TECHNICAL CODE

INTERNET OF THINGS - DEVICE SECURITY REQUIREMENTS

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date: 4 April 2024

MCMC MTSFB TC G045:2024

Development of technical codes

The Communications and Multimedia Act 1998 ('the Act') provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Internet of Things Security Sub Working Group supervised by Security, Trust and Privacy Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

Celcom Axiata Berhad

FNS (M) Sdn Bhd

Maxis Broadband Sdn Bhd

SIRIM Berhad

TM Technology Services Sdn Bhd

Universiti Kuala Lumpur

Foreword

This technical code for Internet of Things - Device Security Requirements ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Security, Trust and Privacy Working Group.

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INTERNET OF THINGS - DEVICE SECURITY REQUIREMENTS

0. Introduction

The Internet of Things system has been de facto standard in many vertical applications. In the previous MCMC MTSFB TC G031, the security requirements related to IoT application layer has been developed. As the IoT involves a lot of interconnected devices, the security of the devices needs to be administered, especially in industrial applications e.g. heavy machinery, factories, automation, transportation, and healthcare.

IoT devices are the major components in IoT ecosystem where the interaction between the IoT software with the world happened through sensors and actuators as well as smart devices. These smart devices if not well protected will be the major security threats to the IoT system. Any malicious action could cause significant harm to their current settings. Therefore, a closer examination of the IoT device layer within the IoT management framework is needed.

1. Scope

This Technical Code provides the security requirements for IoT devices between the endpoint and gateway domains as depicted in Figure 1, which will benefit the IoT device manufacturers up until the IoT solution provider. The model used as a basis for this Technical Code is the IoT high-level reference model defined in MCMC MTSFB TC G013.

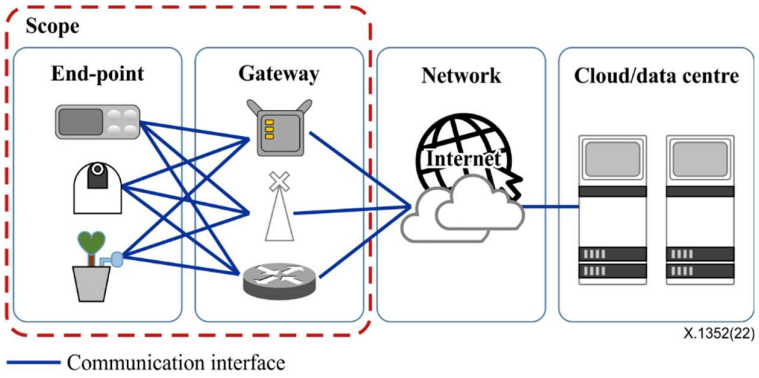


Figure 1. Scope of security requirements

The following are the 5 security dimensions applicable within this scope:

a) Authentication.

b) Cryptography.

c) Data security.

d) Device platform security.

e) Physical security.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

Recommendation ITU-T X.1352, *Security requirements for Internet of things devices and gateways*

Recommendation ITU-T X.1361, *Security framework for the Internet of things based on the gateway model*

Recommendation ITU-T Y.4100, *Common requirements of the Internet of things*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

API	Application Programming Interface
CoAP	Constrained Application Protocol
DoS	Denial of Service
FTP	File Transfer Protocol
I/O	Input/Output
ID	Identifier
IoT	Internet of Things
JTAG	Joint Test Action Group
LwM2M	Lightweight Machine-to-Machine
MCU	Microcontroller Unit
MQTT	Message Queuing Telemetry Transport
OS	Operating System
PII	Personally Identifiable Information
PIN	Personal Identification Number
SD	Secure Digital
SNMP	Simple Network Management Protocol
SSA	Shoulder-Surfing Attack
ST-D	Security Threat - Device

ST-G	Security Threat - Gateway
SWD	Serial Wire Debug
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver/Transmitter
UID	Unique Identifier
UPnP	Universal Plug and Play
USB	Universal Serial Bus

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Internet of Things (IoT) devices

IoT devices are commonly composed of a microcontroller unit (MCU), communication module, memory modules and Input/Output (I/O) peripherals.

A secure element can exist in the form of either hardware or software. Within a microcontroller unit (MCU), components such as firmware, physical interfaces, and memory contribute to its functionality. In this particular context, the software component, which typically includes an Operating System (OS), can be substituted or replaced by firmware.

