INTERNATIONAL STANDARD

ISO/IEC 27402

First edition
2023-11

Cybersecurity — IoT security and privacy — Device baseline requirements

Cybersécurité — Sécurité et protection de la vie privée pour l'IdO — Exigences de base relatives aux dispositifs

Reference number
ISO/IEC 27402:2023(E)

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*.

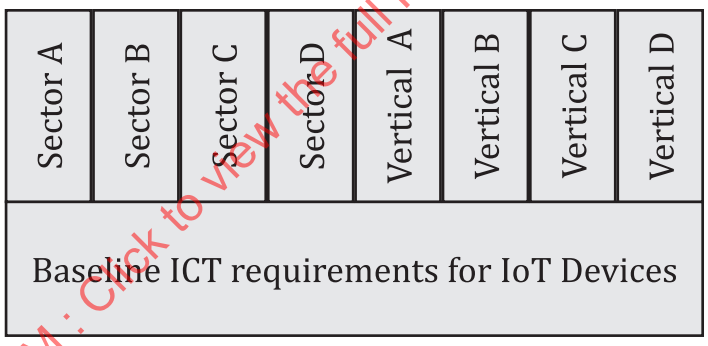
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

With the increasing number of Internet of Things (IoT) devices and increasing reliance on such devices, the security and privacy risks relating to those "things" are expected to grow. Their widespread deployment in networks and systems make them easy and prime targets for cyber attacks.

This document provides a baseline set of information and communication technologies (ICT) requirements so that IoT devices are able to support security and privacy controls. A risk assessment is critical to develop a risk treatment plan that identifies the necessary IoT device features and countermeasures. The management of systems which use IoT devices depends upon the capabilities of those devices (among other factors).

Broadly speaking, this document addresses ICT requirements for IoT devices that are made available to the market. The requirements in this document are intended as a baseline, upon which vertical markets (such as health, financial services, industrial, consumer electronics and transportation) can build additional requirements for the expected use and risks of IoT devices in their applications, as depicted in Figure 1. In addition to this document, various sectors (e.g. private/industrial, public, defence, national security) and vertical markets have sector- or vertical-specific requirements, for example those found in ETSI EN 303 645[11] for consumer devices and the IEC 62443 series for industrial devices and systems. While this document can provide requirements for a conformity assessment scheme, it is expected that stakeholders for specific sectors and vertical markets will develop consensus around requirements specific to their contexts, building "on top" of this document. Subsequently, conformity assessment programmes can be developed around those specific sectors and vertical markets. This document would be effectively integrated into such programmes while providing a common set of baseline requirements.



NOTE Additional requirements can be developed or required by specific sectors and vertical markets.

Figure 1 — Relationship between baseline requirements in this document and potential additional requirements

As the complex technical landscape of IoT devices evolves, this document can support a scalable globally harmonized approach to the baseline security and privacy requirements and inform technical policy and regulatory initiatives.

Cybersecurity — IoT security and privacy — Device baseline requirements

1 Scope

This document provides baseline ICT requirements for IoT devices to support security and privacy controls.

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 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*

ISO 31000:2018, *Risk management — Guidelines*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27400, ISO 31000, 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/

3.1.1
identifier
information that unambiguously distinguishes one entity from another one in a given identity context

[SOURCE: ISO/IEC 23093-1:2022, 3.2.7]

3.1.2
user interface
set of all components of an interactive system that provide information and controls for the user to accomplish specific tasks with the interactive system

[SOURCE: ISO 9241-110:2020, 3.10]

3.1.3
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 20924:2021, 3.2.4]

3.1.4
IoT system
system providing functionalities of *internet of things (IoT)* (3.1.3)

Note 1 to entry: An IoT system can include, but is not limited to, *IoT devices* (3.1.5), *IoT gateways* (3.1.7), sensors, and actuators.

Note 2 to entry: Conventional IT devices such as smartphones and laptops can form part of an IoT system.

