JST-CR-01-01-2024R1

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements (JC-STAR) STAR-1 Conformance Requirements and Assessment Methods

December 2024

Information-technology Promotion Agency, Japan (IPA)

Table of Contents

1. Introduction

The JC-STAR (Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements) is a Japanese scheme to confirm and visualize conformance of IoT products to conformance requirements based on its own conformance requirements (security technical requirements), in harmony with ETSI EN 303 645, NISTIR 8425, and other standards. For details of the scheme, refer to the following:

Scheme details (in English): https://www.ipa.go.jp/en/security/jc-star/index.html

JC-STAR has set four levels of security technology requirements in accordance with the required security level: STAR-1 conformance requirements and assessment procedures for products to respond to the minimum level of threats, and STAR-2 to STAR-4 conformance requirements and assessment procedures for each type of IoT product. This document describes the **“Conformance Requirements for STAR-1.”**

Table 1: Positioning of Requirement Levels in JC-STAR

Level	Positioning	Conformance Requirements	Assessment Method
STAR-4	Generic security requirements for each **product type** for **use in critical systems of government agencies, critical infrastructure providers, local governments, and large enterprises**, and an **independent third party's evaluation to show that the** requirements are met.	By product type	Third-party certification
STAR-3			
STAR-2	Basic security requirements that should be added to STAR-1 **in consideration of the characteristics of each product type**, and a self-**declaration by the product vendor that** it satisfies the requirement.		Self-declaration of conformance
STAR-1	**Minimum security** requirements commonly required for **a product**, and a self-declaration by the **product vendor that** it satisfies these requirements.	Common product type	

1.1 What is a Conformance Label?

A conformance label **indicates that an IoT product has achieved the minimum level of security functionality required** to counter the threats anticipated by the conformance requirements and assessment criteria for conformance. In order to promote the fact that their IoT products have already acquired a conformance label, IoT product vendors can include, attach, or use the conformance label on the product itself, packaging, instruction manuals, brochures, websites, etc., and this will allow them to appeal their security measures to procurers and purchasers.

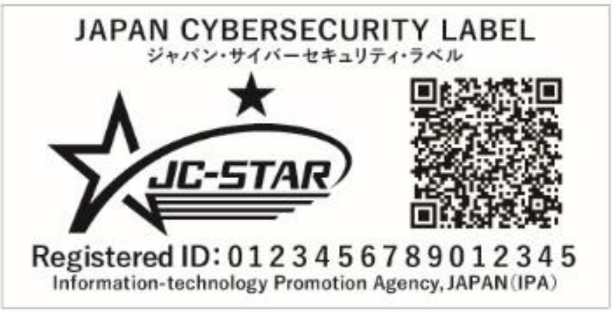

JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
JC-STAR
Registered ID: 012345678901234 5
Information-technology Promotion Agency, JAPAN (IPA)

Figure 1: STAR-1 conformance label

The following points shall be considered when acquiring and maintaining the conformance label:

- The conformance label is an indication of conformance with stipulated conformance requirements but does not assure complete and total security.

- STAR-1 and STAR-2 are a self-declaration of conformance method whereby IPA grants a conformance label based on a checklist describing the results of self-assessment conducted by IoT product vendors in accordance with the conformance criteria and assessment procedures specified in this Scheme. IPA does not check whether the vendor conforms to the conformance requirements at the time the conformance label is issued. In other words, the reliability of the assessment depends on the vendor's reliability.

- STAR-3 and STAR-4 are intended for products for government agencies, critical infrastructure providers, etc., and are certified by IPA, based on evaluation reports from independent third-party evaluation bodies, and a conformance label is attached to ensure a higher level of reliability.

- The obligation to store evidence shall be imposed on IoT product vendors.

On the other hand, in the case of labeled products where there are any doubts about the conformance of a labeled product to the conformance requirements, IPA has the right to conduct ex-post inspections and surveillance, and if necessary, IPA may request the submission of evidence, the re-implementation and reporting of conformance assessment. IPA also balances credibility by including a mechanism whereby the label of conformance may be revoked depending on the results of the surveillance.

In addition to the level of conformance label and registered ID acquired by the IoT product, the conformance label will incorporate **a two-dimensional barcode** that embeds the URL of the IoT product information page (for each labeled product) managed by IPA to confirm the IoT product information. The product information page incorporates a mechanism to provide a wide scope of information on IoT products with a conformance label, including applicant information, product information, conformance label information, security information (update information, vulnerability information, etc.), and contact information, in a one-dimensional format while keeping the information up to date.

Table 2: Status Indication with Conformance Label Information

Status of conformance label	**Summary**
Active	The conformance label is within the validity period and there are no grounds for withdrawal or revocation.

Deferral of expiration (Extension procedure in progress)	The validity period of the conformance label has expired, but the application procedure for the extension of the validity period is in process.
Expired	The validity period of a conformance label has expired and has not been extended.
Withdrawn	A condition in which a conformance label has been withdrawn by the IoT product vendor at the request of the IoT product vendor during the validity period of the conformance label.
Revoked	A state in which IPA mandatorily suspends the validity of a conformance label when an event that constitutes grounds for revocation of a conformance label occurs during the validity period of the label and no corrective action is taken to resolve the event within a specified period.

1.2 Scope of Acquisition of a Conformance Label

The scope of products that can acquire a conformance label is the **"IoT products"** that meet the following conditions and have a function for sending and receiving data using the Internet Protocol (IP). If a product can use the IP, it is eligible even if it cannot connect directly to the Internet, as long as it can connect to another device to connect to the Internet. On the other hand, "systems" are not covered at this point.

- "IoT products" are those that are sold by suppliers or purchased by users, and refer to either a single **"IoT device"** or a set that is composed of an **"IoT device"** and **"associated services"** that are used to achieve the intended purpose.