The communication module requires cryptography for data security on transmission. Data in flash memories is stored securely for authentication, cryptography, data confidentiality and integrity.

User authentication is also required for accessing through physical interfaces such as a Universal Asynchronous Receiver/Transmitter (UART). In addition, any unused hardware interfaces should be either removed or switched off to mitigate potential security risks.

Figure 2 illustrates the 5 security dimensions that are applicable to IoT devices and gateways.

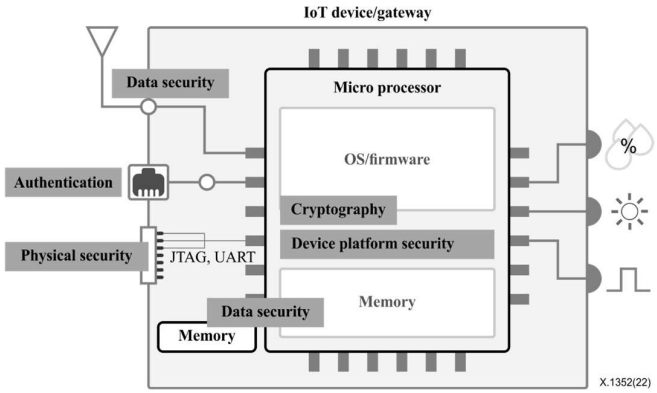


Figure 2. Example for applied security dimensions on IoT devices and gateways

4.1.1 Sensors and actuators

Sensor functions as input devices, collecting information about the environment and its context, which is then processed. On the other hand, actuators serve as output units, acting upon the processed information and executing decisions. In many IoT deployments, sensors and actuators are not only utilised as standalone components but also integrated into embedded systems.

Sensors and actuators are fundamental elements of IoT which may be connected to the cloud backend through gateways. This connectivity enables the data collected by the sensors to be transmitted and processed, in order to facilitate decision making.

4.1.2 Gateway

IoT gateway functions as a crucial link between the cloud and various controllers, sensors, and intelligent devices. It can be either a physical device or a software program. All data transmitted between IoT devices, and the cloud passes through the IoT gateway, which may be referred to as an intelligent gateway.

The role of an IoT gateway extends beyond simple data transmission. It also serves as a network router, facilitating the routing of data between IoT devices and the cloud. In the early stages, gateway devices predominantly enabled one-way traffic, allowing data to flow from the IoT devices to the cloud. However, nowadays, it is common for a gateway device to handle both inbound and outbound traffic, ensuring seamless bidirectional communication.

4.2 Internet of Things (IoT) high level reference model

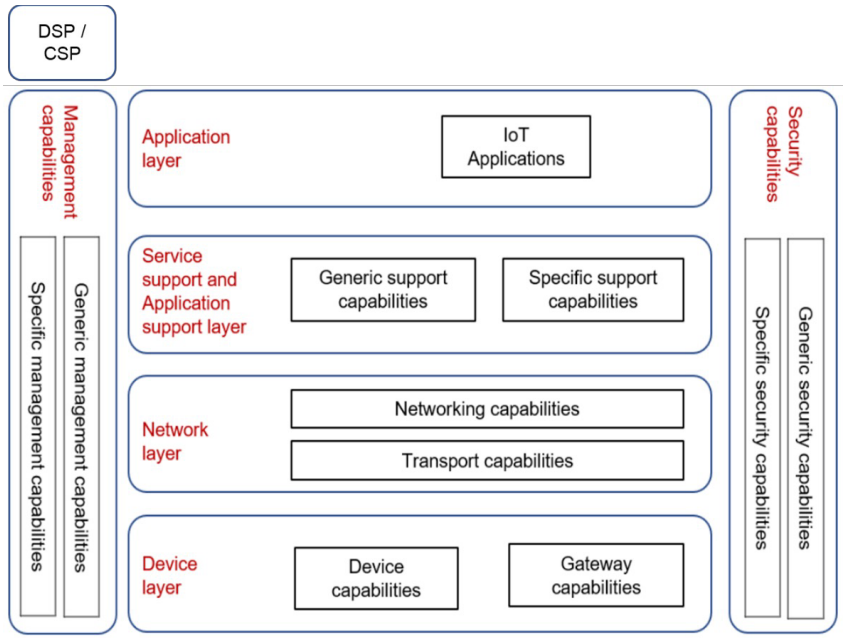
The IoT high level reference model, as defined in MCMC MTSFB TC G013, consists of the following 4 main layers, as illustrated in Figure 3.

a) Device layer represents an object that has a specific identifier, with sensors and/or actuators.

b) Network layer represents the communication capabilities.

c) Service and application support layer represent the cloud platform, backend and services.

d) Application layer represents IoT use cases.



