IPA

JST-CR-01-01-2024

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements（JC-STAR）

★1 Level Conformance Criteria and Assessment Method

September 2024

Information-technology Promotion Agency, Japan

Security Requirement		☆1 Security Requirement	☆1 Conformance Criteria #	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
1. No vulnerable authentication/authorization mechanism (e.g., universal default passwords, vulnerable passwords)	1-2. Where pre-installed unique passwords are used, these shall be sufficiently randomized against automated attacks.	✓	2	For IoT products that use passwords or passcodes in the user authentication mechanism via a network against the IoT products or in the client authentication mechanism at initial setup of the IoT device, either of the following criteria (1) or (2) shall be met when default passwords are used at the time of IoT product installation: (1) The default password shall be unique per IoT device and shall be at least 6 characters long and not easily guessable. (2) The IoT product shall implement a function that requires the user to change the default password at initial started up, and shall force the user to set a password of 8 or more characters as a password that can be set in such function.	Conditions for N/A: No mechanism for user authentication using password or passcode via a network (Provide rationale as to why user authentication using password or passcode is not necessary to counter threats in "Reasons for N/A")	Document: (1) (2) Device check: None	[ETSI EN 303 645]5.1-2 M C (2) [UK: PSTI Act]SCHEDULE 1: 1-(3) [Singapore: CLS][＊]5.1-2 [IEC 62443-4-2]CR1.7	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (2) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 2) [JISEC-C0755]FMT_IPWD_EXT
1. No vulnerable authentication/authorization mechanism (e.g., universal default passwords, vulnerable passwords)	1-3. Authentication mechanisms used to authenticate users against the product shall use technologies that reduce the assumed risks appropriate to the properties of the product usage etc.	✓	1	Access to information assets to be protected by users or other IoT devices via IP communications against IoT products shall be made by access control based on appropriate authentication mechanisms. ** **IoT products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (IoT products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for the [A] Mark)".)	Conditions for N/A: No mechanism for authentication and access via IP communications for access to information assets to be protected (Provide rationale as to why authentication and access are not necessary to counter unauthorized external access in "Reasons for N/A") Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device.	Document : Yes Device check: None	[ETSI EN 303 645]5.1-3 M [UK: PSTI Act]SCHEDULE 1: 1-(3) [US: NISTIR 8425]Interface Access Control2-b [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-3 [IEC 62443-4-2]CR1.5	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 4), 1-2 Data Protection[Mandatory] 3) [RBSS]Certification Standard for Security Camera 5.2.12 (2), Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2) [JISEC-C0755]FIA_UAU, FMT_SMR
1. No vulnerable authentication/authorization mechanism (e.g., universal default passwords, vulnerable passwords)	1-4. For user authentication against the product, the products shall provide to the user or an administrator a simple mechanism to change the authentication value used.	✓	3	Enables changing the authentication value for user authentication via a network against the IoT product, regardless of authentication type (password, token, fingerprint, etc.).	Conditions for N/A: No mechanism for user authentication via a network (Provide rationale as to why user authentication is not necessary to counter unauthorized external access in "Reasons for N/A") Definition of term: "authentication value" The individual value of an attribute used by the authentication mechanism to the IoT product. (e.g., for a password-based authentication mechanism, the authentication value is a string of characters. In the case of biometric fingerprint authentication, the authentication value is, for example, the fingerprint data of the index finger of the left hand).	Document: Yes Device check: None	[ETSI EN 303 645]5.1-4 M C (8) [Singapore: CLS][＊]5.1-4 [IEC 62443-4-2]CR1.5	[CCDS Certification]1-1-2 Change of credentials [Mandatory] 1) [BMSec]IA-2 [RBSS]Certification Standard for Digital Recorder（Security Uses） 5.2.12 (2) [JISEC-C0755]FMT_IPWD_EXT
1. No vulnerable authentication/authorization mechanism (e.g., universal default passwords, vulnerable passwords)	1-5. When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via a network impracticable.	✓	4	When the IoT device is not a constrained device, the user authentication mechanism via a network against the IoT device shall be a mechanism which makes brute-force attacks difficult.	Conditions for N/A: One of the following conditions applies. (OR Condition) ・There is no mechanism for user access to the equipment via a network against IoT device (Provide a rationale as to why user access is not necessary to counter unauthorized external access in "Reasons for N/A") ・The IoT device falls under the category of "restricted equipment" (Provide evidence that the device falls under the category of "restricted equipment" in "Reasons for N/A") Definition of term: "constrained device" A device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use. (For examples of IoT device, refer to "Terms.")	Document: None Device check: Yes	[ETSI EN 303 645]5.1-5 M C (5) [EU: CRA]ANNEX I 1.(3)(b) [Singapore: CLS][＊]5.1-5 [IEC 62443-4-2]CR1.11	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (1) [CCDS Certification]1-1 Access Control and Authentication [Mandatory] 3) [BMSec]IA-3 [JISEC-C0755]FIA_AFL