Note 3 to entry: IoT systems also include cloud and network connectivity.

[SOURCE: ISO/IEC 20924:2021, 3.2.9, modified — notes 2 and 3 to entry have been added.]

3.1.5
IoT device
entity of an *internet of things (IoT) system* (3.1.4) that interacts and communicates with the physical world through sensing or actuating

Note 1 to entry: An IoT device can be a sensor or an actuator.

Note 2 to entry: An IoT device, in this context, is an assembled device usable for its intended IoT functions without relying on being embedded or integrated into any other product.

Note 3 to entry: IoT devices generally interact via communication interfaces.

[SOURCE: ISO/IEC 20924:2021, 3.2.6, modified — notes 1, 2 and 3 to entry have been added.]

3.1.6
IoT device developer
entity that creates an assembled final *internet of things (IoT) device* (3.1.5)

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

[SOURCE: ISO/IEC 27400:2022, 3.4]

3.1.7
IoT gateway
entity of an IoT system that connects one or more proximity networks and the IoT devices on those networks to each other and to one or more access networks

[SOURCE: ISO/IEC 20924:2021, 3.2.8]

3.1.8
trusted computing base
TCB
totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy

3.1.9
cryptographic module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.1.10
critical security parameter
CSP
security-related information whose disclosure or modification can compromise the security of a *cryptographic module* (3.1.9)

Note 1 to entry: A CSP can be plaintext or encrypted.

Note 2 to entry: In the example, “certificates” refers to private keys matching public keys inside certificates.

EXAMPLE 1 Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

EXAMPLE 2 Configuration settings required for initialization.

[SOURCE: ISO/IEC 19790:2012, 3.18, modified — note 2 to entry and example 2 have been added.]

3.1.11
sensitive security parameter
SSP
critical security parameters (3.1.10) and public security parameters

[SOURCE: ISO/IEC 19790:2012, 3.110]

3.1.12
factory default
state of the device after factory reset or after final production/assembly

Note 1 to entry: This includes the physical device and software (including firmware) that is present on it after assembly.

3.1.13
fail-safe mode
device or feature which, in the event of failure, responds in a way that causes no harm, or minimizes the harm, to other devices, and causes no danger, or minimizes the danger, to personnel

[SOURCE: ISO 25197:2020, 3.32]

3.2 Abbreviated terms

API application programming interface

ASLR address space layout randomization

CPU central processing unit

CSP critical security parameter

ICT information and communication technologies

IoT internet of things

PIN personal identification number

PSP public security parameter

RoT root of trust

TCB trusted computing base

SWID software identification

XML extensible markup language

4 Overview

IoT systems bring security and privacy risks, and ISO/IEC 27400 provides general information and guidance about these risks and threats to security and privacy. To address these risks, users (organizations and consumers) should implement appropriate controls, which are also detailed in

ISO/IEC 27400. These controls cannot be implemented if the IoT devices do not have the supporting functionality (process policies, capabilities etc.)

The IoT system developers are expected to develop their own requirements and seek IoT devices that support them. This document provides baseline ICT requirements for IoT devices. In many cases, additional requirements will be imposed or are expected to address the security and privacy risks of specific vertical markets or higher risk environments.

5 Requirements

5.1 Requirements for IoT device policies and documentation

5.1.1 Risk management

5.1.1.1 Requirements

5.1.1.1.1 IoT devices shall have documentation recording the results of a risk assessment process performed at the IoT device level in the context of a risk assessment at the system level.

5.1.1.1.2 The risk assessment process shall take into account intended outcomes for the intended use case.

5.1.1.1.3 The risk assessment process shall also take into account the needs and expectations of interested parties (e.g. those parties on networks to which the IoT device is connected), including physical and logical undesired effects.

NOTE 1 Risk assessment techniques can be found in IEC 31010 and ISO/IEC 27005.

NOTE 2 IoT device developers usually perform the risk assessments and produce the risk treatment plans.