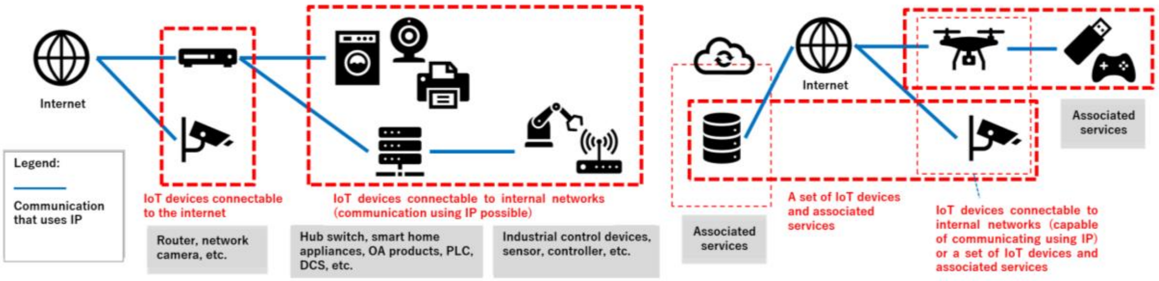

Internet
Legend:
Communication that uses IP
IoT devices connectable to the internet
Router, network camera, etc.
IoT devices connectable to internal networks (communication using IP possible)
Hub switch, smart home appliances, OA products, PLC, DCS, etc.
Industrial control devices, sensor, controller, etc.
Associated services
Internet
A set of IoT devices and associated services
Associated services
IoT devices connectable to internal networks (capable of communicating using IP) or a set of IoT devices and associated services

Figure 2: Scope of Conformance Label

- An "IoT device" means an Internet-capable device that can send and receive data using the Internet Protocol (IP) and for which it is difficult for the user to easily add security software to the IoT device itself by installing software products or other means.

- "Associated services" refer to digital services that must be provided in conjunction with an IoT device for the IoT product to provide its intended purpose. It is provided in conjunction with the IoT device when the IoT device itself alone cannot provide the purpose intended by the IoT product.

- An "internal network" refers to a network separated from the Internet by gateways, firewalls, etc.

1.3 Flow of STAR-1 to Grant a Conformance Label based on the Self-declaration of Conformance

The procedure differs depending on the level of conformance label for which the application is made.

<Procedures>

1. IoT product vendor conducts its own assessment and create a checklist in accordance with the conformance requirements and assessment procedures for STAR-1, in order to demonstrate that the IoT product for which a conformance label is to be acquired meets the required security requirements. If necessary, the vendor may request an external JC-STAR evaluation body or JC-STAR assessment body to conduct the evaluation.

2. IoT product vendor submits a label application to IPA with the prepared checklist. Note that while it is not necessary to submit a trail to IPA when submitting the checklist, the vendor is obligated to keep the trail during the validity period of the checklist.

3. IPA, together with the Ministry of Economy, Trade and Industry (METI), will accept the label application after conducting the necessary verification work.

4. If the application is accepted, the IoT product vendor pays a new application fee to IPA.

5. IPA will grant a conformance label for its IoT products[1].

1.4 Validity period of STAR-1

The validity period is two years from the date of issuance of the conformance label (or a validity period of less than two years can be set upon application). If the applicant wishes to extend the validity period, an application for extension based on the self-declaration of conformance must be submitted again, and if the application is approved, the validity period will be extended for two years (or an extension for less than two years can be set upon application). Even if there is a major revision of the conformance requirements during the validity period (addition of items or major changes in the conformance requirements) and the grace period (transition period during which the old version is kept along with the new version) ends, the label will not expire in the middle of the validity period.

However, if there is a change in the security specifications of the IoT product at a level that affects the self-declaration of conformance assessment during the validity period, the IoT product vendor must confirm the change by itself and report it to IPA, at which point the conformance label will expire (treated as a voluntary withdrawal).

[1] For applications to acquire a label, IPA makes inquiries to relevant government agencies, including the Ministry of Economy, Trade and Industry (METI), regarding supply chain risks before issuing the label, and grants a label based on the results of such inquiries.

2. Concept of Conformance Requirement, etc.

2.1 Structure of Conformance Requirements, etc.

STAR-1 conformance requirements consist of three parts: “**STAR-1 Security Requirement,” “STAR-1 Conformance Requirements,”** and **“STAR-1 Assessment Procedure**.”

- “STAR-1 Security Requirements” are security requirement that should be equipped as STAR-1 security functions of IoT products to counter the threats, information assets to be protected, etc., considering the threats, information assets to be protected, etc., assumed in STAR-1. Note that STAR-1 is not focused on a specific product type but is a unified standard for a wide scope of IoT products to address a minimum level of threats.

- “STAR-1 Conformance Requirements” are established as standards to which IoT products must conform to comply with STAR-1 security requirements. For each of the target security requirements, the specific minimum level that must be met in order to be recognized as having STAR-1 security functions.

- “The STAR-1 Assessment Procedure” is a procedure (consisting of the Assessment Method and Assessment Guide) for assessment and conformance decision on whether the security functions provided in an IoT product conform to STAR-1 conformance requirements. The assessor needs to conduct the assessment in accordance with this Assessment Procedure.

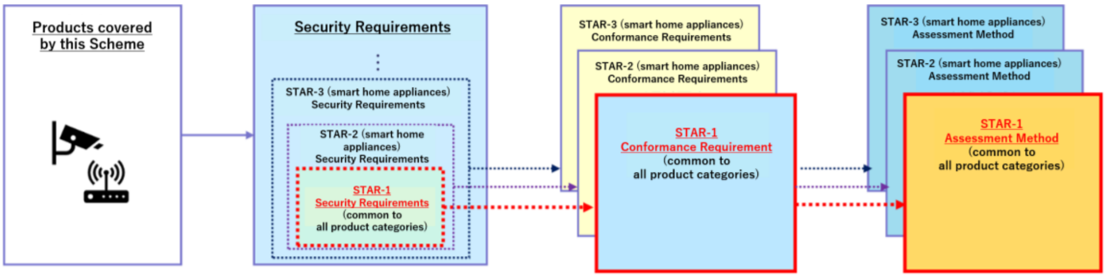

Products covered by this Scheme
Security Requirements
STAR-3 (smart home appliances) Security Requirements
STAR-2 (smart home appliances) Security Requirements
STAR-1 Security Requirements (common to all product categories)
STAR-3 (smart home appliances) Conformance Requirements
STAR-2 (smart home appliances) Conformance Requirements
STAR-1 Conformance Requirement (common to all product categories)
STAR-3 (smart home appliances) Assessment Method
STAR-2 (smart home appliances) Assessment Method
STAR-1 Assessment Method (common to all product categories)

Figure 3: STAR-1 Structure of Conformance Requirements, etc.

The security requirements (overall set) are based on the relationships between the sets of domestic and international security requirements, such as ETSI EN 303 645, NISTIR 8425, and EU-CRA, with a view to achieving mutual recognition in the future, and the requirements that are in an overlapping relationship (∪) are organized as the overall set of security requirements (long list) that may be required for IoT products covered by this Scheme.

2.2 Positioning of STAR-1

STAR-1 requires that the following three points be achieved at a minimum:

- Conformance to the STAR-1 Conformance Requirements **allows minimal threat protection**.

    - A uniform standard to address a minimum set of threats for a broad scope of IoT products, rather than focusing on a specific product type.