Security controls and capabilities applicable at device layer

Figure 3. IoT high level reference model

5. Internet of Things (IoT) device security threats

Sections 5.1 and 5.2 of this Technical Code describes security threats and vulnerabilities that IoT sensors, devices, and gateways may encounter, making them potential targets for cyber-attacks. The security threats to gateways also encompass threats to IoT devices.

5.1 Security threats or vulnerabilities to IoT sensors or devices

The device-specific threats or vulnerabilities are specified in Table 1.

Table 1. IoT device security threats

Code	Security threats or vulnerabilities	Descriptions
ST-D-1	Authentication bypass	An unauthorised user successfully gains access to a device and is able to access critical data, which includes user data and configuration files stored in the device.
ST-D-2	Unauthorised device connection	A situation where a device is vulnerable to being connected or exposed to any unauthorized device. It also includes the risk of data, such as user data, being transmitted to unauthorized devices.

Table 1. IoT device security threats *(continued)*

Code	Security threats or vulnerabilities	Descriptions
ST-D-3	Excessive privilege	Giving excessive privilege or unnecessary privilege allows an attacker to be able to access all acceptable operations and controlled data including the user data of a device.
ST-D-4	Unrestricted repeated authentication attempts	An unauthorized user repeatedly attempts to authenticate themselves in order to gain access to a legitimate user account.
ST-D-5	Error due to concurrent access	A concurrent access from multiple administrator accounts may cause uncoordinated changes in the configuration of critical functionalities.
ST-D-6	Authentication information exposure and guessing	When authentication information such as a password is hardcoded or stored in plain text, or when an authentication password or Personal Identification Number (PIN) is exposed in plain text (also known as a Shoulder-Surfing Attack (SSA)), the authentication information may be exposed to or guessed by an attacker.
ST-D-7	Weak password	An attacker may obtain an unsecured combination, such as a default or weak password, which could enable them to impersonate a legitimate user.
ST-D-8	Weak encryption key or random number	An insufficient cryptographic key or predictable “random” number poses a significant risk to the protection of critical data.
ST-D-9	Weak cryptographic algorithm	An attacker may predict key data or discover the plain text of an encrypted message (ciphertext) by analysing traffic that uses a weak cryptographic algorithm.
ST-D-10	Absence of input validation	An absence of input validation may cause a device to malfunction.
ST-D-11	Data exposure and data manipulation	Critical data, including user data, device configuration, and cryptographic keys is susceptible to exposure, exploitation, or manipulation by an attacker.
ST-D-12	Session hijacking	An attacker may gain unauthorised access to a device if a session is closed abnormally or by exploiting valid sessions of multiple devices that uses the same cryptographic key.
ST-D-13	Unsafe update	A downloadable update file may not be accessible as intended, or an unauthorised or unauthenticated source may be executable.
ST-D-14	Update failure	Abnormal device operation may occur as a result of an error during the update process.
ST-D-15	Integrity error	An unintended manipulation of executable codes or configuration values may cause a device to malfunction.
ST-D-16	Malicious Software	Code that has unintended functions may be used with a malicious purpose.
ST-D-17	Residual memory information exploitation	The cryptographic key, password and sensitive data used for cryptological operations, authentications and data transmissions remain in the memory and may be exploited.
ST-D-18	Unintended change in critical configurations	An absence of device security controls may cause unintended changes in critical configurations and unsafe service deliveries.
ST-D-19	Unsafe error response	An absence of appropriate detection of and response to errors and malicious behaviour of a device may cause unsafe service deliveries.
ST-D-20	Unsafe development	The design and implementation of a device may introduce potential security vulnerabilities, and the testing process may lack an appropriate assessment and response to these vulnerabilities.

