BS ISO/IEC 27403:2024

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27403:2024

National foreword

This British Standard is the UK implementation of ISO/IEC 27403:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 12448 4

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2024.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27403:2024

International Standard

ISO/IEC 27403

First edition
2024-06

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

Reference number
ISO/IEC 27403:2024(en)

© ISO/IEC 2024

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27403:2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27403:2024

Contents

Page

Foreword ... **v**
Introduction ... **vi**
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 ... 2
5.3 Stakeholders ... 4
5.4 Life cycles ... 4
5.5 Reference model ... 5
5.6 Security and privacy dimensions ... 8
6 Guidelines for risk assessment ... **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 ... 13
6.3.1 Privacy risks for service sub-systems ... 13
6.3.2 Privacy risks for IoT-domotics gateway ... 14
6.3.3 Privacy risks for IoT-domotics devices and physical entitles ... 16
6.3.4 Privacy risks for networks ... 16
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 ... 17
7.1.4 Failsafe domotics devices ... 17
7.1.5 Restricted access to content services ... 17
7.1.6 Consideration for children ... 17
7.1.7 Scenario-specific privacy preferences ... 17
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 ... 18
7.2.5 Secure disposal or re-use of equipment ... 18
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 ... 19
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 ... 20
7.2.13 Protection of logs ... 20
7.2.14 Use of suitable networks for the IoT-domotics systems ... 20
7.2.15 Secure settings and configurations in delivery of IoT-domotics devices and services ... 20
7.2.16 User and device authentication ... 21

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

7.2.17 Provision of software and firmware updates ... 21
7.2.18 Sharing vulnerability information ... 21
7.2.19 Security measures adapted to the life cycle of IoT-domotics system and services ... 21
7.2.20 Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services ... 21
7.2.21 Determination of security roles for stakeholders ... 22
7.2.22 Management of vulnerable devices ... 22
7.2.23 Management of supplier relationships in IoT-domotics security ... 22
7.2.24 Secure disclosure of Information regarding security of IoT-domotics devices ... 22
7.3 Privacy controls ... 22
7.3.1 Prevention of privacy invasive events ... 22
7.3.2 IoT-domotics privacy by default ... 22
7.3.3 Provision of privacy notice ... 23
7.3.4 Verification of IoT-domotics functionality ... 23
7.3.5 Consideration of IoT-domotics users ... 23
7.3.6 Management of IoT-domotics privacy controls ... 23
7.3.7 Unique device identity ... 24
7.3.8 Fail-safe authentication ... 24
7.3.9 Minimization of indirect data collection ... 24
7.3.10 Communication of privacy preferences ... 24
7.3.11 Verification of automated decision ... 24
7.3.12 Accountability for stakeholders ... 24
7.3.13 Unlinkability of PII ... 24
7.3.14 Sharing information on PII protection measures of IoT-domotics devices ... 25

Annex A (informative) **Use cases of IoT-domotics** ... **26**

Annex B (informative) **Security and privacy concerns from stakeholders** ... **31**

Annex C (informative) **Security and privacy responsibilities of stakeholders** ... **35**

Annex D (informative) **Security measures for different types of IoT-domotics devices** ... **37**

Bibliography ... **39**

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

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 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

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.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

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*

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, 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
entity
physical or non-physical element, which has a distinct and independent existence

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

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

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

3.3
domain
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.

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	Internet of Things
NB-IoT	narrow band Internet of Things
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.

5.2 Features

Some examples of IoT-domotics systems can be found in Annex A. Many of the features of IoT-domotics can affect the security and privacy considerations. These features should be specifically considered in the context of security and privacy. Such features include:

a) open and varied home environments;

   1) terminal devices: devices can be smart devices, lightweight function devices or appliances;

   2) communication protocols: such as ethernet, wireless, and/or bluetooth;

   3) physical input methods: such as voice commands, touch, and/or gestures;

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

4) varied applications and services: an IoT-domotics solution can provide multiple services simultaneously, like entertainment, electrical appliance control, security system, assistance service and energy management;

5) dynamic network: a device or service can join and leave the environment dynamically and flexibly;

6) complex interactions: interactions can be in multiple forms, such as human-device, device-device, device-service and human-service;

7) multi-party interactions: multiple devices/points of connectivity in domiciles.

b) features related to domiciles;

1) context awareness: as devices and services get smarter, it can be necessary for IoT-domotics to have awareness of social and cultural imperatives in order to be useful for end users. A human can interact with the IoT-domotics device which in turn can share context information with another device or another human;

2) privacy concerns: devices and services are likely to have access to personal data (e.g. location, habits, and/or relationships). Besides, devices and services exchange context information which can contain personal data;

3) relationships:

i) human to device relationships: interactions relying on a variety of information inputs such as images and user presence, as well as identification methods such as speech;

ii) device-to-device relationships: interactions where devices communicate with one another actively (e.g. a thermostat that triggers the lowering of a window shade) or passively (e.g. a device that identifies presence of a user when the user leaves one area of the domicile and enters another).