- Assessment of STAR-1 Conformance Requirements **can be handled at low cost through self-declaration of conformance.**

    - Self-declaration of conformance by the IoT product vendor itself is permitted.

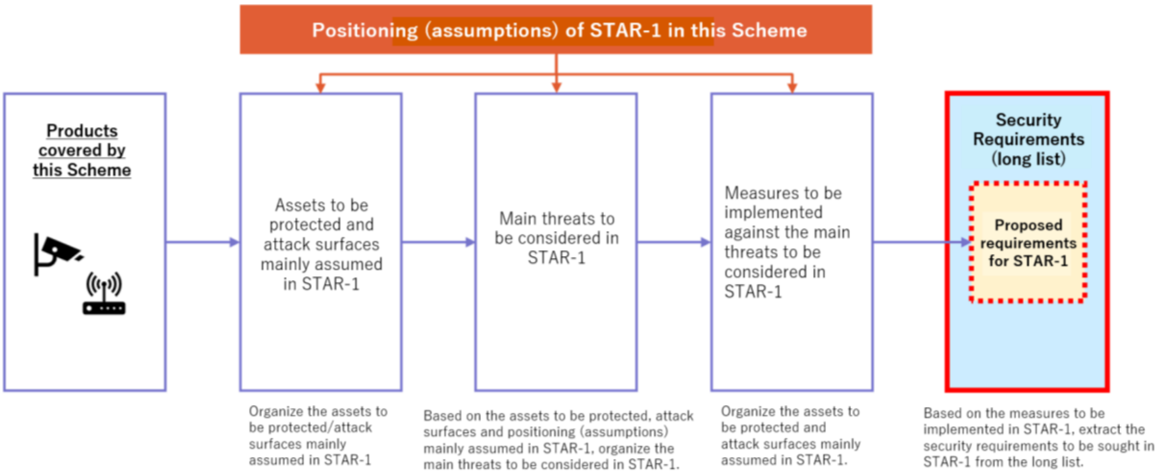
    - The level should be such that the person in charge of assessment and evaluation can self-assess at low cost by reviewing the checklist and assessment guide.

    - Label is assigned based on the application for conformance assessment checklist. (IPA does not check the contents of the checklist.)

- STAR-1 conformance requirement should be compatible with overseas schemes and international collaboration.

    - The requirements should be internationally linkable to overseas schemes, such as Singapore's CLS or the UK's PSTI Act.

Based on the positioning of STAR-1 (assumptions) above, the security requirements for STAR-1 were extracted from the long list as security requirements to be implemented against threats, after organizing the main threats to be considered in STAR-1 from the assets to be protected and the attack surfaces in STAR-1.


Positioning (assumptions) of STAR-1 in this Scheme
Products covered by this Scheme
Assets to be protected and attack surfaces mainly assumed in STAR-1
Main threats to be considered in STAR-1
Measures to be implemented against the main threats to be considered in STAR-1
Security Requirements (long list)
Proposed requirements for STAR-1

Organize the assets to be protected/attack surfaces mainly assumed in STAR-1

Based on the assets to be protected, attack surfaces and positioning (assumptions) mainly assumed in STAR-1, organize the main threats to be considered in STAR-1.

Organize the assets to be protected and attack surfaces mainly assumed in STAR-1.

Based on the measures to be implemented in STAR-1, extract the security requirements to be sought in STAR-1 from the long list.

Figure 4: Image of the Process for Extracting Security Requirements in STAR-1

Regarding the assets to be protected regarding information in IoT products (considering the four assets in the table below), the following are targeted as assets to be protected in STAR-1:

Table 3: List of Assets to be Protected by STAR-1

Assets to be protected in IoT products	Assumed Assets to be protected in STAR-1	Assumed Assets to be protected in STAR-2 and above
1. IoT functions Functions for devices and systems to connect to the IoT	● **Wired communications function** ● **Wireless communication function**	• Wired communications function • Wireless communication function
2. Original information Original function of the "thing" function for security and safety measures	● **Security functions**	• Security functions • Original product function • Safety-related functions
3. Information User's personal information, collected information, configuration information for each function, etc.	● **Configuration information on IoT functions (communication functions)** ● **Configuration information on security functions** ● **Generally sensitive personal information that the device collects, stores or communicates during the intended use of the device**	• Configuration Information • Personal information • Collected Information • Information on the device to be connected, etc.
4. Other physical assets	-	• Human assets • Physical assets

The five attack surfaces targeted by STAR-1 are (1) normal use interface, (2) maintenance interface, (3) unused interface, (4) potential attack points, and (5) physical contact at product disposal. Based on the level of threats countered by STAR-1, attack surfaces of "physical contact during product operation" and "contact in the supply chain such as product development and procurement" are not assumed.

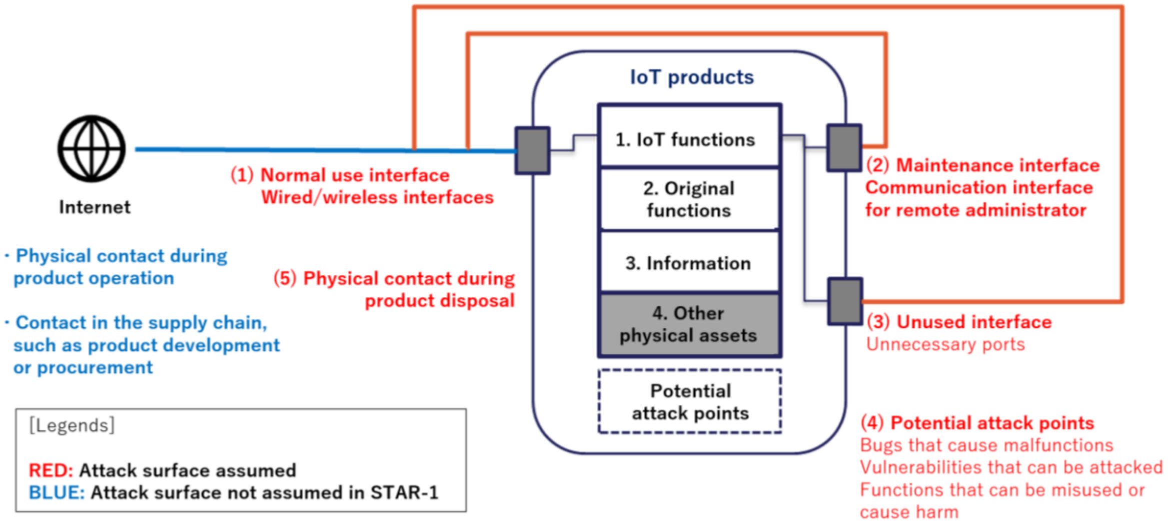

Internet
(1) Normal use interface
Wired/wireless interfaces
IoT products
1. IoT functions
2. Original functions
3. Information
4. Other physical assets
Potential attack points
(2) Maintenance interface
Communication interface for remote administrator
(3) Unused interface
Unnecessary ports
(4) Potential attack points
Bugs that cause malfunctions
Vulnerabilities that can be attacked
Functions that can be misused or cause harm
・Physical contact during product operation
(5) Physical contact during product disposal
・Contact in the supply chain, such as product development or procurement
[Legends]
RED: Attack surface assumed
BLUE: Attack surface not assumed in STAR-1

Figure 5: Attack Surfaces Targeted by STAR-1

Based on the assets to be protected and attack surfaces targeted in STAR-1, the following threats to IoT products in STAR-1 are targeted.