Security Requirement		☆1 Security Requirement	☆1 Conformance Criteria #	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
2. Managing vulnerability reports	2-1. The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.	✓	5	The manufacturer shall make a vulnerability disclosure policy publicly available (e.g. post on the manufacturer's website) that includes all of the following information (1) through (3). (1) Contact information for the reporting of IoT product security issues to the manufacturer (e.g. manufacturer's website URL, phone number, email address) (2) Procedures to be followed by the manufacturer after receipt of a report on the security of the IoT product and an outline of such procedures. (3) Any procedures regarding IoT product and vulnerability status updates until the vulnerability is resolved, and an outline of such procedures.	–	Document: (1) (2) (3) Device check: None	[ETSI EN 303 645]5.2-1 M [UK: PSTI Act]SCHEDULE 1: 2-(2), 2-(3) [US: NISTIR 8425]Information & Query Reception1, 1-a, 1-b, Product Education & Awareness [EU: CRA]ANNEX I 2.(5), ANNEX I 2.(6), ANNEX II 1, ANNEX II 2 [Singapore: CLS][＊]5.2-1 [IEC 62443-4-1]DM-1	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 1) [BMSec] FR-1
3. Keep software updated	3-1. Particular software components included in products shall be updateable.	✓	6	All of the following criteria (1) through (3) shall be met for the update function of the software components included in the IoT product. ** (1) The firmware (software) package of the IoT product shall be updateable. (2) The firmware (software) package shall have a means to confirm that the latest firmware (software) is installed, such as being able to check the version of the firmware (software) package. (3) The version of the firmware (software) package that has been updated shall be kept up-to-date even after power-off. **IoT products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (IoT products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for the [A] Mark)".)	–	Document: None Device check: (1) (2) (3)	[ETSI EN 303 645]5.3-1 R [US: NISTIR 8425]Software Update 1 [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊＊＊]CK-LP-03 [IEC 62443-4-1]SM-6, SUM-1 [IEC 62443-4-2]CR4.3, CR3.10 EDR3.10, HDR3.10 NDR 3.10	[CCDS Certification]1-3 Software Update [Mandatory] 1) [Recommended] 1) [BMSec]PT-1 [JISEC-C0755]FMT_SMF
3. Keep software updated	3-3. When the product implements an update mechanism, the update shall be simple for the user to apply.	✓	7	The product enables users to perform software updates in a simple and understandable procedure when applying updates.	–	Document: Yes Device check: None	[ETSI EN 303 645]5.3-3 M C (12) [EU: CRA]ANNEX I 2.(8) [Singapore: CLS][＊]5.3-3 [IEC 62443-4-1]SUM-4	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (3) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-7. When the product implements an update mechanism, the product shall use best practice cryptography to facilitate secure update mechanisms.	✓	8	When updating software via a network, there shall be a mechanism to verify the software integrity prior to updating.	Conditions for N/A: No mechanism for updating software via a network (Describe the expected update mechanism in "Reasons for N/A")	Document: Yes Device check: None	[ETSI EN 303 645]5.3-7 M C (12) [US: NISTIR 8425]Software Update 1 [Singapore: CLS][＊]5.3-7 [IEC 62443-4-2]CR4.3	[CCDS Certification]1-3 Software Update [Recommended] 2) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-8. When the product implements an update mechanism, security updates shall be timely.	✓	9	The manufacturer shall document policies and guidelines for prioritizing security updates to achieve rapid updates to security issues.	–	Document: Yes Device check: None	[ETSI EN 303 645]5.3-8 M C (12) [EU: CRA]ANNEX I 2.(2), ANNEX I 2.(7), ANNEX I 2.(8) [Singapore: CLS][＊]5.3-8 [IEC 62443-4-1]SUM-5	[CCDS Certification]2-1 Contact point and security support system [Mandatory] 2) [BMSec]PT-1 b)-4), e)-1) [JISEC-C0755]FMT_SMF
3. Keep software updated	3-14. The model designation of the products shall be clearly recognizable, either by labelling on the product or via a physical interface.	✓	10	The model number of the IoT product shall be provided to the users in any of the following ways. (1) The model number of the IoT product shall be written directly on the IoT product itself. (2) Users shall be able to recognize the model number from the GUI, web UI, etc. of the IoT product, or from the GUI, web UI, etc. of software or applications (e.g., smartphone applications) attached to the product.	–	Document: None Device check: (1) or (2)	[ETSI EN 303 645]5.3-16 M [US: NISTIR 8425]Information Dissemination 2 [EU: CRA]ANNEX II 3 [Singapore: CLS][＊]5.3-16	
4. Securely store sensitive parameters	4-1. Sensitive security parameters in the product’s storage shall be stored securely by the product.	✓	11	Information assets to be protected that are stored in IoT product storage (including information assets to be protected that are stored in storage media such as SD cards, etc.) shall be securely stored against unauthorized access except spoofing attack via a network.	Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device.	Document: Yes Device check: None	[ETSI EN 303 645]5.4-1 M [US: NISTIR 8425]Data Protection 1, Interface Access Control 2-a [Singapore: CLS][＊＊]5.4-1 [IEC 62443-4-2]CR1.5, CR1.9, CR1.14, CR3.8, CR4.1, CR3.12 EDR3.12 HDR3.12 NDR3.12, CR3.13 EDR3.13 HDR3.13 NDR3.13	[CCDS Certification]1-2 Data Protection[Mandatory] 1) 3) [JISEC-C0755]FMT_MTD