5.1.1.1.4 The risk assessment shall take into account that IoT devices can be constrained (e.g. limited battery, little memory, "weak" CPU), which informs the risk treatment process.

5.1.1.1.5 Risk assessment and treatment processes shall be defined and applied as follows:

a) determine if separate risk assessment and treatment processes are necessary for different products;

b) select appropriate risk treatment options, taking account of the risk assessment results;

NOTE 1 Sector- or vertical market-specific standards can be used in addition to this document. Such a standard can provide a risk assessment and/or risk treatment plan specific to the sector or vertical market. Complying with such standards can be used to satisfy requirements in this document.

c) determine all controls that are necessary to implement the risk treatment option(s) chosen;

d) identify all security and privacy features of the IoT device from the controls identified in c) above;

NOTE 2 IoT device developers can design features as required or identify them from any appropriate source, such as an industry standard or sector guidance.

e) compare the features identified in d) above with those in 5.2, and verify that no necessary features have been omitted;

NOTE 3 5.2 contains a list of baseline features. Users of this document are directed to 5.2 to ensure that no requirements are overlooked.

NOTE 4 The features listed in 5.2 are not exhaustive. Additional features and controls can be necessary based on specific vertical market segments or to address higher-risk use cases.

f) produce a statement of applicability that contains the necessary features [see steps d) and e)] and justification for inclusions and the justification for exclusions of features from 5.2;

g) if other standards related to device requirements are used, implement the requirements of those standards after steps a) through to f);

h) formulate a risk treatment plan;

i) inform the risk owner of the risk treatment plan and any residual risks, or where applicable, obtain their approval of the plan and acceptance of the residual risks.

5.1.1.1.6 IoT devices shall implement the features and controls identified as necessary in its statement of applicability, as well as features and controls identified in 5.1.1.1.5**,** step g).

5.1.1.1.7 The documentation shall be available for the supported lifetime of the product.

5.1.1.2 Additional recommendation(s)

The risk assessment and treatment processes should follow a widely-accepted method such as the one given in ISO 31000. For additional guidance on using ISO 31000, see Annex A.

5.1.1.3 Additional information

Interested parties, such as IoT device developers, system integrators, importers, retailers or regulatory bodies can perform such risk assessments.

IoT devices can contain security and privacy features and controls identified from any source such as sector- or vertical market-specific standards as well those defined in this document. IoT devices may contain additional controls other than those identified as necessary by the risk assessment.

5.1.2 Information disclosure

5.1.2.1 Requirements

5.1.2.1.1 IoT devices shall have user documentation that lists the features that the IoT device provides to support controls for security and privacy, making it clear if any of the IoT device requirements in 5.2 are not included.

5.1.2.1.2 Such information shall be publicly available for the period of time the IoT device is supported.

5.1.2.1.3 IoT devices shall be covered by a security support policy and other supporting documentation wherein users are made aware in advance of when security updates will be discontinued.

5.1.2.2 Additional recommendation(s)

The requirements 5.1.2.1.1 to 5.1.2.1.3 should first be provided at the time of sale.

Guidance should be made available to the user post-purchase, possibly as part of the installation process, highlighting future IoT device events (such as updating software) and offering a means for the user to receive future communications.

The period of time when support is provided, as defined in the IoT device documentation, should be appropriate relative to the risks and to the expected lifetime of the product. Changing announced support periods should be avoided as doing so can disrupt the planning and operational cycles of users.

Device documentation should include information on how users can discover if support periods have been subsequently changed.

Clear and understandable information about the user's responsibilities to set up and maintain security and privacy in using the device should be provided.

All licensing agreements with users should clearly define the scope of security and privacy controls and rights during the use of the product, including any data collected during this period. These agreements should be provided in clear and easy to understand language.

