [b-ITU-T X.1400]: Agreement that a set of transactions is valid.

3.1.5 consensus mechanism [b-ITU-T X.1400]: Rules and procedures by which consensus is reached.

3.1.6 control [b-ISO/IEC 27000]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.7 credentials [b-ITU-T X.1311]: Set of security-related information consisting of keys, keying materials, and cryptographic algorithm-related parameters permitting successful interaction with a security system.

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

3.1.9 distributed ledger [b-ITU-T X.1400]: A type of ledger, that is shared, replicated, and synchronized in a distributed manner.

3.1.10 distributed ledger technology [b-ISO 22739]: Technology that enables the operation and use of distributed ledgers.

NOTE – This is the technology underlying Bitcoin and other crypto currencies.

3.1.11 hardware security module [b-ISO 13491-1]: Secure cryptographic device that provides a set of secure cryptographic services, e.g., key generation, cryptogram creation, PIN translation, and certificate signing.

3.1.12 hash function [b-NISTIR 8202]: A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. One-way: It is computationally infeasible to find any input that maps to any pre-specified output, and
2. Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output

3.1.13 identity proofing [b-ISO/IEC 24760-1]: Verification based on identity evidence aimed at achieving a specific level of assurance.

NOTE 1 – Identity proofing is typically performed as part of enrolment. Identity evidence can also be needed during maintenance of registered identity information, e.g., recovery of a user account.

NOTE 2 – Typically, identity proofing involves a verification of provided identity information and can include uniqueness checks, possibly based on biometric techniques.

NOTE 3 – Verification for identity proofing is usually based on an enrolment policy that includes specification of the verification criteria of the identity evidence to be provided by the entity.

NOTE 4 – The verified identity information obtained when performing identity proofing can be included in the registration and can serve to facilitate future identification of the entity.

3.1.14 node [b-ITU-T X.1400]: Device or process that participates in a distributed ledger network.

NOTE – A node can store a complete or partial replica of the distributed ledger.

3.1.15 off-chain [b-ISO/TC 307]: Related to a blockchain system, but located, performed or run outside that blockchain system.

3.1.16 on-chain [b-ISO/TC 307]: Located, performed or run inside a blockchain system

3.1.17 personally identifiable information (PII) [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE –To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.18 proof of stake [b-ITU-T X.1400]: Consensus process, where an existing stake in the distributed ledger system (e.g., the amount of that currency that you hold) is used to reach consensus.

3.1.19 proof of work [b-ITU-T X.1400]: Consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to correctly verify.