Security Requirement		☆1 Security Requirement	☆1 Conformance Criteria #	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
5. Communicate securely	5-1. The product shall use best practice cryptography to communicate securely.	✓	12	For information assets to be protected that are transmitted via a network, one of the following protection measures against information eavesdropping shall be implemented. (1) For information assets to be protected that are transmitted via a network to other IoT devices or servers (including servers in the cloud), the IoT device themselves shall take protective measures against information eavesdropping. (2) For information assets to be protected that are transmitted via a network to other IoT devices or servers (including servers in the cloud), the information assets shall be transmitted only in a protected communication environment (VPN environment or connection environment via leased line).	Conditions for N/A: No information assets to be protected are transmitted via a network. (Provide evidence that there are no information assets to be protected transmitted via a network in "Reasons for N/A") Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device.	Document: (1) or (2) Device check: None	[ETSI EN 303 645]5.5-1 M [US: NISTIR 8425]Data Protection 3 [EU: CRA]ANNEX I 1.(3)(c) [Singapore: CLS][＊＊]5.5-1 [IEC 62443-4-2]CR3.1, CR4.3	[CCDS Certification]1-2 Data Protection[Mandatory] 2), 1-4-1 Wi-Fi authentication method [Mandatory] 1), 1-4-2 Bluetooth vulnerability countermeasures [Mandatory] 1) [BMSec]TP-1
6. Minimize exposed attack surfaces	6-1. All unused network physical interfaces and logical interfaces shall be disabled.	✓	13	In order to reduce the risk of external cyberattacks, interfaces that are unnecessary for the use of the IoT product and are at risk of being attacked shall be disabled, and vulnerability assessments shall be performed on the IoT product. Specifically, all of the following criteria (1) and (2) shall be met. (1) For the following interfaces that are used frequently in the IoT product and are assumed to be at risk such as via a vulnerability, the interfaces that are unnecessary for the use of the IoT product and are at risk of being attacked shall be disabled. A) TCP/UDP port B) Bluetooth C) USB (2) The IoT product shall be inspected for known vulnerabilities by vulnerability scanning tools and vulnerabilities that could be exploited shall not be detected.	–	Document: (1) Device check: (1) (2) **(1) requires both document and device check However, for device check, if there is no recommended vulnerability testing tool, it shall be excluded (document check only).	[ETSI EN 303 645]5.6-1 M [US: NISTIR 8425]Interface Access Control 1-a [EU: CRA]ANNEX I 1.(3)(h) [Singapore: CLS][＊＊]5.6-1 [IEC 62443-4-2]CR7.7	[CCDS Certification]1-1-1 Disabling of TCP/UDP ports [Mandatory] 1) [BMSec]NI-1, VA-1, VA-2, VA-3
9. Resilience to outages	9-1. Resilience shall be built into the products and services, taking into account the possibility of outages of data networks and power.	✓	14	When the power supply and network functions are restored after the IoT device is turned off due to a power or network outage, the settings of authentication values (passwords, secret keys, etc.) used for access control and the software that has been updated shall maintain the state immediately before the power-off, without returning to the factory default state. **IoT products that have received certification for conformity to the technical regulations specified in the Telecommunications Business Act including the Technical Standards for Terminal Equipment Security (IoT products to which the Technical Standards Conformity T Mark or A Mark is affixed) shall be deemed to conform to this criteria. (In this case, enter the Technical Standards Conformity Approval number etc. based on the Telecommunications Business Law in the "Basic Information" sheet (the Design Certification number for the Technical Standards Conformity T Mark or the Technical Standards Conformity Approval number for the [A] Mark)".)	–	Document: None Device check: Yes	[ETSI EN 303 645]5.9-1 R [EU: CRA]ANNEX I 1.(3)(f) [IEC 62443-4-2]CR7.1, CR7.3	[MIC: Ordinance Concerning Terminal Facilities, etc.]Article 34-10 (4) [CCDS Certification]1-1 Access Control and Authentication [Mandatory]⑤
11. Delete user data	11-1. The user shall be provided with functionality such that user data can be erased from the product in a simple manner.	✓	15	All of the following criteria (1) and (2) shall be met for the delete function of data stored in IoT product storage during the use of the IoT product. (1) The user can delete at least the following data related to the user via the IoT device itself or associated services (such as a mobile application) A) information assets (including personal information) obtained during the use of the IoT product B) user configuration values C) authentication values set by user, cryptographic keys and digital signatures obtained during use of the IoT product (2) The updated version of firmware (software) package related to security features shall be maintained after data deletion	–	Document: (1) Device check: (1) (2) **(1) requires both document and device check	[ETSI EN 303 645]5.11-1 M [US: NISTIR 8425]Data Protection 2 [Singapore: CLS][＊＊]5.11-1 [IEC 62443-4-2]CR4.2	[CCDS Certification]1-2-1 Data erasure function [Mandatory] 1) [BMSec]MT-2 [JISEC-C0755]FMT_MTD

