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)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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

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).

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*