Table 1. IoT device security threats *(concluded)*

Code	Security threats or vulnerabilities	Descriptions
ST-D-21	Vulnerable OS	Device functionalities may be compromised or bypassed in a vulnerable OS environment.
ST-D-22	Vulnerable third-party modules or libraries	Vulnerable third-party modules or libraries may allow an attacker to call those at risk.
ST-D-23	Unsecured sensitive information record in system log	Sensitive information logged in a system may be vulnerable to exposure and exploitation by an attacker.
ST-D-24	Critical information exposure through debugging	Critical information may be exposed to and exploited by an attacker through log generation and debugging when a device is released and distributed.
ST-D-25	Unauthorised physical access	A device is exposed to unauthorised physical access and unintended changes in its configuration.
ST-D-26	Device capture	Refers to a device being physically compromised within device lifecycle (manufacturing, distribution, installation and post-installation) or having its keys lost.
ST-D-27	Impersonating of sensor or device	This attack occurs when an attacker effectively impersonates the identity of a legitimate sensor or device.
ST-D-28	Replay attack	This attack occurs when an attacker intercepts and records a legitimate communication between a device and a gateway, and then successfully obtains a legitimate response by replaying the recorded communication.
ST-D-29	Untrusted data transmission	An untrusted data transmission has the potential to result in device malfunction or the distribution of malicious code.

5.2 Security threats to IoT gateways

The gateway-specific threats or vulnerabilities are specified in Table 2.

Table 2. IoT gateways security threats

Code	Security threats or vulnerabilities	Descriptions
ST-G-1	Denial of Service (DoS) attack	A DoS attack is characterized by its ability to severely slow down or completely halt the services provided by a target system. This is achieved by overwhelming the target's memory and/or computing capacity through a flood of illegitimate traffic. Wireless sensor networks are particularly susceptible to DoS attacks due to their open medium, dynamically changing topology, and the absence of a clear line of defence. As DoS attacks continue to pose a significant challenge in modern networks, it is important to note that many defence techniques developed for fixed wired networks may not be directly applicable to mobile network environments.
ST-G-2	Unauthorised access	Unauthorised access to a gateway can lead to the exposure of sensitive information, unauthorised data modification, DoS attack and illicit use of resources. For instance, when an attacker gains access to a gateway, they can monitor unencrypted data, which may result in the compromise of usernames, passwords, location information and secure configuration data.

Table 2. IoT gateways security threats *(continued)*

Code	Security threats or vulnerabilities	Descriptions
ST-G-3	Rogue gateway	A rogue wireless access point, commonly known as an "evil twin," may be intentionally and covertly installed to facilitate unauthorised access to the network, either locally or remotely. The perpetrator has the ability to replace an existing wireless access point with their own, granting them complete configuration and monitoring access. Alternatively, they may configure a rogue wireless access point with similar settings but a higher power ratio, surpassing the signal of the legitimate wireless access point. When a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be obtained.

6. Security requirements

Based on the security capabilities described in ITU-T X.1361 and ITU-T Y.4100, the security requirements for addressing the challenges and threats of IoT devices and gateways (excluding network systems and platforms) are defined across 5 security dimensions, which are as follows:

6.1 Authentication

The authentication mechanisms in IoT devices include the following as shown in Table 3.

6.1.1 User authentication

Table 3. User authentication security requirements

Code	Controls	Descriptions
AU-1-1	Password shall be changed timely.	During the initial authentication, it is necessary to create or change a password. It is crucial to ensure that the new password is different from the initial or previous value.
AU-1-2	A user shall first be identified and authenticated when security management or sensitive data are accessed.	When attempting to access security management functions such as configuring an IoT device, user account, or privilege, the user shall undergo identification and authentication. Users with privileged access to security management or sensitive data should be managed separately and independently from regular users.
AU-1-3	The number of authentication attempts shall be limited.	An IoT device may be susceptible to brute force attacks if it allows repeated authentication attempts. Consequently, it shall incorporate a functionality to handle continuous authentication attempts effectively. This function shall be included in the IoT device, and it can be implemented using one of the following methods: limiting the number of authentication attempts to lock the account or temporarily disabling the authentication function for a specific duration.
AU-1-4	Unique pre-installed password.	The pre-installed password of the device shall be unique.

