

ISO/IEC ~~DIS~~**FDIS** 27403:2023(E)

ISO/IEC JTC-1/SC-27/WG-4

Date: 2023-12-12

Secretariat: ~~ILNAS~~ DIN

Date: 2024-03-12

Style Definition

Formatted: zzCover large

Formatted: Left: 1.5 cm, Right: 1.5 cm, Top: 1.4 cm, Bottom: 1 cm, Width: 21 cm, Height: 29.7 cm, Header distance from edge: 1.27 cm, Footer distance from edge: 1.27 cm

Formatted

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

Formatted: Cover Title_A1

iTeh Standards
(<https://standards.itih.ai>)

FDIS stage Preview

ISO/IEC FDIS 27403

<https://standards.itih.ai/catalog/standards/iso/16d945b9-a01f-4cc5-b6cf-af79df304647/iso-iec-fdis-27403>

~~Edited DIS –~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

Formatted: HeaderCentered

© ISO/IEC 20232024

Formatted: Default Paragraph Font

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ~~ISO's~~ISO's member body in the country of the requester.

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

Formatted: French (Switzerland)

Formatted: zzCopyright address, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

E-mail: copyright@iso.org

Formatted: French (Switzerland)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Web www.iso.org

Website: www.iso.org

Published in Switzerland.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27403

<https://standards.iteh.ai/catalog/standards/iso/16d945b9-a01f-4cc5-b6cf-af79df304647/iso-iec-fdis-27403>

~~Edited DIS -~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

© ISO/IEC 2023 – All rights reserved

© ISO/IEC 2024 – All rights reserved

Formatted: FooterPageRomanNumber

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27403

<https://standards.iteh.ai/catalog/standards/iso/16d945b9-a01f-4cc5-b6cf-af79df304647/iso-iec-fdis-27403>

