International Standard

ISO/IEC 27404

Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT

Cybersécurité — Sécurité et protection de la vie privée pour l'IDO — Cadre d'étiquetage de cybersécurité pour l'IDO grand public

First edition
2025-10

Reference number
ISO/IEC 27404:2025(en)

© ISO/IEC 2025



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

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 member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **4**
5 Overview of cybersecurity labelling for consumer IoT **5**
5.1 Cybersecurity labelling for consumer IoT 5
5.2 Guiding principles 5
5.3 Programme objectives 6
5.4 Threats and risks to consumer IoT products 6
5.4.1 General 6
5.4.2 Assumptions 6
5.4.3 Risk considerations and high-level categories 7
5.4.4 Security threats and risks 7
5.4.5 Privacy threats and risks 8
5.5 Relevant standards and guidance documents 9
6 International alignment through a cybersecurity labelling framework **9**
6.1 Objectives for international alignment 9
6.2 Determination of cybersecurity requirements through relevant standards and guidance documents 9
7 Requirements and guidance for the components of the cybersecurity labelling framework for consumer IoT **10**
7.1 General 10
7.2 Requirements for the cybersecurity labelling framework components 10
7.3 Guidance on the core components of cybersecurity labelling framework 11
7.4 Guidance on key stakeholders' roles and responsibilities 12
7.5 Guidance on binary and multi-level labelling schemes 13
7.5.1 General 13
7.5.2 Binary versus multi-level labelling schemes 13
7.5.3 Basis for levels 14
7.6 Guidance on mutual- and cross-recognition 14
7.6.1 General 14
7.6.2 Benefits 14
7.6.3 Equivalency determination 15
7.7 Guidance on conformity assessment 15
7.7.1 General 15
7.7.2 Assessment activities considerations 15
7.8 Guidance on implementation considerations 16
8 Requirements and guidance for labelling issuance and maintenance for consumer IoT **16**
8.1 General 16
8.2 Requirements for labelling issuance and maintenance for consumer IoT 17
8.3 Guidance on acceptance criteria and validation of application 17
8.4 Guidance on label validity 18
8.4.1 Scope of validity 18
8.4.2 Recommendations for labelled consumer IoT products during validity period 18
8.5 Guidance on surveillance and monitoring 18
8.6 Guidance on label maintenance and lifecycle of consumer IoT 19
8.7 Guidance on renewal of labels 19
8.8 Guidance on revocation of labels 19
8.9 Guidance on change of underlying standard 20
8.10 Guidance on label design and characteristics 20

© ISO/IEC 2025 – All rights reserved

8.10.1 General 20
8.10.2 Label design 20
8.10.3 Label characteristics 21
Annex A (informative) **Types and features of cybersecurity labels** **22**
Annex B (informative) **Illustrative examples of multi-level labelling schemes** **25**
Annex C (informative) **Illustrative examples of binary labelling schemes** **34**
Annex D (informative) **Determination of equivalency among labelling schemes** **39**
Annex E (informative) **Examples of cybersecurity baseline provisions** **47**
Annex F (informative) **Examples of security-by-design provisions** **58**
Annex G (informative) **Examples of privacy assessment requirements** **60**
Bibliography **62**

© ISO/IEC 2025 – All rights reserved

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).

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.

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.

© ISO/IEC 2025 – All rights reserved

Introduction

Globally, there is an accelerated increase in the number of IoT (Internet of Things) products. Consumer IoT products often have short time-to-market and quick obsolescence lifecycles. Coupled with low price-points and low profit margins for consumer items, it is often the case that such products are not designed or manufactured with adequate cybersecurity provisions, meaning that these products can have fundamental security weaknesses and common flaws. As these connected products proliferate, the lack of adequate provisions for cybersecurity in such products creates extensive attack surfaces, causing them to be susceptible to cyber attacks using malware and penetration testing tools that are easily available.

Consumer IoT labelling schemes are instances of conformity assessment programmes, providing information on whether labelled products are resilient to common cybersecurity attacks. These consumer IoT labelling schemes follow the concepts and functional approach defined in ISO/IEC 17000 and ISO/IEC 17067, providing guidance on essential security traits for consumer IoT that is intended to encourage developers to proactively incorporate cybersecurity when designing their products.

The development of individual consumer IoT labelling schemes, which are designed to address the cybersecurity concerns in a particular region or market, has the potential to create confusion in the international marketplace by making it difficult to compare across labelled products. A cybersecurity labelling framework is therefore needed to help align the concepts and cybersecurity requirements represented by each of the consumer IoT cybersecurity labels.

This document outlines a consumer IoT cybersecurity labelling framework that is intended to reduce the need for duplicative testing, reduce the cost of compliance, and help facilitate a global market for developers. In addition, this framework can help facilitate the development of mutual- and cross-recognition agreements by providing the basis for repeatable and meaningful comparison between the standards- and guidance-based requirements that underpin consumer IoT labelling schemes that use this framework.