Dependency information about third-party software components relevant for IoT device security should be provided. This information can be provided in a machine-readable format. Software identification (SWID) tags (see ISO/IEC 19770-2) can be used to identify software components.[16]

5.1.2.3 Additional information

Communication to the user can be done via an online reference, in a mobile application, in printed documentation for the IoT device and/or given on a label on the packaging. More than one method can be used.

Many different people can interact with, or be sensed by, any specific IoT device. The same person can interact with the IoT device in several different roles, e.g. as purchaser, installer, active user of functionality and passive target of sensing. When planning and executing communications with users, it is essential to be clear and accurate about the target of each communication and make it easy for users to access those communications both in role-specific and all-roles-for-one-person perspectives.

Communication can include a minimum period of support (in addition to the required communication on discontinuing updates).

5.1.3 Vulnerability disclosure and handling processes

5.1.3.1 Requirements

5.1.3.1.1 IoT devices shall have documentation that defines the vulnerability disclosure and handling processes that will apply for the supported lifetime of the device.

5.1.3.1.2 Vulnerability disclosure and handling processes shall include, at a minimum, a capability to receive reports of potential vulnerabilities from the public.

5.1.3.2 Additional recommendation(s)

Requirements 5.1.3.1.1 and 5.1.3.1.2 should be implemented in accordance with ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability handling processes).

5.2 Requirements for IoT device capabilities and operations

5.2.1 General

This clause includes IoT device features to be used with a risk assessment and treatment process in accordance with 5.1.1.

The required IoT device features in this document are included because they are suitable for a baseline standard. Each of the requirements in 5.2 are broadly applicable, technically feasible, impactful and can be assessed.

5.2.2 Configuration

5.2.2.1 Requirements

5.2.2.1.1 If the configuration settings of the IoT device can be modified, only authorized entities shall be able to modify the configuration settings of the IoT device.

NOTE Authorized entities can be a person or another device.

5.2.2.1.2 If IoT devices are capable of changing the configuration of IoT and other devices, they shall only be capable of making such changes when authorized.

5.2.2.2 Additional recommendation(s)

A procedure to update or change configuration settings should also include:

a) a way for authorized entities to transfer configuration data to the IoT device and store it on the device in validated data structure and/or data format;

b) a way to validate the integrity of the transmitted configuration settings before use;

c) a means for secure transmission of the settings including validation of the source of the update;

d) a way to confirm the settings have been successfully updated.

5.2.2.3 Additional information

Depending on device constraints, authorization for modifying configuration settings may be granted in different ways. Some examples include: having separate user roles as in modern operating systems, having physical access to the device (e.g. being able to press the "reset" button), being able to perform certain action(s) in a particular way (e.g. irradiate devices with a specially modulated signal on a specific frequency). The examples given here are for illustration purposes and are not exhaustive.

5.2.3 Software reset

5.2.3.1 Requirements

5.2.3.1.1 If IoT devices have the capability to be reset, that process shall be secure.

5.2.3.1.2 This capability shall only be executable by an authorized entity.

5.2.3.2 Additional information

Sometimes a vulnerability is remedied by changing the configuration, and by reverting to the factory defaults after such a remedy, the vulnerability can become exploitable again. An example of such a scenario is changing the current configuration to prevent the device from using cypher suites that are deemed insecure. The factory default can allow all cypher suites, so restoring to factory default in this scenario would expose vulnerabilities again.

This function can sometimes be combined with 5.2.4, so that configuration reset and user data removal can be performed in one action by an authorized entity. IoT device configuration and user data are sometimes combined or difficult to separate.

5.2.4 User data removal

5.2.4.1 Requirements

5.2.4.1.1 If the IoT device stores user data, it shall provide a function for deleting appropriate user data stored on the device in any type of memory.

5.2.4.1.2 The function shall be restricted to authorized entities only.

5.2.4.2 Additional recommendation(s)

The user should be provided with a notification that their data has been securely removed if the device is able to do so.