Note that the attack surfaces of "physical contact during product operation" and "contact in the supply chain during product development and procurement" are not covered, and thus the threats of "physical unauthorized manipulation (during operation)," "physical destruction/theft (during operation)," and "unauthorized modification" are not covered. In addition, although "denial" is listed as one threat in the STRIDE model, this threat is not covered because there are no assets to be protected under STAR-1 that are affected by "denial."

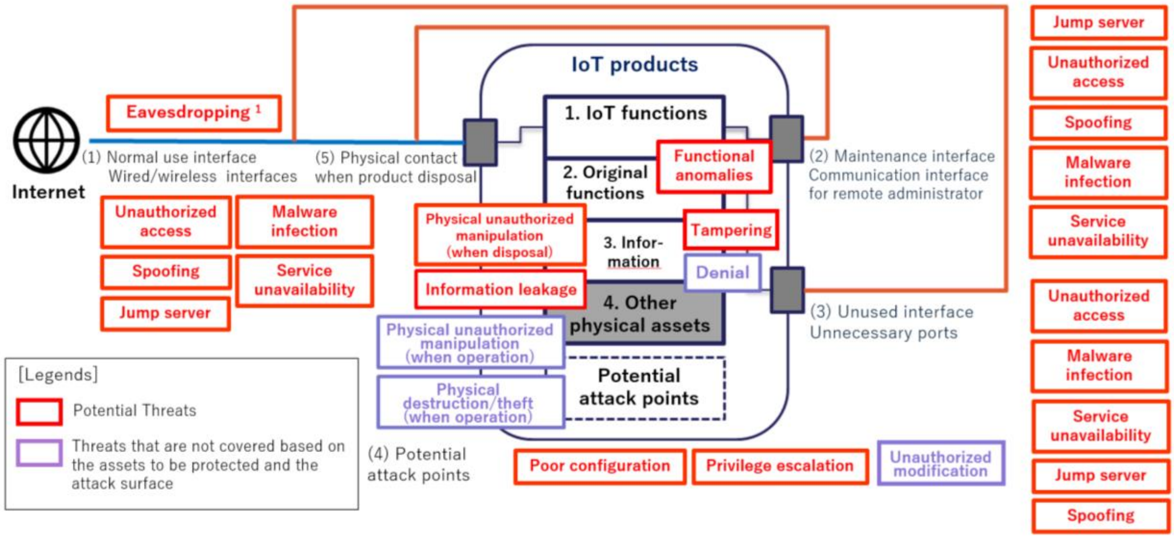


Figure 6: Threats Targeted by STAR-1

For the threats that should be covered by STAR-1, the following countermeasures that should be realized by IoT products/IoT product vendors were selected based on the positioning of STAR-1 and the standards of overseas schemes.

Table 4: List of Measures to be Realized in STAR-1 to Counter Threats

Main threats to be considered in STAR-1			Measures to be realized at STAR-1 to counter threats			
			Measures in IoT Products		Measures at IoT Product Vendors	
			Category	Countermeasures	Category	Countermeasures
1.	(i) By weak authentication function,	Threats that can lead to information leaks, tampering, and functional anomalies by becoming the target of unauthorized	Identification, authentication, access control	• Implement a mechanism that does not allow easy-to-guess passwords to be set. • Provide a secure authentication mechanism • Provide a mechanism to prevent brute force	Information provision	• Provide information on secure usage

		access from outside, malware infection, or attacks that serve as a jump host		authentication attempts		
	(ii) Due to neglect of vulnerabilities,		Vulnerability Mitigation, Software updates	• Take action against known vulnerabilities of high severity and major CWEs • Implement a mechanism whereby software components can be updated	information and inquiries reception, information provision	• Provide information on products and vulnerabilities • Provide information on how to apply security patches
	(iii) By enabling unused interfaces,		Logical access to interface	• Disable unnecessary interfaces	-	-
			Data protection	• Provide functions to protect the information to be protected that the device possesses (measures common to threats (1) through (3))	-	-
2. Threat of eavesdropping on device communications and leakage of the information to be protected			Data protection	• Implement safeguards against information leaks and modifications to protect the information to be protected that is transmitted over the Internet	-	-
3. Threats of leakage of the information to be protected from devices that have been disposed of or resold			Data protection	• Provide the ability to delete the information to be protected stored in the device while the device is in use, via the product itself or the associated services. • Provide the functionality to protect the information to be protected initially installed in the device.	Information provision	• Provide information on secure disposal methods

4. Threats of anomalies in security functions in the event of network disconnections, power outages, or other events	Improvement of Resilience	• Even if an event such as network disconnection or power failure occurs and the system is restored, authentication information and software settings do not return to their initial state, providing the state before the power was turned off.	-	-

3. STAR-1 Conformance Requirements

[Security Requirement Category]
1. No vulnerable authentication/authorization mechanism (e.g., universal default passwords, vulnerable passwords)

[Security Requirement]
1-3. Authentication mechanisms used to authenticate users to the product shall use technology that can reduce the assumed risk, which is appropriate for the characteristics of the product's intended use, etc.

[Security Requirement Category]
5. Communicate securely

[Security Requirement]
5-5. Product functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the product and where the manufacturer cannot assure what configuration will be required for the product to operate.

[STAR-1 Conformance Requirement S1.1-01]

Access control based on appropriate authentication shall be in place for access by other IoT devices or users to the information assets to be protected via IP communication to the IoT product.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) are deemed to be in conformance with this conformance requirement. In this case, the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)" shall be described on the JC-STAR Conformance Label Application. (Note that JC-STAR Conformance Label Application is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

No mechanism exists for authentication and access to the information assets to be protected via IP communication. (The rationale why user authentication is not required to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA)" field.)

[Definition of Terms: information assets to be protected]

All of the following information:

- Setting information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

STAR-1 Assessment Method

- Document assessment: subject

It shall be assessed that the technical documentation of the IoT product clearly describes the method of access control based on appropriate authentication for access to the information assets to be protected from other IoT devices or users.

- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.1-3 M, 5.5-5 M
[UK: PSTI Act] SCHEDULE 1: 1-(3)
[US: NISTIR 8425] Interface Access Control 2-b
[EU-CRA] ANNEX I 1. (3)(b)
[Singapore: CLS] [*]5.1-3, [**]5.5-5
[IEC 62443-4-2] CR1.5, CR1.6 NDR1.6, CR2.12, CR6.1

[Reference] Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (1)
[CCDS Certification Program] 1-1 Access Control and Authentication [Mandatory requirements] 4), 1-2 Data Protection [Mandatory requirements] 3), 1-1-1 Disabling of TCP/UDP ports [Recommended requirements] 2), 1-3 Software Update [Recommended requirements] 3)
[BMSec] Administrator authentication IA-1, device security settings management MT-1
[RBSS] Certification Standard for Security Camera 5.1.12 Advanced Security Function (2)-4, Certification Standard for Digital Recorder (Security Uses) 5.2.7 Advanced Security Function (2)-4
[JISEC-C0755] FIA_UAU (User authentication), FMT_SMR (security management roles), FIA_UID (User identification)

[Security Requirements]

1-1. Where passwords are used and, in any state, other than the factory default, all passwords shall be unique per device or defined by the user.

1-2. Where pre-installed unique passwords are used, these shall be sufficiently randomized against automated attacks.

[STAR-1 Conformance Requirement S1.1-02]

If IoT product uses passwords in the user authentication mechanism via the network and a default password is used at the time of installation of the IoT product, either of the following requirements (1) or (2) shall be satisfied.

(1) The default password shall be a unique value that differs for each IoT device and shall be at least 6 characters in length that cannot be easily guessed.
(2) For the default password, a function that requires the user to change the password at the first startup shall be implemented, and the user is required to set a password of 8 characters or more that can be set in such a function.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

No mechanism for password-based user authentication over the network.
(The rationale why password-based user authentication is not necessary to counter threats shall be described in “Reasons for being Not Applicable (NA)” field.)

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT product clearly describes the measures for default passwords for the user authentication mechanism via network when installing the IoT product that uses passwords.
- Device check: none

Refer to the "STAR-1 Assessment Guide" for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.1-1 MC (1), 5.1-2 MC (2)
[UK: PSTI Act] SCHEDULE 1: 1-(2), 1-(3)
[US: NISTIR 8425] Interface Access Control 1-b
[Singapore: CLS] [*]5.1-1, 5.1-2
[IEC 62443-4-2] CR1.5, CR1.7

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (2)
[CCDS Certification Program] 1-1 Access Control and Authentication [Mandatory requirements] 2), 1-1-2 Change of Credentials [Mandatory requirements] 2)
[BMSec] Change default password IA-2 b)-2), e)-2) 2.2)
[JISEC-C0755] FMT_IPWD_EXT (Extended: Initial password)

[Security Requirement]
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.

[STAR-1 Conformance Requirement S1.1-03]

It shall be possible to change the authentication value used for user authentication through the network to the IoT product, regardless of the type of authentication (e.g., password, token, fingerprint).

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
There is no mechanism for user authentication over the network. (The rationale why user authentication is not necessary to counter unauthorized access from outside shall be described in the "Reasons for being Not Applicable (NA)" field.)

[Definition of Terms: authentication value]
Individual values of attributes used in authentication mechanisms for IoT products. (e.g., For the password-based authentication mechanism, the authentication value is a string of characters. For the biometric fingerprint authentication, the authentication value is the fingerprint data of the index finger of the left hand, for example.)

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of the IoT product clearly describes the method to change the authentication values used in user authentication for the IoT product.

- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.1-4 MC (8)
[Singapore: CLS] [*]5.1-4
[IEC 62443-4-2] CR1.5

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 1-1-2 Change of credentials [Mandatory requirements] 1）
[BMSec] Change default password IA-2
[RBSS] Certification Standard for Digital Recorder (Security Uses) 5.2.7 Advanced Security Functions (2)-2
[JISEC-C0755] FMT_IPWD_EXT (Extended: Initial password)

[Security Requirement]
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.

[STAR-1 Conformance Requirement S1.1-04]

If the IoT device is not a constrained device, the IoT device shall employ the mechanism of user authentication over the network to the IoT device that make brute force attack difficult.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

One of the following conditions applies. (OR Condition)

- There is no mechanism for user authentication over the network for IoT devices. (The rationale why user authentication is not necessary to counter unauthorized access from the outside shall be described in the “Reasons for being Not Applicable (NA)” field.)
- The IoT device falls under the category of “constrained device.” (The rationale why the device falls under the category of “constrained device” shall be described in the “Reasons for being Not Applicable (NA)” field.)

[Definition of Terms: constrained device]

A device that is physically constrained for its intended use, either in its ability to process data, communicate data, store data, or interact with the user. (Refer to the Glossary for examples of such IoT devices.)

STAR-1 Assessment Method

- Document assessment: none
- Device check: subject
  Through device check, it shall be assessed that the mechanism for user authentication via the network for the IoT devices employ a mechanism that makes brute force attacks difficult.

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.1-5 MC (5)
[EU-CRA] ANNEX I 1. (3)(b)
[Singapore: CLS] [*]5.1-5
IEC 62443-4-2] CR1.11

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (1)
[CCDS Certification Program] 1-1 Access Control and Authentication [Mandatory requirements] 3)
[BMSec] Action in case of authentication failure IA-3
[JISEC-C0755] FIA_AFL (Authentication failures)

[Security Requirement Category]
2. Managing vulnerability reports

[Security Requirement]
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.

[STAR-1 Conformance Requirement S1.1-05]

The manufacturer shall make publicly available (e.g., post on the manufacturer's website) a vulnerability disclosure policy that includes all of the following information (1) through (3) below:

(1) Contact information for reporting IoT product security issues to the manufacturer (e.g., Web site URL of the manufacturer etc., phone number, email address).
(2) Procedures and overview of what manufacturer does after receiving reports on the security of IoT product.
(3) Procedures and overview of what manufacturer does for status updates of the IoT product and vulnerability until the vulnerability is resolved.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
None

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the vulnerability disclosure policies are clearly stated on IoT product websites or the other user-accessible media.
- Device check: none

Refer to the "STAR-1 Assessment Guide" for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.2-1 M
[UK: PSTI Act] SCHEDULE 1: 2-(2), 2-(3)
[US: NISTIR 8425] Information and Query Reception 1, 1-a, 1-b, Product Education and 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

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents
[CCDS Certification Program] 2-1 Contact and security support [Mandatory requirements] 1)
[BMSec] Contact FR-1

[Security Requirement Category]
3. Keep software updated.