The cybersecurity labelling framework facilitates international alignment by providing guidance on selecting relevant standards and guidance documents (e.g. ETSI EN 303 645,[1] ETSI TS 103 701,[2] NIST IR 8259,[3] NIST IR 8259A,[4] NIST IR 8425,[5] ISO/IEC 27400, ISO/IEC 27402 and ISO/IEC 27403) for labelling schemes to derive their cybersecurity requirements. Implementing a consumer IoT cybersecurity labelling scheme based on this framework can simplify the mutual- and cross- recognition process. Furthermore, the implementation of cybersecurity labelling schemes, which provide additional specificities (such as test cases and capacities) are complementary to this framework.

The document explains the fundamental concepts of the cybersecurity labelling framework and provides the underlying requirements to help producers and suppliers participate in the process of improving cybersecurity protections for consumer IoT products and to develop products which meet or exceed minimum cybersecurity requirements.

This cybersecurity labelling framework addresses the expected and intended use of consumer IoT products by consumers, that is, the general public and non-technical users. Due to potentially more serious implications if compromised, IoT products used in an enterprise context are not classified as consumer IoT products. Furthermore, threat models of consumer IoT products assume the products are not being centrally managed by a professional system administrator.

The cybersecurity labelling framework provides guidance for binary or multi-level schemes based on common requirements in relevant standards and guidance documents. Products developed referencing these labelling schemes can be mutually- or cross-recognized when scheme owners of the corresponding negotiated schemes have determined that they are compatible. Developers can develop products referencing these labelling schemes, and then achieve mutual- or cross- recognition by examining the interoperability among schemes.

The cybersecurity labelling framework seeks to achieve outcomes in the following aspects:

— Transparency for consumers: The cybersecurity provision of consumer IoT products is opaque to general consumers. The cybersecurity labelling framework for consumer IoT aims to specify the requirements for cybersecurity labelling to make such cybersecurity provisions transparent to consumers, and to enhance consumer awareness of cybersecurity risks. Through the use of cybersecurity labelling, consumers can

© ISO/IEC 2025 – All rights reserved

make informed choices when purchasing consumer IoT products and adopt a cybersecurity mindset in a digital world.

— Developer branding: Cybersecurity labelling can cultivate a more proactive and sustainable industry, with developers differentiating their products and enhancing their brand quality. It also incentivises developers to produce more secure products and monetise their efforts spent in provisioning cybersecurity in their products.

— Mutual- and cross-recognition for the economy/ecosystem: As the digital economy grows, compatibility of cybersecurity labelling can help to reduce the need for duplicated testing across borders, reduce the cost of compliance for developers for improved market access and pave the way for mutual- or cross-recognition of labelling initiatives across countries.

The cybersecurity labelling framework supports a basis to detail the security features in consumer IoT products. With a framework, scheme owners can specify their labelling schemes, developers are incentivised to identify common requirements and implement better security features, and consumers can make informed purchasing decisions. The result can lead to a safer and more secure cyberspace.

Cybersecurity labelling for consumer IoT products does not offer formal security assurance. Users seeking higher security assurance in sectors such as enterprises, manufacturing, industrial applications and healthcare are recommended to consider products certified under formal evaluation and certification schemes (e.g. as described in ISO/IEC 15408-1).

© ISO/IEC 2025 – All rights reserved

Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT

1 Scope

This document defines a cybersecurity labelling framework for the development and implementation of cybersecurity labelling programmes for consumer Internet of things (IoT) products. It provides requirements and guidance on the following topics:

— risks and threats associated with consumer IoT products;

— stakeholders, roles and responsibilities;

— relevant standards and guidance documents;

— conformity assessment;

— labelling issuance and maintenance;

— mutual recognition.

This document is limited to consumer IoT products, such as:

— IoT gateways, base stations and hubs to which multiple devices connect; smart cameras, televisions, and speakers;

— wearable devices;

— connected smoke detectors, door locks and window sensors;

— connected home automation and alarm systems;

— connected appliances, such as washing machines and fridges;

— smart home assistants; and

— connected children's toys and baby monitors.

Products that are not intended for consumer use are excluded from this document. Examples of excluded devices are those that are primarily intended for manufacturing, healthcare and other industrial purposes.

This document is applicable to consumers, developers, issuing bodies of cybersecurity labels and conformity assessment bodies.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

© ISO/IEC 2025 – All rights reserved

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 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
binary scheme
labelling scheme with a list of cybersecurity features which must be included for the device to pass and obtain a label

3.2
conformity assessment
demonstration that specified requirements are fulfilled

[SOURCE: ISO/IEC 17000:2020, 4.1, modified — notes to entry have been deleted.]

3.3
conformity assessment programme
conformity assessment scheme
set of rules and procedures that describes the objects of conformity assessment, identifies the specified requirements and provides the methodology for performing *conformity assessment* (3.2)

Note 1 to entry: A conformity assessment programme can be managed within a conformity assessment system.

