

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1352

(09/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things
(IoT) security

Security requirements for Internet of things devices and gateways

Recommendation ITU-T X.1352

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 (1)	X.1140–X.1149
Application Security (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.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
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
Cyber Defence	X.1590–X.1599
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
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1352

Security requirements for Internet of things devices and gateways

Summary

Recommendation ITU-T X.1352 establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security, based on the IoT reference model specified in Recommendation ITU-T Y.4100 and the IoT security framework in Recommendation ITU-T X.1361.

The authentication dimension includes user authentication, secure use of authentication credentials and device authentication. The cryptography dimension includes the use of secure cryptography, secure key management and secure random number generation. The data security dimension includes secure transmission and storage, information flow control, secure session management and personally identifiable information (PII) management. The device platform security dimension includes five elements: software security; secure update; security management; logging; and timestamp. Likewise, the physical security dimension includes a secure physical interface and tamper-proofing.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1352	2022-09-02	17	11.1002/1000/14990

Keywords

Authentication, cryptography, data security, device platform security, IoT device and gateway security, IoT gateway, IoT security evaluation, physical security.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2022

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	3
6	Overview	4
7	Security threats/vulnerabilities to IoT devices and gateways.....	5
	7.1 Security threats/vulnerabilities to IoT devices	5
	7.2 Security threats/vulnerabilities to IoT gateways	6
8	Security requirements	7
	8.1 Authentication	7
	8.2 Cryptography	8
	8.3 Data security	9
	8.4 Device platform security	9
	8.5 Physical security	11
	Annex A Mapping list between Internet of things security requirements and security threats/vulnerabilities.....	12
	Appendix I – Security capabilities for the Internet of things.....	15
	I.1 Overview	15
	I.2 Security capabilities for sensor/device	16
	I.3 Security capabilities for gateways	17
	I.4 Security capabilities for network.....	18
	I.5 Security capabilities for platforms/service	18
	Appendix II – Use cases of applying security requirements for Internet of things devices and gateways.....	20
	II.1 Use case of authentication – Vulnerability to man in the middle attack	20
	II.2 Use case of cryptography domain – Weak cryptography algorithm	20
	II.3 Use case of data security and cryptography domain – Weak integrity checking of sending data	21
	II.4 Use case of device platform security domain – Weak coding against exploit	21
	II.5 Use case of physical security domain – Inner interface vulnerability in a printed circuit board	22
	Bibliography.....	23

Recommendation ITU-T X.1352

Security requirements for Internet of things devices and gateways

1 Scope

This Recommendation establishes detailed requirements for five security dimensions applicable to Internet of things (IoT) device and gateway: authentication; cryptography; data security; device platform security; and physical security. These security requirements are based on the IoT reference model specified in [ITU-T Y.4100] and on the IoT security framework specified in [ITU-T X.1361].

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.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.
- [ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 authentication** [b-ITU-T X.1254]: Provision of assurance of the claimed identity of an entity.
- 3.1.2 capability** [b-ISO 16100-1]: Set of functions and services with a set of criteria for evaluating the performance of a capability provider.
- 3.1.3 confidentiality** [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- 3.1.4 credential** [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.
- 3.1.5 cryptographic-quality random number** [b-ITU-T X.667]: A random number or pseudo-random number generated by a mechanism, which ensures sufficient spread of repeatedly generated values to be acceptable for use in cryptographic work (and is used in such work).
- 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 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

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

3.1.10 patch management [ITU-T X.1361]: Process which encompassing acquiring, testing, and installing multiple patches to information systems.

NOTE – Vulnerability management capability could be considered.

3.1.11 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.

3.1.12 physical security [b-ITU-T X.800]: The measures used to provide physical protection of resources against deliberate and accidental threats.

3.1.13 secure configuration [ITU-T X.1361]: Process by which network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

3.1.14 security gateway [ITU-T X.1361]: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy in the IoT environment.

NOTE – The term is sometimes referred to a gateway. The definition is adapted from [b-ISO/IEC 27033-1].

3.1.15 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which can result in harm to a system or organization.

3.1.16 vulnerability [b-ISO/IEC 27000]: Weakness of an asset or control that can be exploited by one or more threats.