Table 3. User authentication security requirements *(continued)*

Code	Controls	Descriptions
AU-1-5	A function to manage user accounts and privileges should be provided.	All user accounts, including the administrator account, that are utilised on an IoT device shall be capable of being managed. This includes the ability to add and remove accounts, as well as assign privileges. If a role-based access control model is implemented, it shall clearly define the access privileges associated with all functions of the IoT device and assign them accordingly.
AU-1-6	Least privilege.	The principle of least privilege should be applied to all user accounts.
AU-1-7	Concurrent access to the administrator account should be restricted.	Concurrent access to management services should be limited to the same administrator account, and a function to disconnect previous access or limit new access attempts should be provided.
AU-1-8	A secure password complexity should be provided.	IoT devices shall enable users to set secure passwords that consider factors such as length, character variations, and the avoidance of repetitive and sequential characters.
AU-1-9	Certificate-based authentication	Using digital certificates is a more secure method for verifying the identity of a device and establishing a secure connection. However, it requires more complex implementation and operation compared to password-based authentication, which may not suit to all business use cases.
AU-1-10	Certificate lifecycle management	Digital certificates shall be managed diligently, ensuring a secure and reliable method for updating both the digital certificate and its certificate chain on a device before expiration. Furthermore, a unique certificate should be assigned to each device for identification purposes, strictly preventing the reuse of certificates across multiple devices.

6.1.2 Secure use of authentication credentials

The authentication credentials security requirements are specified in Table 4.

Table 4. Authentication credentials security requirements

Code	Controls	Descriptions
AU-2-1	Hard-coded credentials should not be used.	Password shall be neither hard coded nor stored in plain text.
AU-2-2	During authentication by password the password should be masked.	If a password is displayed in plain text, it may be vulnerable to an SSA.
AU-2-3	Error handling.	No specific feedback for authentication failure shall be provided.

6.1.3 Device authentication

The device authentication security requirements are specified in Table 5.

Table 5. Device authentication security requirements

Code	Controls	Descriptions
AU-3-1	The Unique Identifier (UID) of each hardware device shall be retained.	The IoT device shall have an Identifier (ID) that is unique and fixed.
AU-3-2	Mutual authentication.	Devices should be mutually authenticated before sensitive data is transmitted or the devices are interconnected for control purposes. Mutual authentication examples are as follows: a) use of a private key based on the public key encryption method; b) use of security attributes (UID, key, etc.) and security chips; The application of Transport Layer Security (TLS) or Datagram TLS to the lightweight communication protocols, namely the Constrained Application Protocol (CoAP), Lightweight Machine-to-Machine (LwM2M) protocol, or Message Queuing Telemetry Transport (MQTT), shall be considered.

6.2 Cryptography

If the limited memory and storage capacity make it challenging to utilise general cryptographic algorithms, appropriate cryptography algorithms shall be employed. For detailed cryptography requirements, please refer to Table 6.

Table 6. Cryptography requirements

Code	Controls	Descriptions
CR-1-1	Industry standard cryptography.	Cryptographic algorithms to protect against side-channel attacks should be used. Ensure cryptographic key methodology generates sufficient randomness.
CR-1-2	Key management.	Cryptographic keys shall be securely managed throughout their entire lifecycle. Keys should be generated, updated, distributed, used, stored and destroyed in a secure way.
CR-1-3	Unique cryptographic keys.	To mitigate compromise, it is advisable to use each cryptographic key for a single purpose. For instance, data encryption keys should be used exclusively for encrypting data, whereas keys used to secure passwords should be different. It is crucial to not mix or share keys or key pairs between encryption and authentication functions. Each key, including the unique key for each IoT device, should serve a distinct and specific purpose.

6.3 Data security

The data security dimension comprises several elements, including transmission data protection, data protection at rest, information flow control, secure session management and personally identifiable information (PII) protection.

6.3.1 Secure transmission and storage

The transmission and storage security requirements are specified in Table 7.

Table 7. Transmission and storage security requirements

Code	Controls	Descriptions
DS-1-1	Data transmitted shall be encrypted.	Data transmitted shall be encrypted using a secure cryptographic algorithm (see CR-1-1).
DS-1-2	A secure mode should be applied when a data or control channel is created.	When data is transmitted, a security protocol should be used ensure the confidentiality and integrity of the transmitted data, as well as authenticate the source and destination parties.
DS-1-3	Data stored in devices should be encrypted.	Data storage devices shall be encrypted using a secure cryptographic algorithm (see CR-1-1).
DS-1-4	Deleted data should not be restored.	A secure erase capability is required to ensure data cannot be recovered.
DS-1-5	Secure reset recovered and scraped devices.	Perform secure data deletion prior storage of recovered devices and pre-disposal of scraped devices (see DS-1-4).