Note 2 to entry: A conformity assessment programme can be operated at an international, regional, national sub-national, or industry sector level.

Note 3 to entry: A conformity assessment programme can cover all or part of the conformity assessment functions.

[SOURCE: ISO/IEC 17000:2020, 4.9, modified — "Annex A" has been removed from Note 3 to entry for contextual reasons.]

3.4
conformity assessment body
CAB
body that performs *conformity assessment* (3.2) activities, excluding accreditation

[SOURCE: ISO/IEC 17000:2020, 4.6]

3.5
consumer
natural person who is acting for purposes that are outside their trade, business, craft or profession

Note 1 to entry: This can include a person who is a potential buyer of a labelled product.

3.6
cyber attack
attack
malicious attempts to exploit vulnerabilities in information systems or physical systems in cyberspace and to damage, disrupt or gain unauthorized access to these systems

Note 1 to entry: Expression of an offensive operation in or through the cyberspace leading to unauthorized use of services, creating illicit services, orchestrating denial of service, altering or deleting data or resources.

Note 2 to entry: Common cyber attacks to consumer IoT are basic attacks that could be carried out by script kiddies and amateur hackers.

[SOURCE: ISO/IEC TS 27100:2020, 3.1, modified — Note 2 to entry has been added.]

© ISO/IEC 2025 – All rights reserved

3.7
developer
entity that creates an assembled final *Internet of things* (*IoT) device* (3.10) or *IoT product* (3.11)

Note 1 to entry: "Final" in this definition means the stage of delivery to the IoT service developer in the assembly process.

Note 2 to entry: A developer is usually the applicant for a cybersecurity label or the holder of the issued label, i.e. the party responsible for the security characteristics of a product.

3.8
evidence
directly measurable characteristics of an *Internet of things product* (3.11) that represent objective and demonstrable proof that a specific activity satisfies a specified requirement

Note 1 to entry: Test reports, handbooks, files, checklists, scripts or images.

[SOURCE: ISO/IEC 21827:2008, 3.19, modified — "process and/or product" has been replaced with "Internet of things product"; the Example has been added.]

3.9
Internet of Things
IoT
infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2024, 3.2.8]

3.10
Internet of Things device
IoT device
entity of an *IoT system* (3.13) or *IoT solution* (3.12) that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: In this document, an IoT device is usually a physical product, which can be bought off the shelf by a consumer, e.g. a router, bulb or toy.

[SOURCE: ISO/IEC 27400:2022, 3.3, modified — note 1 to entry has been added.]

3.11
Internet of Things product
IoT product
Internet of Things good or service

Note 1 to entry: A good in this context can take the form of an *IoT device* (3.10), *IoT solution* (3.12), or *IoT system* (3.13) along with bundled software.

Note 2 to entry: Services can include connectivity, cloud computing resources, maintenance, technical support, etc.

3.12
Internet of Things solution
IoT solution
seamlessly integrated bundle of technologies, potentially including sensors, gateways and actuators

Note 1 to entry: These can solve a specific problem or need, or they can be used to build additional functionality in other non-IoT solutions.

Note 2 to entry: Within the scope of this document, a solution typically combines hardware components (physical devices like a router, bulb, toy or sensors/actuators) and associated IoT services (e.g. an application for remote control or cloud space) and can be bought e.g. off the shelf by a consumer.

[SOURCE: ISO/IEC 27400:2022, 3.7, modified — note 2 to entry has been added.]

© ISO/IEC 2025 – All rights reserved

3.13
Internet of Things system
IoT system
system providing functionalities of Internet of Things

Note 1 to entry: IoT system is inclusive of *IoT devices* (3.10), *IoT solutions* (3.12), IoT gateways, sensors and actuators.

Note 2 to entry: In the context of this document, this also includes applications and backend that support IoT solutions.

[SOURCE: ISO/IEC 27400:2022, 3.6]

3.14
independent test laboratory
ITL
security testing body that conducts third-party security evaluations of products

3.15
labelling scheme
application or instantiation of the *conformity assessment programme* (3.3) for the labelling of consumer Internet of Things, taking into account the additional administrative or regulatory requirements of each nation or region

Note 1 to entry: A labelling scheme is an example of a conformity assessment scheme from ISO/IEC 17000.

3.16
object of labelling
Internet of Things product (3.11) seeking eligibility and currently being assessed for a particular cybersecurity label

3.17
product
any good or service

[SOURCE: ISO 14050:2020, 3.5.12]

4 Abbreviated terms

API	application programming interface
BOM	bill of materials
CAB	conformity assessment body
DAST	dynamic analysis security testing
DDoS	distributed denial of service
HCI	human computer interface
ITL	independent test laboratory
PII	personally identifiable information
SAST	static application security testing

© ISO/IEC 2025 – All rights reserved