Security Requirement		☆1 Security Requirement	☆1 Conformance Criteria #	☆1 Conformance Criteria	Conditions for N/A (Non-applicable), Supplementary Explanation	☆1 Evaluation Method	[Ref.] Existing schemes/documents of other countries	[Ref.] Existing domestic schemes/documents
Category	Requirement							
17. Provide information on products	17-2. The manufacturer shall provide users with guidance on how to securely set up, use and dispose of their products.	✓	16	The manufacturers shall meet all of the following criteria (1) through (5) to provide information regarding the cybersecurity of IoT products. (1) The procedures for safe use of the IoT product, such as initial setup procedures, and other settings and usage procedures that may affect cybersecurity in the use of the product, shall be made known to the public. (2) They shall have the procedures to inform customers of the content and necessity of the IoT product security update and the consequence of not updating the IoT product for each security update release. (3) They shall make disclaimers known of accidents or failures that can be expected if updates are not made, and of accidents or failures that can generally be expected. (4) They shall make known the policy when the support for the target product or service expires or is terminated. (5) They shall make known the assumed risk associated with disposal or resale of the IoT product with residual information assets to be protected, and how to safely terminate use of the IoT product, including data removal.	Definition of term: "information assets to be protected" include all of the following information ・Configuration information related to communication functions ・Configuration information related to security functions ・Information that is generally sensitive, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device.	Document: (1) (2) (3) (4) (5) Device check: None	[ETSI EN 303 645]5.12-2 R [US: NISTIR 8425]Documentation 1-a, 1-d, Product Education & Awareness 1-a, Information Dissemination 2 [EU: CRA]ANNEX II 4, ANNEX II 9 [IEC 62443-4-1]SUM-2	[CCDS Certification]2-3 Provision of information to users [Mandatory] 1) [BMSec]PT-1, TP-1