[Security Requirements]
3-1. Particular software components included in products shall be updateable.

3-2. When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.

[STAR-1 Conformance Requirement S1.1-06]

All of the following criteria (1) through (3) shall be met for the update function of software components of the IoT product:

(1) The firmware (software) package of the IoT product shall be updatable.
(2) The firmware (software) package shall have a means to verify that the latest firmware (software) is installed, e.g., the IoT product implements a function to check the version of the firmware (software) package.
(3) The version of the updated firmware (software) package shall be kept after the power is turned off.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) can be deemed to be in conformance with this Conformance Requirement. In this case, the “Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)” shall be described on the JC-STAR Conformance Label Application. (Note that JC-STAR Conformance Label Application is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
None

STAR-1 Assessment Method

- Document assessment: none
- Device check: subject
  It shall be assessed the update functions for software components included in the target IoT products by device check.

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.3-1 R, 5.3-2 MC (5)
[US: NISTIR 8425] Software Update 1
[EU-CRA] ANNEX I 2. (8)
[Singapore: CLS] [**]CK-LP-03, [*]5.3-2
[IEC 62443-4-1] SM-6, SUM-1
[IEC 62443-4-2] CR4.3, CR3.10 EDR3.10, HDR3.10 NDR 3.10

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (3)
CCDS Certification Program] 1-3 Software Update [Mandatory requirements] 1) [Recommended requirements] 1)
[BMSec] Firmware update function PT-1 b)-3)
[JISEC-C0755] FMT_SMF (Specification of Management Functions)

[Security Requirement]
3-3. When the product implements an update mechanism, the update shall be simple for the user to apply.

[STAR-1 Conformance Requirement S1.1-07]

It shall be enabled for users to perform software updates in an easy and understandable procedure when applying updates.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

None

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that easy and understandable procedures for software updates are clearly stated in the user-accessible media (e.g., manuals, websites of IoT product).
- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.3-3 MC (12)
[EU-CRA] ANNEX I 2. (8)
[Singapore: CLS] [*]5.3-3
[IEC 62443-4-1] SUM-4

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (3)
[BMSec] Firmware update function PT-1 b)-4), e)-1)

[JISEC-C0755] FMT_SMF (Specification of Management Functions)

[Security Requirements]
3-2. When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.

3-7. When the product implements an update mechanism, the product shall use best practice cryptography to facilitate secure update mechanisms.

3-10. Where updates are delivered over a network interface, the product shall verify the authenticity and integrity of each update via a trust relationship.

[STAR-1 Conformance Requirement S1.1-08]

When updating software via a network, there shall be a mechanism to verify software integrity prior to updating.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
No mechanism exists to update software over the network. (The assumed update mechanism shall be described in the "Reasons for being Not Applicable (NA)" field.)

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of the IoT product clearly describes the implementation of a mechanism to verify software integrity prior to updating.
- Device check: none

Refer to the "STAR-1 Assessment Guide" for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.3-2 MC (5), 5.3-7 MC (12), 5.3-10 M (11,12)
[EU-CRA] ANNEX I 1. (3)(e)
[US: NISTIR 8425] Software Update 1
[Singapore: CLS] [*]5.3-2, 5.3-7, 5.3-10
[IEC 62443-4-1] SM-6
[IEC 62443-4-2] CR3.1, CR3.2 SAR3.2, EDR3.2 HDR3.2, NDR3.2, CR4.3

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (3)
[CCDS Certification Program] 1-3 Software Update [Mandatory requirements] 1) [Recommended requirements] 1), 2)
[BMSec] Firmware update function PT-1 b)-3)
[JISEC-C0755] FMT_SMF (Specification of Management Functions)

[Security Requirements]
3-8. When the product implements an update mechanism, security updates shall be timely.

[STAR-1 Conformance Requirement S1.1-09]

The manufacturer shall document policies and guidelines for prioritizing security updates for the purpose of rapid updates to security issues.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

None

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the organization's rules, policies, procedures, etc., or technical documentation of IoT products clearly state policies and guidelines for determining security update priorities.
- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.3-8 MC (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

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program]2-1Contact and security support [Mandatory requirements] 2)
[BMSec] Firmware update function PT-1 b)-4), e)-1)
[JISEC-C0755] FMT_SMF (Specification of Management Functions)

[Security Requirement]
3-14. The model designation of the products shall be clearly recognizable, either by labelling on the product or via a physical interface.

[STAR-1 Conformance Requirement S1.1-10]

The model number of the IoT product shall be provided to the user in one of the following measures:

(1) The model number of the IoT product is labelled directly on the IoT product itself.
(2) Users can recognize the model number by the GUI, web UI, etc., of the IoT product or the GUI, web UI, etc., of software or applications (e.g., smartphone apps) associated with the IoT product.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

None

STAR-1 Assessment Method

- Document assessment: none
- Device check: subject
  Assess whether a method is provided for users to confirm the model number of the IoT product.

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.3-16 M
[US: NISTIR 8425] Information Dissemination 2
[EU-CRA] ANNEX II 3
[Singapore: CLS] [*]5.3-16

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

Not applicable

[Security Requirement Category]
4. Securely store sensitive parameters

[Security Requirement]
4-1. Sensitive security parameters in the product’s storage shall be stored securely by the product.

[STAR-1 Conformance Requirement S1.1-11]

Information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media such as SD cards) shall be stored securely.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

None

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT products clearly describes that the information assets to be protected that are stored in the storage of IoT products (including information assets to be protected that are stored on storage media, such as SD cards, etc.) are securely stored.
- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[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

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 1-2 Data Protection [Mandatory requirements] 1), 3)
[JISEC-C0755] FMT_MTD (Management of TSF data)

[Security Requirement Category]
5. Communicate securely

[Security Requirements]
5-1. The product shall use best practice cryptography to communicate securely.

5-7. The product shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

[STAR-1 Conformance Requirement S1.1-12]

For information assets to be protected that are transmitted over a network, one of the following protection measures against information interception shall be in place:

(1) For information assets to be protected that are transmitted over a network to other IoT devices and servers (including servers in the cloud), the IoT device itself takes protective measures against information eavesdropping.

(2) Information assets to be protected that are transmitted over a network to other IoT devices or servers (including servers in the cloud) are transmitted only in a protected communication environment (Virtual Private Network environment or connection environment via a leased line).

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

There are no information assets to be protected that are transmitted over the network. (The rationale why there are no information assets to be protected that are transmitted over the network shall be described in the “Reasons for being Not Applicable (NA)” field.)