6.3.2 Information flow control

The information flow control security requirements are specified in Table 8.

Table 8. Information flow control security requirements

Code	Controls	Descriptions
DS-2-1	Unauthorised network traffic should not be allowed.	Network segregation principle should be applied.

6.3.3 Secure session management

The session management security requirements are specified in Table 9.

Table 9. Session management security requirements

Code	Controls	Descriptions
DS-3-1	The session should be terminated after idle time-outs.	If accessing again after session termination, re-authentication should be conducted.
DS-3-2	The session ID should be an unpredictable value.	The generation of session IDs shall utilize a secure random number algorithm. The session ID should be changed and the previously used session IDs shall be destroyed during each session authentication process.

6.3.4 Personally Identifiable Information (PII) management

The PII management security requirements are specified in Table 10.

Table 10. PII management security requirements

Code	Controls	Descriptions
DS-4-1	PII data shall be securely managed.	PII data shall be encrypted and enforced with authentication prior access (see DS-1-2 and DS-1-3).

6.4 Device platform security

The device platform security dimension encompasses 5 key components as follows:

a) Software security.

b) Secure update.

c) Security management.

d) Logging.

6.4.1 Software security

The platform software security requirements are specified in Table 11.

Table 11. Platform software security requirements

Code	Controls	Descriptions
PL-1-1	Secure coding should be applied.	Software should be designed and implemented with consideration of security.
PL-1-2	Known security vulnerabilities shall be checked and removed.	If the software utilised in the development process incorporates protocols, libraries, an Application Programming Interface (API), packages, or open sources that are known to have security vulnerabilities, it is possible that these vulnerabilities may also exist within the firmware and operating system (OS) of the device. To ensure security, it is imperative to employ the public domain of known security vulnerabilities in order to conduct thorough security assessments of the device and eliminate any identified vulnerabilities.
PL-1-3	Obfuscation should be applied.	These requirements can be applied mostly to developed applications, which facilitates source code restoration. Since open reverse engineering tools can be used to extract important logic or key information, an appropriate level of protection is in order.
PL-1-4	An integrity verification function for configuration parameters and executable codes should be supported.	To ensure the authenticity and integrity of IoT devices, it is crucial to verify the integrity of configuration parameters and executable codes during booting time. This verification process should be performed periodically in automatic mode or manually. In the event of an integrity error, an appropriate response should be promptly executed.

6.4.2 Secure update

The secure update requirements are specified in Table 12.

Table 12. Secure update requirements

Code	Controls	Descriptions
PL-2-1	The update shall be conducted by authorised users.	Only the assigned role shall have the ability to perform the update. The authenticity of a user may be confirmed by re-authenticating the user immediately before proceeding with the update procedure.
PL-2-2	The rollback function should be supported if the update fails.	To reinstate the previous security and working condition of the device.
PL-2-3	Integrity should be checked prior to an update.	Checking the integrity and authenticity of update files can be done by verifying a cryptographic digital signature

6.4.3 Security management

The security management requirements are specified in Table 13.

Table 13. Security management requirement

Code	Controls	Descriptions
PL-3-1	Unnecessary services should be disabled.	Clearly identify the necessary services which are required for the device to run correctly, and disable unnecessary services such as Telnet, File Transfer Protocol (FTP), Universal Plug and Play (UPnP), Simple Network Management Protocol (SNMP), etc.
PL-3-2	Remote management.	Remote management should be done in a reliable environment using a secure protocol.
PL-3-3	A secure third-party library should be applied.	The third-party library and module used for development should be the latest version, ensuring the absence of any known security vulnerabilities or defects.
PL-3-4	A self-test should be provided.	A self-test function shall be provided to detect errors in the main hardware and software during the power-up process of the IoT device.

6.4.4 Logging

The logging security requirements are specified in Table 14.