*The Security Requirements (1-1 to 2-3, 3-1 to 3-14, 4-1 to 5-8, 6-1 to 6-9, 7-1 to 9-3, 10-1, 11-1 to 12-2, 13-1 to 14-5, 17-2 to 17-4, 17-8, 18-5) within this document are extracted from the ETSI EN 303 645 ©European Telecommunications Standards Institute 2020. Further use, modification, copy and/or distribution are strictly prohibited.
*Republished courtesy of the National Institute of Standards and Technology.

Term	Definition
administrator	user who has the highest-privilege level possible for a user of the device, which can mean they are able to change any configuration related to the intended functionality
associated services	digital services that, together with the device, are part of the overall IoT product and that are typically required to provide the product's intended functionality EXAMPLE 1: Associated services can include mobile applications, cloud computing/storage and third party Application Programming Interfaces (APIs). EXAMPLE 2: A device transmits telemetry data to a third-party service chosen by the device manufacturer. This service is an associated service.
authentication mechanism	method used to prove the authenticity of an entity NOTE: An "entity" can be either a user or machine. EXAMPLE: An authentication mechanism can be the requesting of a password, scanning a QR code, or use of a biometric fingerprint scanner.
authentication value	individual value of an attribute used by an authentication mechanism EXAMPLE: When the authentication mechanism is to request a password, the authentication value can be a character string. When the authentication mechanism is a biometric fingerprint recognition, the authentication value can be the index fingerprint of the left hand.
best practice cryptography	cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques NOTE 1: This does not refer only to the cryptographic primitives used, but also implementation, key generation and handling of keys. NOTE 2: Multiple organizations, such as SDOs and public authorities, maintain guides and catalogues of cryptographic methods that can be used. EXAMPLE: The device manufacturer uses a communication protocol and cryptographic library provided with the IoT platform and where that library and protocol have been assessed against feasible attacks, such as replay.
configuration settings	set of parameters that can be changed in hardware, software, or firmware that affect the security posture and function of an information system

Term	Definition
constrained device	device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use NOTE 1: Physical limitations can be due to power supply, battery life, processing power, physical access, limited functionality, limited memory or limited network bandwidth. These limitations can require a constrained device to be supported by another device, such as a base station or companion device. EXAMPLE 1: A window sensor's battery cannot be charged or changed by the user; this is a constrained device. EXAMPLE 2: The device cannot have its software updated due to storage limitations, resulting in hardwarereplacement or network isolation being the only options to manage a security vulnerability. EXAMPLE 3: A low-powered device uses a battery to enable it to be deployed in a range of locations. Performing high power cryptographic operations would quickly reduce the battery life, so it relies on a base station or hub to perform validations on updates. EXAMPLE 4: The device has no display screen to validate binding codes for Bluetooth pairing. EXAMPLE 5: The device has no ability to input, such as via a keyboard, authentication information. NOTE 2: A device that has a wired power supply and can support IP-based protocols and the cryptographic primitives used by those protocols is not constrained. EXAMPLE 6: A device is mains powered and communicates primarily using TLS (Transport Layer Security).
consumer	natural person who is acting for purposes that are outside her/his trade, business, craft or profession NOTE: Organizations, including businesses of any size, use consumer IoT. For example, Smart TVs are frequently deployed in meeting rooms, and home security kits can protect the premises of small businesses.
critical security parameter	security-related secret information whose disclosure or modification can compromise the security of a security module EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.
debug interface	physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality EXAMPLE: Test points, UART, SWD, JTAG.
defined support period	minimum length of time, expressed as a period or by an end-date, for which a manufacturer will provide security updates NOTE: This definition focuses on security aspects and not other aspects related to product support such as warranty.
external sensing capabilities	element or device that collects information on an object and converts it into signals that can be handled by a machine EXAMPLE: An external sensing capability can be an optic or acoustic sensor.
factory default	state of the device after factory reset or after final production/assembly NOTE: This includes the physical device and software (including firmware) that is present on it after assembly.
hard-coded unique per device identity	value unique to each device written directly in the source code EXAMPLE: A master key used for network access that is unique to the device
initialization	process that activates the network connectivity of the device for operation and optionally sets authentication features for a user or for network access