ContentsPage

Foreword x

Introduction..... xi

1 Scope..... 1

2 Normative references..... 1

3 Terms and definitions 1

4 Abbreviated terms..... 2

5 Overview..... 2

5.1 General 2

5.2 Features 3

5.3 Stakeholders 4

5.4 Life cycles 5

5.5 Reference model..... 7

5.6 Security and privacy dimensions 10

6 Guidelines for risk assessment..... 11

6.1 General 11

6.2 Sources of security risks 12

6.2.1 Security risks for service sub-systems..... 12

6.2.2 Security risks for IoT-domotics gateway 13

6.2.3 Security risks for IoT-domotics devices and physical entities..... 15

6.2.4 Security risks for networks..... 16

6.3 Sources of privacy risks..... 17

6.3.1 Privacy risks for service sub-systems 17

6.3.2 Privacy risks for IoT-domotics gateway..... 18

6.3.3 Privacy risks for IoT-domotics devices and physical entities..... 19

6.3.4 Privacy risks for networks 20

7 Security and privacy controls 21

7.1 Principles..... 21

7.1.1 General..... 21

7.1.2 Different levels of security for different services 21

7.1.3 Easy security settings for users..... 21

7.1.4 Failsafe domotics devices..... 21

7.1.5 Restricted access to content services..... 21

7.1.6 Consideration for children..... 21

7.1.7 Scenario-specific privacy preferences..... 21

7.2 Security controls..... 22

7.2.1	Policy for IoT-domotics security	22
7.2.2	Organization of IoT-domotics security	22
7.2.3	Asset management	22
7.2.4	Equipment and assets located outside physical secured areas	22
7.2.5	Secure disposal or re-use of equipment	23
7.2.6	Learning from security incidents	23
7.2.7	Secure IoT-domotics system engineering principles	23
7.2.8	Secure development environment and procedures	23
7.2.9	Security of IoT-domotics systems in support of safety	24
7.2.10	Security in connecting varied IoT-domotics devices	24
7.2.11	Verification of IoT-domotics devices and systems design	24
7.2.12	Monitoring and logging	24
7.2.13	Protection of logs	25
7.2.14	Use of suitable networks for the IoT-domotics systems	25
7.2.15	Secure settings and configurations in delivery of IoT-domotics devices and services	25
7.2.16	User and device authentication	25
7.2.17	Provision of software and firmware updates	25
7.2.18	Sharing vulnerability information	26
7.2.19	Security measures adapted to the life cycle of IoT-domotics system and services	26
7.2.20	Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services	26
7.2.21	Determination of security roles for stakeholders	26
7.2.22	Management of vulnerable devices	27
7.2.23	Management of supplier relationships in IoT-domotics security	27
7.2.24	Secure disclosure of Information regarding security of IoT-domotics devices	27
7.3	Privacy controls	27
7.3.1	Prevention of privacy invasive events	27
7.3.2	IoT-domotics privacy by default	27
7.3.3	Provision of privacy notice	27
7.3.4	Verification of IoT-domotics functionality	28
7.3.5	Consideration of IoT-domotics users	28
7.3.6	Management of IoT-domotics privacy controls	28
7.3.7	Unique device identity	28
7.3.8	Fail-safe authentication	29
7.3.9	Minimization of indirect data collection	29
7.3.10	Communication of privacy preferences	29
7.3.11	Verification of automated decision	29
7.3.12	Accountability for stakeholders	29

7.3.13 Unlinkability of PII..... 30

7.3.14 Sharing information on PII protection measures of IoT-domotics devices..... 30

Annex A (informative) Use cases of IoT-domotics 31

A.1 Use case 1: entertainment..... 31

A.2 Use case 2: electrical appliance control..... 32

A.3 Use case 3: monitoring and security system 33

A.4 Use case 4: care service..... 34

A.5 Use case 5: energy management..... 35

A.6 Use case 6: car video communication..... 36

Annex B (informative) Security and privacy concerns from stakeholders..... 38

B.1 Security concerns..... 38

B.1.1 General..... 38

B.1.2 Security concerns from IoT-domotics service provider..... 38

B.1.3 Security concerns from IoT-domotics service developer..... 39

B.1.4 Security concerns from IoT-domotics user..... 40

B.2 Privacy concerns..... 40

B.2.1 General..... 40

B.2.2 Privacy concerns from IoT-domotics service provider..... 41

B.2.3 Privacy concerns from IoT-domotics service developer..... 41

B.2.4 Privacy concerns from IoT-domotics user..... 42

Annex C (informative) Security and privacy responsibilities of stakeholders..... 43

C.1 Responsibilities of IoT-domotics service provider..... 43

C.2 Responsibilities of IoT-domotics service developer..... 43

C.3 Responsibilities of IoT-domotics user..... 44

Annex D (informative) Security measures for different types of IoT-domotics devices..... 45

D.1 General..... 45

D.2 Class I..... 45

D.3 Class II..... 45

D.4 Class III..... 46

D.5 Class IV..... 46

Bibliography..... 47

FOREWORD..... vi

INTRODUCTION..... vi

1 Scope..... 1

2 Normative references..... 1

3 Terms and definitions..... 1

4 Abbreviations	1
5 Overview	2
5.1 General	2
5.2 Features	2
5.3 Stakeholders	3
5.4 Life cycles	4
5.5 Reference model	5
5.6 Security and privacy dimensions	8
6 Guidelines to assess risks	8
6.1 General	8
6.2 Sources of security risks	9
6.2.1 Security risks for service sub-systems	9
6.2.2 Security risks for IoT-domotics gateway	10
6.2.3 Security risks for IoT-domotics devices and physical entities	12
6.2.4 Security risks for networks	13
6.3 Sources of privacy risks	14
6.3.1 Privacy risks for service sub-systems	14
6.3.2 Privacy risks for IoT-domotics gateway	15
6.3.3 Privacy risks for IoT-domotics devices and physical entities	16
6.3.4 Privacy risks for networks	17
7 Security and privacy controls	17
7.1 Principles	17
7.1.1 General	17
7.1.2 Different levels of security for different services	17
7.1.3 Easy security settings for users	18
7.1.4 Failsafe domotics devices	18
7.1.5 Restricted access to content services	18
7.1.6 Consideration for children	18
7.1.7 Scenario-specific privacy preferences	18
7.2 Security controls	18
7.2.1 Policy for IoT-domotics security	18
7.2.2 Organization of IoT-domotics security	18
7.2.3 Asset management	18
7.2.4 Equipment and assets located outside physical secured areas	19
7.2.5 Secure disposal or re-use of equipment	19
7.2.6 Learning from security incidents	19
7.2.7 Secure IoT-domotics system engineering principles	19