5.2.4.3 Additional information

User data may include personal data, user configuration data and cryptographic material such as keys.

Some IoT devices may implement this functionality by deleting all data for a group of users (perhaps even all data for all users). Deletion of more than the required data for a single user can be an acceptable means of complying with this requirement. However, this can result in user data being stored for longer than required to serve its purpose. This should therefore only be done with reasonable justification.

User data are often stored in other parts of the IoT system (e.g. in mobile applications and the cloud), and users expect that removal applies to all parts of the IoT system, not just the device itself.

5.2.5 Protection of data

5.2.5.1 Requirements

5.2.5.1.1 IoT devices shall be capable of protecting the data they store and transmit from unauthorized access, modification and disclosure.

5.2.5.1.2 This shall include configuration settings, identifying data, user data, event logs and sensitive security parameters.

5.2.5.1.3 IoT devices shall be capable of protecting their software (including firmware) from unauthorized access and modification.

5.2.5.1.4 IoT devices shall use cryptography (e.g. encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of data requiring protection from being compromised.

NOTE International and other globally recognized standards can be used for cryptography requirements.

5.2.5.2 Additional recommendation(s)

5.2.5.2.1 General

When IoT devices are started up, they should check the integrity and authenticity of the software and/or firmware and enforce security controls. If the IoT device fails these checks, it should:

— notify the user of any violation,

— render itself inoperable,

— operate in a fail-safe mode that provides security protection, or

— initiate device recovery if recovery actions can be performed with integrity.

Upon first installation or maintenance, IoT devices should set themselves to secure default configurations. User configuration options should prevent users from choosing insecure configurations or provide a warning.

If capable, IoT devices should have the ability to provide compartmentalization.

IoT devices should use function modules to restrict access to system resources, which should only be granted to authorized entities.

Trusted computing bases (TCB) should be kept as small as possible to minimize the surface that is exposed to attackers and to reduce the probability that a bug or feature can be used to circumvent security protections.

Memory protection mechanisms such as memory safe languages, stack canaries, address space layout randomization (ASLR) and limited or no execute permissions are recommended wherever applicable.

5.2.5.2.2 Event logging

If capable, IoT devices should record sufficient details for each event to facilitate an authorized entity's ability to identify anomalous events and meaningfully analyse the associated data.

IoT devices and event logs should be synced with an authoritative system or passed to centralized repositories if the data has been appropriately de-identified.

5.2.5.2.3 Sensitive security parameters

The outcome of the risk assessment in 5.1.1 should help determine whether an IoT device may include hard-coded or shared sensitive security parameters, if such parameters are unique per device and not universal.

5.2.5.3 Additional information

5.2.5.3.1 General

Hardware-based solutions such as built-in crypto accelerators and dedicated hardware can enhance the use of cryptographic modules and cryptographic key protection capabilities to protect the data in storage and transit to meet the performance requirements. Physical countermeasures can support resistance to side-channel attacks. Such functions can include hardware-based root of trust (RoT). RoT is a foundational feature to provide platform integrity and ensure a foundation to develop and support the device's chain of trust. The root of trust is ideally based on a hardware-validated boot process to ensure the system can be started using code from an immutable source. As such, RoT is essential to enable platform attestation including for a verified boot process. When used to protect secrets and device correctness, hardware can support a foundational root of trust upon which rich software functionality can be implemented more securely and safely.

Compartments are protected by hardware-enforced boundaries to prevent a flaw or breach in one software compartment from propagating to other software compartments in the system. Compartmentalization introduces additional protection boundaries within the hardware and software stack to create additional layers of defence in depth. For example, a common technique is to use operating systems processes or independent virtual machines as compartments.

Integrity checking and recovery modes may not be appropriate in safety critical applications where continuous operation is essential.

5.2.5.3.2 Event logging

Implementation of event logging, including editing of logs, depends on device storage capabilities. IoT devices can support remote logging.