3.1.17 vulnerability management [ITU-T X.1361]: Process that consists of identifying, classifying, remediating, and mitigating vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security dimension: A set of security measures designed to address a particular aspect of security.

3.2.2 device platform security: A security set for firmware and its updated capability and management of third party software together with audit capability on an Internet of things device and gateway.

NOTE – Firmware is replaced by software on an operating system depending on the hardware capability.

3.2.3 obfuscation: Effect of an operation performed on the program code or application data that results in the applications being hidden or obscured in some way without affecting the output of the code.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CoAP	Constrained Application Protocol

DoS	Denial of Service
F/W	Firmware
FTP	File Transfer Protocol
H/W	Hardware
ID	Identifier
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IPS	Intrusion Prevention System
LwM2M	Lightweight Machine to Machine
MAC	Media Access Control
MCU	Microcontroller Unit
MQTT	Message Queuing Telemetry Transport
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
S/W	Software
SD	Secure Digital
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSA	Shoulder-Surfing Attack
SWD	Serial Wire Debug
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver/Transmitter
UID	Unique Identifier
UPnP	Universal Plug and Play
USB	Universal Serial Bus

5 Conventions

This Recommendation uses the following conventions:

The auxiliary verb "should" indicates a requirement that is recommended, but which is not absolutely required.

The auxiliary verb "shall" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformity to this Recommendation is to be claimed.

In the body of this Recommendation, the auxiliary verb "can" sometimes appears, in which case it is to be interpreted as "is able to".

The appearance of the auxiliary verb "should" in Appendix I has no normative intent.

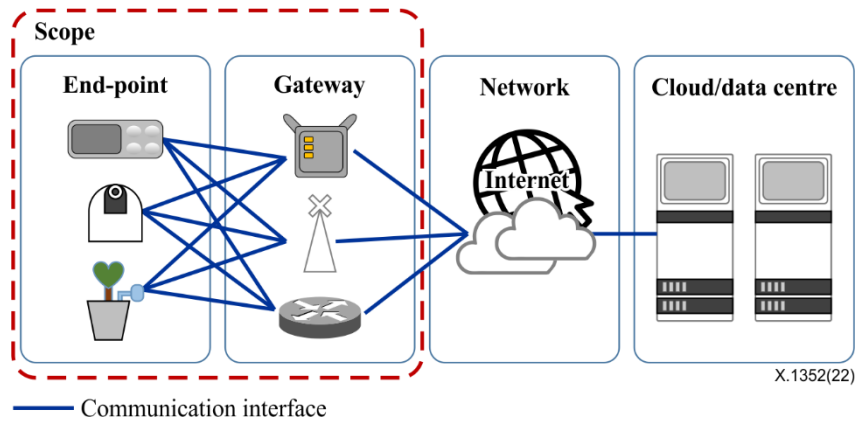


Figure 1 – Scope of security requirements

Based on the security capabilities proposed in [ITU-T X.1361] and [ITU-T Y.4100], and as discussed in Appendix II, security requirements to address the challenges and threats of IoT devices and gateways (excluding network systems and platforms) are specified for five security dimensions, namely: authentication; cryptography; data security; device platform security; and physical security.

The authentication dimension consists of user authentication, secure use of authentication credentials and device authentication.

The cryptography dimension includes the use of a secure cryptographic algorithms, secure key management, and secure random number generation.

The data security dimension is composed of transmission data protection and data protection in rest, information flow control, secure session management and PII protection.

For the device platform security dimension, there are five items: software (S/W) security; secure update; security management; logging; and timestamp.

Likewise, for the physical security dimension, a secure physical interface and defence against tampering have been specified.

Figure 2 shows the targets for security dimensions in an IoT device and gateway. An IoT device and gateway are commonly composed of a microcontroller unit (MCU), communication module, memory and in/out ports. A secure element exists as a form of hardware (H/W) or S/W. In an MCU, there are firmware (F/W), physical interfaces and memory. Here, S/W with an operating system (OS) can be replaced by F/W. The communication module requires cryptography for data security on transmission. Data in flash memories is stored securely for authentication, cryptography and data confidentiality/integrity. Access through physical interfaces like a universal asynchronous receiver/transmitter (UART) also demands user authentication. Unused H/W interfaces shall be removed or switched off.