4) access restrictions: IoT-domotics devices are used in scenarios involving children and can involve the protection of children from accessing the Internet, such as payment business restrictions, content hierarchical access restrictions;

5) biometric protection: IoT-domotics devices can record personal biometric information such as irises, fingerprints, faces and voice. It involves the secure storage, verification and protection of data;

6) operational protection mechanism: IoT-domotics devices can have hierarchical use or interoperability secondary confirmation security protection, such as preventing children from operating washing machines and microwave ovens, as well as protection buttons to prevent pets and children from misoperations.

c) users, inhabitants and other living entities that can be present and/or impacted by the deployment and use of an IoT-domotic solution in a home, such as:

1) by categories: elderly, adults, teenagers, children, babies, people with reduced autonomy, persons with disabilities and pets;

2) by roles: owners, administrators, users, as well as individuals and other living entities, such as pets and plants that can be impacted;

3) by adverse impact: victims of coercive control (e.g. of smart locks or thermostats), or surveillance (e.g. by hidden cameras or microphones).

d) interoperability: this is an important aspect for seamless communication between all devices in an IoT-domotics environment, regardless of their make or model.

e) user-friendly interface and usability: IoT-domotics systems' interfaces should be intuitive and designed to be easy for users to navigate, especially considering that it is possible that not all users are tech-savvy.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

5.3 Stakeholders

Stakeholders of IoT-domotics are IoT-domotics service providers, IoT-domotics service developers and IoT-domotics users. These stakeholders are identified in the context of the features of IoT-domotics (see 5.2) in conformance with the stakeholders of IoT systems defined in ISO/IEC 30141. Table 1 shows the stakeholders of IoT-domotics with explanations.

Table 1 — Stakeholders involved in IoT-domotics

Stakeholders	Sub-role	Descriptions
IoT-domotics service provider	Business manager Delivery manager Domicile network/sensor installer System operator	To document the approach to be taken for the risk assessment, and to manage and operate IoT-domotics services and/or to provide network connectivity.
IoT-domotics service developer	Solution architect Solution/application/device developer Developer manager System integrator	To design, implement, test and integrate IoT-domotics services, devices and applications.
IoT-domotics user	Residents in domicile Domicile visitors	End users of IoT-domotics services

The definitions of the roles of IoT-domotics stakeholders are as follows:

a) IoT-domotics service provider

Role definition: to document the approach to be taken for the risk assessment, and to manage and operate IoT-domotics services and/or to provide network connectivity. Since IoT-domotics devices can be physically linked to the domicile, an important sub-role is IoT-domotics installer, who installs the IoT-domotics within the domicile.

b) IoT-domotics service developer

Role definition: to develop, test and integrate IoT-domotics services, devices and applications.

c) IoT-domotics user

Role definition: owners, administrators, users, as well as individuals and other digital and living entities that can use or be impacted by the deployment and use of an IoT-domotic solution in a domicile.

Refer to Annex B for the security and privacy concerns of these stakeholders. Refer to Annex C for the responsibilities of these stakeholders.

5.4 Life cycles

This document describes the IoT-domotics life cycles adapted from the IoT service life cycles in ISO/IEC 27400:2022, 5.5. According to related stakeholders, three different life cycles processes are considered for different stakeholders. Figure 1 shows the IoT-domotics life cycles processes of stakeholders.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