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT products clearly describes the implementation of protection measures against information eavesdropping for information assets to be protected that are transmitted over the network; if there is an application that works with IoT products, the information transmitted from the application shall also be assessed as an information asset to be protected.
- Device check: none

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.5-1 M, 5.5-7 M
[US: NISTIR 8425] Data Protection 3
[EU-CRA] ANNEX I 1.(3)(c)
[Singapore: CLS] [**]5.5-1, 5.5-7
[IEC 62443-4-2] CR3.1, CR4.3

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 1-2 Data Protection [Mandatory requirements] 2), 1-4-1 Wi-Fi authentication method [Mandatory requirements] 1), 1-4-2 Bluetooth vulnerability countermeasures [Mandatory requirements] 1)

[Security Requirement Category]
6. Minimize exposed attack surfaces

[Security Requirement]
6-1. All unused network physical interfaces and logical interfaces shall be disabled.

[STAR-1 Conformance Requirement S1.1-13]

In order to reduce the risk of external cyber-attacks on IoT products, interfaces that are unnecessary for the use of IoT products and at risk of being attacked shall be disabled, and vulnerability tests shall be performed on IoT products. Specifically, all of the following criteria (1) and (2) shall be met:

(1) In IoT products, for the interfaces that are used frequently and are assumed risks of vulnerability, the following interfaces which is unnecessary to use the IoT product and at a risk of being attacked shall be disabled.
(A) TCP/UDP port
(B) Bluetooth
(C) USB

(2) Vulnerability inspection shall be conducted against the IoT product using vulnerability scanner and no vulnerabilities that could be exploited in an attack are detected.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
None

STAR-1 Assessment Method

- Document assessment: subject
  In the technical documentation of IoT products, it shall be confirmed and evaluated that all interfaces used in IoT products are identified, that the purpose of use, etc., are clarified, and that no unnecessary items for the use of IoT products are included. In addition, when using ports that are particularly at risk of being misused in attacks, it shall be assessed that whether the technical documentation clearly describes that the system has a management process in place to monitor the attack status and take appropriate action as necessary.
- Device check: subject

It shall be assessed that interfaces that are unnecessary for the use of IoT products are disabled and that vulnerabilities that could be exploited in attacks are not detected by device check using port scanner and vulnerability scanner.

Note that in principle, both document assessment and device check shall be conducted. However, if there is no recommended port scanner or vulnerability scanner, the device check can be excluded (document assessment only).

Refer to the "STAR-1 Assessment Guide" for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[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

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 1-1-1 Disabling of TCP/UDP ports [Mandatory requirements] 1)
[BMSec] Separation between PSTN fax and network NI-1, Verification by Vulnerability Scanner VA-1, Close unused TCP/UDP ports VA-2, Close debug ports VA-3

[Security Requirement Category]
9. Resilience to outages

[Security Requirement]
9-1. Resilience shall be built into the products and services, taking into account the possibility of outages of data networks and power.

[STAR-1 Conformance Requirement S1.1-14]

When the power supply and network functionality are turned off and restored due to a power outage or other reason, the authentication values (passwords, private keys, etc.) used for access control and the software that has completed the setting and updating shall maintain the state immediately before the power was turned off without returning to the initial factory settings.

Note that IoT products that have acquired technical standards conformity certification including technical standards for terminal equipment security based on the Telecommunications Business Act (IoT products to which the Technical Qualification [T] Mark or [A] Mark is granted) are be deemed to be in conformance with this conformance requirement. In this case, the "Technical Standards Conformity Certification Number, etc., under the Telecommunications Business Act (Design Certification Number for the Technical Qualification [T] Mark or Technical Standards Conformity Certification Number for the [A] Mark)" shall be described on the JC-STAR Conformance Label Application. (Note that JC-STAR Conformance Label Application is attached to the Assessment Guide in Japanese version only.)

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
None

STAR-1 Assessment Method

- Document assessment: none
- Device check: subject
  It shall be assessed by conducting device check for IoT products that have software updated and have changed the authentication values used for access control from factory defaults.

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.9-1 R
[EU-CRA] ANNEX I 1. (3) (f)
[IEC 62443-4-2] CR7.1, CR7.3

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[MIC: Ordinance Concerning Terminal Facilities, etc.] Article 34-10 (4)
[CCDS Certification Program] 1-1 Access Control and Authentication [Mandatory requirements] 5)

[Security Requirement Category]
11. Delete user data

[Security Requirement]
11-1. The user shall be provided with functionality such that user data can be erased from the product in a simple manner.

[STAR-1 Conformance Requirement S1.1-15]

All of the following criteria (1) and (2) shall be met for the function of deleting data stored in the storage of the IoT product while using the IoT product:

(1) At least the following data about the user can be deleted by the user via the IoT device itself or associated services (e.g., mobile applications.):
  (A) Information assets (including personal information) acquired while using the IoT products
  (B) User set value
  (C) Authentication values set by the user, cryptographic keys and digital signatures obtained while using the IoT products

(2) The version of the firmware (software) package related to the updated security functions shall be maintained after the data is deleted.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]
None

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed that the technical documentation of IoT product clearly describes the ability for users to erase their information via the IoT device itself and associated services (e.g., mobile applications).
- Device check: subject

It shall be assessed by device check that the firmware (software) version is maintained after the operation of the data deletion function according to the procedure presented to the user and the data deletion.

Refer to the “STAR-1 Assessment Guide” for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[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

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 1-2-1 Data Erasure [Mandatory requirements] 1)
[BMSec] Initialization of security settings MT-2
[JISEC-C0755] FMT_MTD (Management of TSF data)

[Security Requirement Category]
17. Provide information on products

[Security Requirements]
17-2. The manufacturer shall provide users with guidance on how to securely set up, use and dispose of their products.

17-3. The manufacturer shall inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.

17-5. The manufacturer shall provide the user with a specified procedure for disposing of the product.

17-8. The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.

17-10. The manufacturer shall provide the user with information in a specified manner regarding product usage that may pose a security risk.

[STAR-1 Conformance Requirement S1.1-16]

Manufacturer shall take actions to provide information on cyber security of IoT products that meet all of the following criteria (1) through (5) below:

(1) Manufacture shall inform users about safe procedures for setting up and using IoT products that have implications for cybersecurity for the use of IoT products, including how to configure the initial setting.
(2) There shall be a mechanism to inform the content of the update, the necessity of the update, and the consequences of not updating the product when security updates for IoT products are released.
(3) Manufacturer shall inform disclaimers for accidents and failures that can be expected when updates are not made, and for accidents and failures that can be expected in general.
(4) Manufacturer shall inform the policy on the expiration or termination of support for the product or service.