Table 14. Logging security requirements

Code	Controls	Descriptions
PL-4-1	Logging should be generated for security-related events.	Logging implementation is required to enable the detection and tracing of any abnormal behaviour exhibited by the device.
PL-4-2	A secure logging mechanism should be provided.	The logging mechanism shall provide protection against loss and unauthorised changes. Log forwarding may be required to retain the logs at remote location.
PL-4-3	Timestamp.	Reliable timestamp source shall be provided.

6.5 Physical security

The physical security dimension encompasses securing physical interfaces and protecting IoT devices against tampering.

6.5.1 Secure physical interface

The physical interface security requirements are specified in Table 15.

Table 15. Physical interface security requirements

Code	Controls	Descriptions
PH-1-1	Any unnecessary external interface should be deactivated.	Some of the external interfaces used during development may no longer be required in production. The dimensions and functions of all external interfaces (such as the local area network, Universal Serial Bus (USB), Secure Digital (SD) card port, etc.) exposed to the outside should be specified. If necessary, access should be controlled by software to prevent unauthorised access.
PH-1-2	Unauthorised access to the internal interface shall be prevented.	The dimensions and functions of all internal interfaces (Joint Test Action Group (JTAG), Serial Wire Debug (SWD), UART, etc.) exposed to the outside shall be specified. If deemed necessary, access control shall be implemented to prevent unauthorised access.

6.5.2 Tamper-proofing

The tamper-proofing security requirements are specified in Table 16.

Table 16. Tamper-proofing security requirement

Code	Controls	Descriptions
PH-2-1	Detection and response functions are required.	Unauthorised physical manipulation shall be detected with the appropriate countermeasures such as tamper-evident seals, locks, tamper response, zeroization switches and alarms.

Annex A
(informative)

IoT device security controls threat mapping

A.1 User authentication

Table A.1. User authentication controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
AU-1-1	Password shall be changed timely.	ST-D-6 ST-D-7	ST-G-2
AU-1-2	A user shall first be identified and authenticated when security management or sensitive data are accessed.	ST-D-3 ST-D-6 ST-D-7 ST-D-12 ST-D-27	ST-G-2
AU-1-3	The number of authentication attempts shall be limited.	ST-D-4 ST-D-5	NA
AU-1-4	Unique pre-installed password.	ST-D-6 ST-D-7	NA
AU-1-5	A function to manage user accounts and privileges should be provided.	ST-D-3	ST-G-2
AU-1-6	Least privilege.	ST-D-3	ST-G-2
AU-1-7	Concurrent access to the administrator account should be restricted.	ST-D-5	NA
AU-1-8	A secure password complexity should be provided.	ST-D-6 ST-D-7	ST-G-2
AU-1-9	Certificate-based authentication.	ST-D-2 ST-D-7 ST-D-12 ST-D-27	ST-G-2
AU-1-10	Certificate lifecycle management.	ST-D-2 ST-D-7 ST-D-12 ST-D-27	ST-G-2

A.1.1 Secure use of authentication credentials

Table A.2. Authentication credentials controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
AU-2-1	Hard-coded credentials should not be used.	ST-D-11 ST-D-17 ST-D-20 ST-D-26	NA
AU-2-2	During authentication by password the password should be masked.	ST-D-6 ST-D-7 ST-D-8	NA
AU-2-3	Error handling.	ST-D-11 ST-D-19 ST-D-20 ST-D-24	NA

A.1.2 Device authentication

Table A.3. Device authentication controls mapped to threats

Code	Controls	Threats Mapping	
		ST-D-X	ST-G-X
AU-3-1	The UID of each hardware device shall be retained.	ST-D-6 ST-D-12 ST-D-27 ST-D-28 ST-D-29	NA
AU-3-2	Mutual authentication.	ST-D-2 ST-D-12 ST-D-20 ST-D-27 ST-D-28 ST-D-29	ST-G-2 ST-G-3

A.2 Cryptography

Table A.4. Cryptography controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
CR-1-1	Industry standard cryptography.	ST-D-8 ST-D-9 ST-D-13 ST-D-15 ST-D-17 ST-D-18	NA
CR-1-2	Key management.		NA
CR-1-3	Unique cryptographic keys.		NA