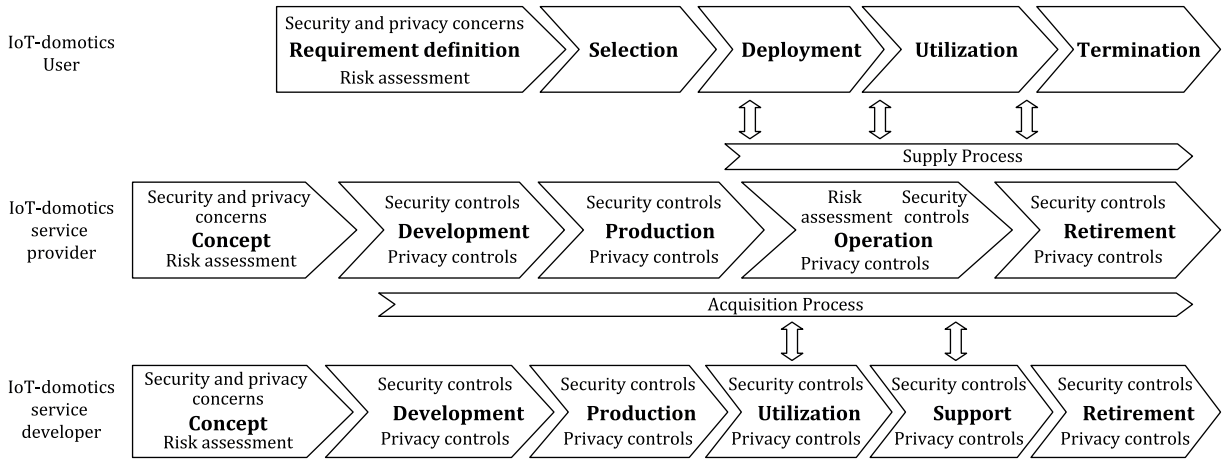


Figure 1 — IoT-domotics life cycles

Life cycles vary depending on each stakeholder. Different stakeholders can be related at different stages in their respective life cycles, especially for service providers. The IoT-domotics service is provided to IoT-domotics users through the supply process of the IoT-domotics service providers. An IoT-domotics service provider acquires an IoT device and software from the IoT-domotics developer in the acquisition process.

When an IoT-domotics user acquires and uses IoT-domotics products or services, life cycles stages include requirement definition, selection, utilization, and termination. In the requirement definition stage, the IoT-domotics user can consider product functional requirements and other aspects, such as security and privacy requirements. Based on the information disclosed in the supply process, an IoT-domotics user selects an IoT-domotics service that meets the required specification. For example, at the termination stage, there are risks of personal data leakage if measures such as account deletion and verification of secure data deletion are not implemented both in the IoT-domotics devices and on the server databases on the back-office side.

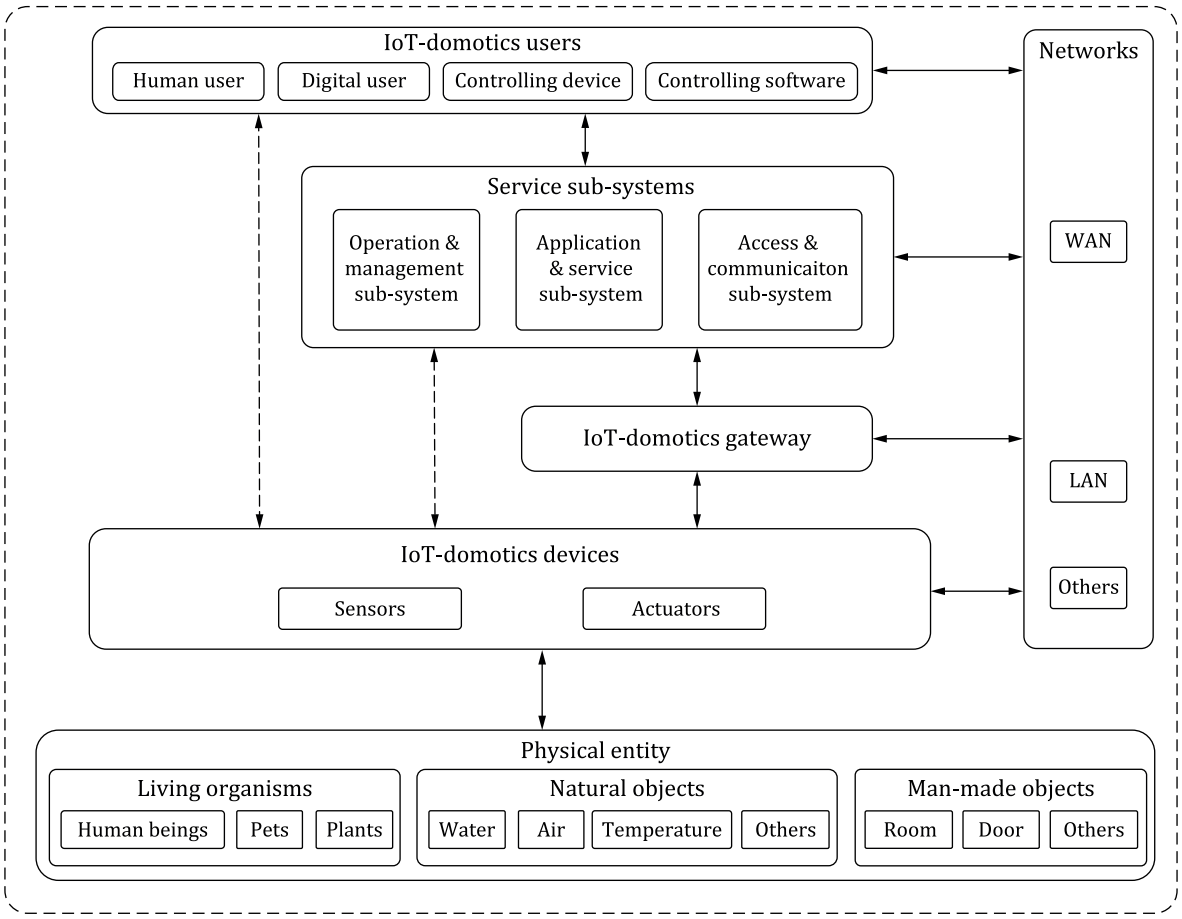
For the developer of IoT-domotic services, it is not only about the development, testing and deployment of software, but also about the production and maintenance of devices. In the process of mass production of the IoT-domotic solution (i.e. software and devices), the demonstration of security consistency with the initial requirements should also be taken into account. For example, software and firmware updates are processes that carry their own set of security risks which can arise during the use and support phases, and which should be mitigated.