(5) Manufacturer shall inform the possible risks of disposing of or selling used IoT products with information assets to be protected remaining in the IoT products, and how to safely terminate the use of IoT products, including data erasure.

Conditions for being Not Applicable (NA) and Supplementary Explanation of the Requirement

[Conditions for being Not Applicable (NA)]

None

[Definition of terms: information assets to be protected]

All of the following information:

- Configuration information on communication functions
- Configuration information on security functions
- Generally sensitive information, such as personal information, that is collected, stored, or communicated by the IoT device in the intended use of the IoT device

STAR-1 Assessment Method

- Document assessment: subject
  It shall be assessed the provision of information on cyber security of IoT products in the manuals, websites, and other user-accessible media of IoT products.
- Device check: none

Refer to the "STAR-1 Assessment Guide" for details on the assessment method.

[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries

[ETSI EN 303 645] 5.12-2 R, 5.3-11 RC (12), 5.3-13 M
[UK: PSTI Act] SCHEDULE 1: 3-(2), 3-(3), 3-(4)
[US: NISTIR 8425] Documentation 1-a, 1-d, Product Education and Awareness 1-a, 1-c, 1-d, 1-e, Information Dissemination 1-b, 1-c, 1-d, 1-e, 2
[EU-CRA] ANNEX I 2. (4), ANNEX I 2.(8), ANNEX II 4, ANNEX II 5, ANNEX II 6, ANNEX II 7, ANNEX II 8, ANNEX II 9
[Singapore: CLS] [*]5.3-13
[IEC 62443-4-1] SG-3, SG-4, SR-1, SUM-2

[Reference] Related Security Requirements of Existing Domestic Schemes/Documents

[CCDS Certification Program] 2-3 Provision of information to users [Mandatory requirements] 1), 2), 3), 4), 5)
[BMSec] Mass storage device data protection DP-1, firmware provision FR-2, firmware update function PT-1, operational environment PR-1, Internet communication data protection TP-1
[JISEC-C0755] FPT_STM (Reliable time stamps)

Appendix A Glossary

Terms	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
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 hardware replacement 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
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
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

Appendix B. Revision History

Version 1.1 (2024R1) has been released on December 5, 2024.

- STAR-1 Conformance Requirement S1.1-01 has been updated to include the security requirements. In addition, "[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries" and "[Reference] Related Security Requirements of Existing Domestic Schemes/Documents" were added.
- STAR-1 Conformance Requirement S1.1-01 has been updated: the unclear "following mechanisms" part of the "STAR-1 Assessment Method" has been clarified as "methods of access control based on appropriate certification."
- STAR-1 Conformance Requirement S1.1-02: integrated security requirements were added. In addition, "[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries" and "[Reference] Related Security Requirements of Existing Domestic Schemes/Documents" were added.
- STAR-1 Conformance Requirement S1.1-02: To clarify the targets of the "STAR-1 Conformance Requirement" and "Conditions for being Not Applicable (NA)," the "passcode" has been deleted.
- STAR-1 Conformance Requirement S1.1-02:"default passwords for the user authentication mechanism via network when installing the IoT product that uses passwords" was added to clarify the subject of "STAR-1 Assessment Method."
- STAR-1 Conformance Requirement S1.1-04: "user access" was revised to "user authentication" to be consistent with "STAR-1 Conformance Requirement" in "Conditions for being Not Applicable (NA)."
- STAR-1 Conformance Requirement S1.1-06: integrated security requirements were added.
  In addition, "[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries" and "[Reference] Related Security Requirements of Existing Domestic Schemes/Documents" were added.
- STAR-1 Conformance Requirement S1.1-06: "STAR-1 Assessment Method" was added as it was not described.
- STAR-1 Conformance Requirement S1.1-08: integrated security requirements were added.
  In addition, "[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries" and "[Reference] Related Security Requirements of Existing Domestic Schemes/Documents" were added.
- STAR-1 Conformance Requirement S1.1-10: "STAR-1 Assessment Method" was added as it was not described.
- STAR-1 Conformance Requirement S1.1-11: as the "Conditions for being Not Applicable (NA)" was not described, it has been clearly described "none."
- STAR-1 Conformance Requirement S1.1-11: in "STAR-1 Assessment Method," description has been unified to "information assets to be protected (including information assets to be protected that are stored on storage media such as SD cards)" for consistency with the "STAR-1 Conformance Requirement."
- STAR-1 Conformance Requirement S1.1-11: in "STAR-1 Assessment Method," "against unauthorized access via network" was deleted to clarify that the attack surface that needs to be securely stored for the information assets to be protected is other than "unauthorized access via network."
- STAR-1 Conformance Requirement S1.1-12: integrated security requirements were added.
  In addition, "[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries" and "[Reference] Related Security Requirements of Existing Domestic Schemes/Documents" were added.
- Conformance Requirement S1.1-12: wording was revised to unify the level of description for "STAR-1 Assessment Method." Specific assessment method was moved "STAR-1 Assessment Guide."
- STAR-1 Conformance Requirement S1.1-13: there were some lacks in "STAR-1 Assessment Method," and the assessment content for the missing parts of "document assessment" and "device check" was added.

- STAR-1 Conformance Requirement S1.1-15: in security requirements, the wording has been modified to avoid misunderstanding that it is a requirement to be implemented by the user.
- STAR-1 Conformance Requirement S1.1-15: “STAR-1 Assessment Method” has been revised in order to unify the level of description. Specific assessment method was moved “STAR-1 Assessment Guide.”
- STAR-1 Conformance Requirement S1.1-16: integrated security requirements were added.
  In addition, “[Reference] Related Security Requirements of Existing Schemes/Documents of Other Countries” and “[Reference] Related Security Requirements of Existing Domestic Schemes/Documents” were added.
- STAR-1 Conformance Requirement S1.1-16: as the “Conditions for being Not Applicable (NA)” was not described, it has been clearly described “none.”
- STAR-1 Conformance Requirement S1.1-16: wording was revised to unify the level of description for “STAR-1 Assessment Method.” Specific assessment method was moved “STAR-1 Assessment Guide.”
- “Surveillance in progress” was and deleted and “Extension procedure in progress” was added from the status in “Table 2: Status indication with conformance label information” in “1.1 What is a conformance label?”
- “2.2 Positioning of STAR-1”: in “Table 4: List of measures to be realized in STAR-1 to counter threats,” “countermeasures” was added for “3. Threats of leakage of protected information from devices that have been disposed of or resold.”
- Other corrections of errors and unification of terms were implemented.

1st edition (2024) published on September 30, 2024.