Term	Definition
initialized state	state of the device after initialization
IoT device / device	network-connected (and network-connectable) device that has relationships to associated services NOTE 1: IoT devices are commonly also used in business contexts. These devices remain classified as consumer IoT devices. NOTE 2: IoT devices are often available for the consumer to purchase in retail environments. IoT devices can also be commissioned and/or installed professionally.
IoT product / product	IoT device and its associated services
isolable	able to be removed from the network it is connected to, where any functionality loss caused is related only to that connectivity and not to its main function; alternatively, able to be placed in a self-contained environment with other devices if and only if the integrity of devices within that environment can be ensured EXAMPLE: A Smart Fridge has a touchscreen-based interface that is network-connected. This interface can be removed without stopping the fridge from keeping the contents chilled.
logical interface	software implementation that utilizes a network interface to communicate over the network via channels or ports
manufacturer	relevant economic operator in the supply chain (including the device manufacturer) NOTE: This definition acknowledges the variety of actors involved in the IoT ecosystem and the complex ways by which they can share responsibilities. Beyond the device manufacturer, such entities can also be, for example and depending on a specific case at hand: importers, distributors, integrators, component and platform providers, software providers, IT and telecommunications service providers, managed service providers and providers of associated services.
network interface	physical interface that can be used to access the functionality of IoT via a network
owner	user who owns or who purchased the device
personal data	any information relating to an identified or identifiable natural person NOTE: This term is used to align with well-known terminology but has no legal meaning within the present document.
physical interface	physical port or air interface (such as radio, audio or optical) used to communicate with the device at the physical layer EXAMPLE: Radios, ethernet ports, serial interfaces such as USB, and those used for debugging.
public security parameter	security related public information whose modification can compromise the security of a security module EXAMPLE 1: A public key to verify the authenticity/integrity of software updates. EXAMPLE 2: Public components of certificates.
remotely accessible	intended to be accessible from outside the local network
security module	set of hardware, software, and/or firmware that implements security functions EXAMPLE: A device contains a hardware root of trust, a cryptographic software library that operates within a trusted execution environment, and software within the operating system that enforces security such as user separation and the update mechanism. These all make up the security module.
security update	software update that addresses security vulnerabilities either discovered by or reported to the manufacturer NOTE: Software updates can be purely security updates if the severity of the vulnerability requires a higher priority fix.
self-contained environment	environment that can be used independently of other services

Term	Definition
sensitive personal data	data whose disclosure has a high potential to cause harm to the individual What is to be treated as "sensitive personal data" varies across products and use cases, but examples are: video stream of a home security camera, payment information, content of communication data and timestamped location data. Carrying out security and data protection impact assessments can help the manufacturer make appropriate choices.
sensitive security parameters	critical security parameters and public security parameters
software service	software component of a device that is used to support functionality EXAMPLE: A runtime for the programming language used within the device software or a daemon that exposes an API used by the device software, e.g. a cryptographic module's API.
storage	medium that stores data or information and from which data or information can be retrieved
technical document	document that describes technical specifications that are referenced in the assessment procedure and that serves as a basis for demonstrating conformity to the conformity criteria, such as product design documents, specifications, development procedures, manuals, etc., or documents that are formulated based on these documents The classification of public or closed is not required, and can be selected based on the applicant's own judgment. The description of technical specifications in formats used in other standards or in free formats is also acceptable.
telemetry	data from a device that can provide information to help the manufacturer identify issues or information related to device usage EXAMPLE: An IoT device reports software malfunctions to the manufacturer enabling them to identify and remedy the cause.
unique per device	unique for each individual device of a given product class or type
user	natural person or organization
zone	Each entity in which the system of interest is divided based on functional, logical, and physical (including location) relationships
zone perimeter	boundary between zones