5.5 Reference model

The reference model in this document is based on the entity-based reference model in ISO/IEC 30141 with instanced objects involving IoT-domotics users and networks as shown in Figure 2. An entity-based representation of IoT-domotics includes physical entities, IoT-domotics users, IoT-domotics devices, IoT-domotics gateway, networks and services for operation and management, applications and services, as well as access and communication.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024



Key

IOT-domotics system

inner-domotics environment

physical connection

logical connection

Figure 2 — IoT-domotics reference model

Figure 2 shows the following entities in IoT-domotics:

a) Physical entity

A physical entity is a discrete, identifiable, and observable part of the physical environment. Examples of physical entities are living organisms (e.g. human beings, pets or plants), natural objects (e.g. water, air or temperature) and man-made objects (e.g. a room, a door, or a curtain).

b) IoT-domotics users

IoT-domotics users are subdivided into user types, for example:

1) human user: interacts with IoT-domotics devices and services with the help of controlling devices and controlling software;

2) controlling device: dedicated devices for human users to interact with IoT-domotics devices or to control IoT-domotics devices on behalf of human users;

3) controlling software: software to assist human users to interact with IoT-domotics devices or to control IoT-domotics devices on behalf of human users;

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024

4) digital user: digital user applications can use capabilities of IoT-domotics devices and IoT-domotics services to create higher level services for human users.

c) IoT-domotics devices

IoT-domotics devices (e.g. smart camera, smart TV, smart door lock, or smoking detector) interact with the physical entity and/or act based on IoT-domotics user's command through devices such as sensors and actuators.

d) IoT-domotics gateway

An IoT-domotics gateway forms a connection between local network(s) and the wide area access network.

e) Networks

IoT-domotics systems can be connected by networks. Internet domotics devices are connected or bridged through wide area networks (WAN), such as those controlled via external server-based solutions that are not collocated on the same network or equivalent address space. These devices can be connected through ground-based RF terrestrial (e.g. cellular/microwave) connections, wired networks (e.g. copper/fibre) provided by telecommunication companies, and satellite/stratospheric RF relays. IoT-domotics devices leverage local area networks (LAN) whereby interaction is limited to collocation and can leverage RF range limiting protocols such as Z-Wave or can be attached to an isolated sub-network.

1) local area networks: short range network to connect kinds of IoT-domotics devices with low energy consumption, such as Zigbee®,[1] Bluetooth®,[2] WiFi, 3G/4G/5G;

2) wide area networks: wide range network to connect devices with application and management platforms;

3) others: other IoT-domotics networks, such as personal area network (PAN).

f) Service sub-systems

As in other IoT systems, IoT-domotics services also contain virtual entities, where a virtual entity is a digital representation of a physical entity.

1) operation and management sub-system: provides monitoring, management and administrative capabilities;

2) application and service sub-system: provides IoT-domotics data storage, data analytics and service process management;

3) access and communication sub-system: provides controlled interfaces for service capabilities, for administration capabilities and for business capabilities.

It should be noted that a domain-based reference model is illustrated in ISO/IEC 27400:2022, 5.6. Table 2 shows the correspondence between the entities described this document and domains described in ISO/IEC 27400.

1) Zigbee® is a trademark of Zigbee alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

2) Bluetooth® is a trademark of Bluetooth special interest group. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named.

© ISO/IEC 2024 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27403:2024