Trusted Platform Modules (TPMs) are one example of hardware roots of trust. They can support cryptographically bound device identification and interface access to help prevent unauthorized access and use of data. More information about TPMs can be found in ISO/IEC 11889-1.

5.2.6 Interface access

5.2.6.1 Requirements

5.2.6.1.1 IoT devices shall have mechanisms to limit logical access to its interfaces to authorized entities only.

5.2.6.1.2 IoT devices shall employ appropriate authentication and access control mechanisms.

5.2.6.1.3 Security and privacy requirements shall be assessed when designing and implementing the functions of IoT devices regarding creation and use of identifiers.

5.2.6.1.4 IoT devices shall ensure that common values for critical security parameters, such as global private keys or standard passwords, are replaced by values that are unique per device or explicitly defined by an appropriate external entity before they are put into operation.

NOTE The risk assessment is the basis of what is "appropriate" in this context.

5.2.6.2 Additional recommendation(s)

The IoT device should be capable of being logically identified. While identifiers can enable a host of cybersecurity controls (such as asset management, automatic device discovery, and software updates), creating or using persistent identifiers should be avoided unless such use is unavoidable. Where such uses arise, the existence of such identifiers should be made clear to users.

Mechanisms to limit logical access (to authorized entities) should be applied to the following:

a) the ability to enable or disable, through software or hardware means, any interfaces (including local and network interfaces);

b) the ability to restrict access (e.g. through authentication) to all remote interfaces;

c) the ability to identify or block devices not supported by an IoT device when it is attempting to access interfaces.

All input and output data should be validated for all kinds of interfaces. Data should be validated for length, character type, acceptable values or ranges, and message format.

IoT devices with remote interfaces that can be used to make configuration changes or that support administrative functions should implement measures to prevent common attack types.

Secure coding practices should be followed including use of a type-safe language. If this is not possible, the IoT device should still implement bounds checking and use safe typing and safe string handling functions.

IoT devices should support one or more mechanisms to limit access to interfaces based on types or groups of users.

Allow-lists (of characters or other token types) should be used instead of deny-lists when filtering data.

5.2.6.3 Additional information

5.2.6.3.1 General

Examples of user interfaces include administrative consoles, web pages, APIs or other externally-exposed IoT device interfaces. Injection, XML external entities, cross site scripting and insecure deserialization are examples of common attacks to remote interfaces.

Hardware-based capabilities can harden interface access protection against privilege escalation and control-flow attacks.

5.2.6.3.2 Identifiers

IoT devices can use identifiers in order to operate within an IoT system. Examples of such identifiers include serial numbers, cryptographic keys, and certificates.

NOTE Physical and logical identifiers can represent the same value.

Hardware-based root of trust can protect identifiers from unauthorized modification and can be used to generate device specific identifiers. Hardware can include important properties that can be used to support device security such as a single purpose hardware supporting the prevention of unintended actions performed by unauthorized entities.

IoT device developers can augment a unique logical identifier by provisioning a strong cryptographic device identity during deployment (or manufacturing) or using other mechanisms to authenticate the physical device involved in specific network based inbound or outbound activity.

5.2.7 Software and firmware updates

5.2.7.1 Requirements

5.2.7.1.1 If the IoT device supports software updates, updates shall be performed using a secure procedure.

5.2.7.1.2 Updates shall only be initiated by authorized entities.

NOTE Firmware is a specific type of software.

5.2.7.1.3 Unexpected interruption of an update shall leave the IoT device in a state that minimizes potential for harm, taking into account the risks of the IoT device not functioning as expected.

5.2.7.2 Additional recommendation(s)

Each update procedure should include the following:

a) a way to confirm the validity, authenticity and integrity of any update before installing it;

b) configuration options that include:

   1) whether automatic updates are enabled or disabled;

   2) for remote update procedures, whether update downloads and installations are automatically or manually initiated;

   3) for remote update procedures, a way of scheduling automatic downloads and installations;

   4) whether notification occurs when an update is available (and who/what is notified).