A.3 Data security

A.3.1 Secure transmission and storage

Table A.5. Secure transmission and storage controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-1-1	Data transmitted shall be encrypted.	ST-D-7 ST-D-11 ST-D-13 ST-D-29	NA
DS-1-2	A secure mode should be applied when a data or control channel is created.	ST-D-11 ST-D-13 ST-D-29	NA
DS-1-3	Data stored in devices should be encrypted.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2.
DS-1-4	Deleted data should not be restored.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2
DS-1-5	Secure reset recovered and scraped devices.	ST-D-11 ST-D-23 ST-D-25 ST-D-26	ST-G-2

A.3.2 Information flow control

Table A.6. Information flow controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-2-1	Unauthorised network traffic should not be allowed.	ST-D-2 ST-D-26 ST-D-27 ST-D-29	ST-G-3

A.3.3 Secure session management

Table A.7. Secure session management controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-3-1	The session should be terminated after idle time-outs.	ST-D-12 ST-D-28	NA
DS-3-2	The session ID should be an unpredictable value.	ST-D-1 ST-D-12 ST-D-28	NA

A.3.4 PII management

Table A.8. PII management controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
DS-4-1	PII data shall be securely managed.	ST-D-6. ST-D-11. ST-D-24.	NA

A.4 Device platform security

A.4.1 Software security

Table A.9. Platform software security controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-1-1	Secure coding should be applied.	ST-D-1 ST-D-5 ST-D-10 ST-D-12 ST-D-15 ST-D-16 ST-D-19 ST-D-20 ST-D-21 ST-D-22 ST-D-23 ST-D-24	NA
PL-1-2	Known security vulnerabilities shall be checked and removed.	ST-D-16 ST-D-21 ST-D-22	NA
PL-1-3	Obfuscation should be applied.	ST-D-15 ST-D-16	NA
PL-1-4	An integrity verification function for configuration parameters and executable codes should be supported.	ST-D-13 ST-D-14 ST-D-15 ST-D-16	NA

A.4.2 Secure update

Table A.10. Secure update controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-2-1	The update shall be conducted by authorised users.	ST-D-13 ST-D-16 ST-D-25	NA
PL-2-2	The rollback function should be supported if the update fails.	ST-D-14	NA
PL-2-3	Integrity should be checked prior to an update.	ST-D-13 ST-D-14 ST-D-16	NA

A.4.3 Security management

Table A.11. Security management controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-3-1	Unnecessary services should be disabled.	ST-D-2 ST-D-11 ST-D-22	ST-G-1
PL-3-2	Remote management.	ST-D-26	NA
PL-3-3	A secure third-party library should be applied.	ST-D-16 ST-D-22	NA
PL-3-4	A self-test should be provided.	ST-D-14 ST-D-15 ST-D-16 ST-D-26	NA

A.4.4 Logging

Table A.12. Logging controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PL-4-1	Logging should be generated for security-related events.	ST-D-23 ST-D-24 ST-D-25 ST-D-27 ST-D-29	ST-G-2
PL-4-2	A secure logging mechanism should be provided.		
PL-4-3	Timestamp.		

A.5 Physical security

A.5.1 Secure physical interface

Table A.13. Secure physical interface controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PH-1-1	Any unnecessary external interface should be deactivated.	ST-D-25 ST-D-26	NA
PH-1-2	Unauthorised access to the internal interface shall be prevented.	ST-D-1 ST-D-2 ST-D-25 ST-D-26	NA

A.5.2 Tamper-proofing

Table A.14. Tamper-proofing controls mapped to threats

Code	Controls	Threats mapping	
		ST-D-X	ST-G-X
PH-2-1	Detection and response functions are required.	ST-D-25 ST-D-26	NA

Acknowledgements

Members of Internet of Things Security Sub Working Group

Prof Dr Shahrulniza Musa (Chair)	Universiti Kuala Lumpur
Dr Ahmad Shahrafidz Khalid (Vice Chair/Draft lead)	Universiti Kuala Lumpur
Mr Khairul Ekhwan Kamarudin (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohd Ridhwan Mohd Salleh	Celcom Axiata Berhad
Ms Mayasarah Maslizan	CyberSecurity Malaysia
Ms Norkhadhra Nawawi	FNS (M) Sdn Bhd
Mr Hassen Abdelhamid Elberkennou	Maxis Broadband Sdn Bhd
Mr Ahmad Amzar Hanis Ahmad Zaki	SIRIM Berhad
Mr Muhamad Hasyimi Shaharuddin	TM Technology Services Sdn Bhd