7.2.8 Secure development environment and procedures.....	20
7.2.9 Security of IoT-domotics systems in support of safety	20
7.2.10 Security in connecting varied IoT-domotics devices	20
7.2.11 Verification of IoT-domotics devices and systems design.....	20
7.2.12 Monitoring and logging.....	21
7.2.13 Protection of logs.....	21
7.2.14 Use of suitable networks for the IoT-domotics systems.....	21
7.2.15 Secure settings and configurations in delivery of IoT-domotics devices and services	21
7.2.16 User and device authentication	21
7.2.17 Provision of software and firmware updates	22
7.2.18 Sharing vulnerability information.....	22
7.2.19 Security measures adapted to the life cycle of IoT-domotics system and services.....	22
7.2.20 Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services.....	22
7.2.21 Determination of security roles for stakeholders.....	22
7.2.22 Management of vulnerable devices.....	23
7.2.23 Management of supplier relationships for information security	23
7.2.24 Secure disclosure of Information regarding security of IoT-domotics devices.....	23
7.3 Privacy controls.....	23
7.3.1 Prevention of privacy invasive events.....	23
7.3.2 IoT-domotics privacy by default.....	23
7.3.3 Provision of privacy notice.....	23
7.3.4 Verification of IoT-domotics functionality.....	24
7.3.5 Consideration of IoT-domotics users.....	24
7.3.6 Management of IoT-domotics privacy controls.....	24
7.3.7 Unique device identity.....	24
7.3.8 Fail-safe authentication.....	25
7.3.9 Minimization of indirect data collection.....	25
7.3.10 Communication of privacy preferences	25
7.3.11 Verification of automated decision	25
7.3.12 Accountability for stakeholders.....	25
7.3.13 Unlinkability of PII.....	25
7.3.14 Sharing information on PII protection measures of IoT-domotics devices.....	26
Annex A (informative) Use cases of IoT-domotics	27
A.1 Use case 1: Entertainment	27
A.2 Use case 2: Electrical appliance control.....	27
A.3 Use case 3: Monitoring and security system.....	28
A.4 Use case 4: Care service.....	29

Formatted: HeaderCentered, Left

A.5 Use case 5: Energy management 30

A.6 Use case 6: Car video communication 30

Annex B (informative) Security and privacy concerns from stakeholders 32

B.1 Security concerns 32

B.1.1 General 32

B.1.2 Security concerns from IoT-domotics service provider 32

B.1.3 Security concerns from IoT-domotics service developer 32

B.1.4 Security concerns from IoT-domotics user 34

B.2 Privacy concerns 34

B.2.1 General 34

B.2.2 Privacy concerns from IoT-domotics service provider 35

B.2.3 Privacy concerns from IoT-domotics service developer 35

B.2.4 Privacy concerns from IoT-domotics user 35

Annex C (informative) Security and privacy responsibilities of stakeholders 37

C.1 Responsibilities of IoT-domotics service provider 37

C.2 Responsibilities of IoT-domotics service developer 37

C.3 Responsibilities of IoT-domotics user 38

Annex D (informative) Security measures for different types of IoT-domotics devices 39

D.1 Class I 39

D.2 Class II 39

D.3 Class III 40

D.4 Class IV 40

Bibliography 41

ISO/IEC FDIS 27403
<https://standards.iteh.ai/catalog/standards/iso/16d945b9-a01f-4cc5-b6cf-af79df304647/iso-iec-fdis-27403>