IoT devices should support automatic updates (in accordance with the requirements 5.2.7.1.1 to 5.2.7.1.3). IoT devices should have an update procedure that periodically checks whether a new security update is available, and if so, indicates this to the user.

IoT devices should ensure that the authenticity and integrity of software updates are verified prior to installing them. This can be performed using digital signatures and public key infrastructure. The update infrastructure, specifically the management of private keys, should be secure.

Leveraging the hardware root of trust-based capabilities to measure and verify the validity of the software and firmware updates should be considered.

Software updates should not impact the basic functioning of IoT devices, or where unavoidable, clear notification should be supplied to the user where an update will interrupt the functioning of an IoT device.

Software on IoT devices should be verified using secure boot mechanisms. If an unauthorized change is detected, the IoT device should alert the user or the local hub/IoT gateway to an issue. Further, the IoT device should terminate any network communication except to send the alert or initiate device recovery.

As part of secure development life cycle or similar, there should be a formal process for assessing either new, replaced, or modified components including firmware updates for material changes that can induce new risks or vulnerabilities.

5.2.7.3 Additional information

IoT devices can have safety relevant functions, and loss of those functions during an update can be an issue for some types of system if not considered and managed. Discarding an update or using a previous update can be used to recover from an interrupted update.

The software update procedure(s) can involve remote (e.g. network download) or local means (e.g. removable media or part replacement).

If the IoT device cannot directly communicate with the remote server, this functionality can be provided by a local hub/IoT gateway. The local hub can be configured to periodically check if new updates are available and, if they exist, download them.

Hardware replacement is a legitimate and acceptable way to perform an update.

5.2.8 User notifications

5.2.8.1 Information

It may be necessary or useful for IoT devices to notify users about to a variety of circumstances. There are several recommendations in this document that describe such circumstances. This clause is intended to provide information to support notifying IoT device users about a negative event or condition.

Some IoT devices do not have capabilities to actively inform the user (e.g. write a message on the screen, emit a sound or light), but they can respond with a message when queried or accessed remotely. IoT devices that do not have capabilities to directly inform users can send notifications and alerts via a local hub. A user query can be as simple as trying to access the device with a browser, mobile application, or something more complex. Alternatively, IoT devices can send a message to an alarm, monitoring, or logging device within the IoT system.

Annex A
(informative)

Risk management guidance

A.1 General

The guidance provided in ISO 31000:2018, 6.4.1 applies. IoT security and privacy risks should be identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization.

A.2 Risk identification

Risk assessment consists of risk identification, risk analysis and risk evaluation. The guidance provided in ISO 31000:2018, 6.4.2 applies. When identifying security and privacy risks of IoT devices, various risk sources should be considered. These risk sources depend on the nature of the IoT device and its applications.

A.3 Risk analysis

The guidance provided in ISO 31000:2018, 6.4.3 applies. Risk analysis may be undertaken in varying degrees of detail depending on the criticality of the values or previously identified assets of the organization, the extent of adverse and positive impacts that are already known, and any accrued knowledge, or experience including incidents (history) involving the organization.

A.4 Risk evaluation

The guidance provided in ISO 31000:2018, 6.4.4 applies. Once the risks have been identified and assigned likelihood and severity of consequence values, organizations should apply their risk acceptance criteria to determine whether or not the risks are acceptable. If they are not acceptable, then they should be prioritized for treatment.

A.5 Risk treatment

The guidance provided in ISO 31000:2018, 6.5.1 and 6.5.2 applies. Risk treatment options defined by the organization should consider the objectives of the organization, contractual, legal and regulatory requirements and the views of relevant interested parties. Risk treatment options may include:

— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

— undertake further analysis to better understand the risk;

— reconsider objectives;

— removing the risk source;

— sharing the risk (e.g. through contracts, buying insurance);

— retaining the risk by informed decision.