International Standard

ISO/IEC 27403

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

Cybersécurité — Sécurité et protection de la vie privée pour l'IDO — Lignes directrices pour la domotique-IDO

First edition
2024-06

Reference number
ISO/IEC 27403:2024(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

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.

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.

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, *Internet of Things (IoT) and digital twin — Vocabulary*

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

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*