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Formatted: English (United Kingdom)

Field Code Changed

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

Formatted: English (United Kingdom)

Field Code Changed

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: FooterPageRomanNumber

*

© ISO/IEC 2023 – All rights reserved

© ISO/IEC 2024 – All rights reserved

x

Introduction

Although IoT-domotics have been widely applied worldwide, many IoT-domotics devices, communication protocols and platforms are developed without sufficient security and privacy considerations, which can pose security and privacy risks. Due to the long supply chain and the large number of stakeholders involved, it is important to establish the stakeholders, identify risks during the life cycle, and put forward proposals for resolving security and privacy issues in IoT-domotics. This document provides guidelines to analyse security and privacy risks and identifies controls that should be implemented in IoT-domotics systems.

IoT-domotics have some features that differ from other forms of IoT deployment, such as non-expert users, and ad hoc architecture. This document therefore adapts the general IoT security and privacy principles to IoT-domotics; and provides stakeholders with thorough and tailored guidelines for scenarios specific to IoT-domotics.

The target audiences of this document include IoT-domotics service providers, IoT-domotics service developers, and those who supervise or verify security and privacy for IoT-domotics.

Formatted: English (United Kingdom)

The goal of this document is to ensure that security and privacy for IoT-domotics are achieved without requiring end-users to have in-depth IT knowledge. Although this document can be used by interested end-users, they are not the target audience.

iteh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 27403

https://standards.iteh.ai/catalog/standards/iso/16d945b9-a01f-4cc5-b6cf-af79df304647/iso-iec-fdis-27403

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

1 Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT)-domotics systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20924, Information technology — Internet of Things (IoT) — Vocabulary

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 29100, Information technology – Security techniques – Privacy framework

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 29100, ISO/IEC 20924 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

IoT-domotics

Internet of Things (IoT) system composed of networks, devices, services and users typically used in the domicile or as electronic wearables

Note 1—to entry:—Devices are usually available to the consumer through retail purchase.

Note 2—to entry:—According to ISO/IEC TR 22417:2017, 6.3, this IoT-domotics denotes the private, hence highly customizable, indoor area where someone lives, alone or with friends/relatives/roommates. Thus, it includes dedicated infrastructure aimed to support those individuals, such as healthcare and wellness systems, building control systems, smart metering and systems for entertainment and gaming.

3.2

Entities

an entity is anything (both physical and non-physical) element, which has a distinct and independent existence.

Note 1 to entry: Every entity has a unique identity.

[SOURCE: Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.2].

3.3

Domains

~~a domain is a~~

major functional group of an Internet of Things (IoT) system:

Note 1 to entry: Every *entity* [\[3.2\]](#) in an IoT system participates in one or more domains and is said to be included or contained by that domain.

[SOURCE: Note 2 to entry: See ISO/IEC 30141:2018, 8.2.1.3].

4 Abbreviated terms

AI	artificial intelligence
App	application
AR	augmented reality
CRM	customer relationship management
DDoS	distributed denial of service
ICT	information and communication technology
IP	internet protocol
IoT	internetInternet of thingsThings
NB-IoT	narrow band internetInternet of thingsThings
PII	personally identifiable information
RF	radio frequency
TV	television
URL	uniform resource locator
USB	universal serial bus
VR	virtual reality

5 Overview

5.1 General

The security and privacy of IoT-domotics have a bearing on the normal operation of in-domicile services, the well-being of residents, and the integrity of infrastructures that are linked directly or indirectly with devices of services. Stakeholders including users, service providers, device manufacturers, network operators and industry supervisors are becoming increasingly concerned by security and privacy issues of IoT-domotics.

In comparison with other IoT solutions, IoT-domotics have specific features and concerns. It is therefore essential to adapt the general IoT security and privacy principles to IoT-domotics and provide stakeholders with thorough and tailored guidelines in specific scenarios of IoT-domotics.

~~The target audiences of this document include IoT domotics service providers, IoT domotics service developers, and those who supervise or verify security and privacy for IoT domotics.~~