Security Testing Specification for ICT Product Supply Chain Part 2: System Software Security V1.0

Taiwan Electrical and Electronic Manufacturers' Association
November 2022

Table of contents

Abstract

Given that in addition to meeting security requirements at the chip level, the operating systems and software applications running on the chip layer shall also comply with security specifications. The Administration for Digital Industries of the Ministry of Digital Affairs, and the Department of Industrial Technology of Ministry of Economic Affairs, have developed a series of security standards for the ICT product supply chain. These standards are formulated to comprehensively enhance the security quality of ICT products and align Taiwanese industries with international standards, thereby improving research and development technology and ensuring product quality.

This specification is promulgated as an industry standard by the Taiwan Electrical and Electronic Manufacturers' Association (TEEMA) after review by the Standards and Safety Committee in accordance with TEEMA's regulations. It serves as a reference blueprint for system software vendors and security testing laboratories regarding relevant product testing technologies. This specification specifically outlines the testing items for system software layer, the information to be provided by vendors, testing methods, and the criteria for passing, facilitating chip vendors and security testing laboratories as a reference blueprint for relevant product testing technologies.

This specification does not recommend all security matters. Before using this specification, appropriate security and health maintenance procedures should be established, and relevant regulations should be followed.

Some contents of this specification may involve patent, trademark, and copyright. TEEMA is not responsible for any or all identification of such patent, trademark, and copyright

1. Scope

The testing items stipulated by this specification are based on the security of the operating system and software (hereinafter referred to as system software). The scope applies to system software vendors corresponding to the levels in the supply chain, as indicated by the red box in Figure 1. This specification does not exhaustively list all security testing items, so users may need additional methods to ensure the security of their products.

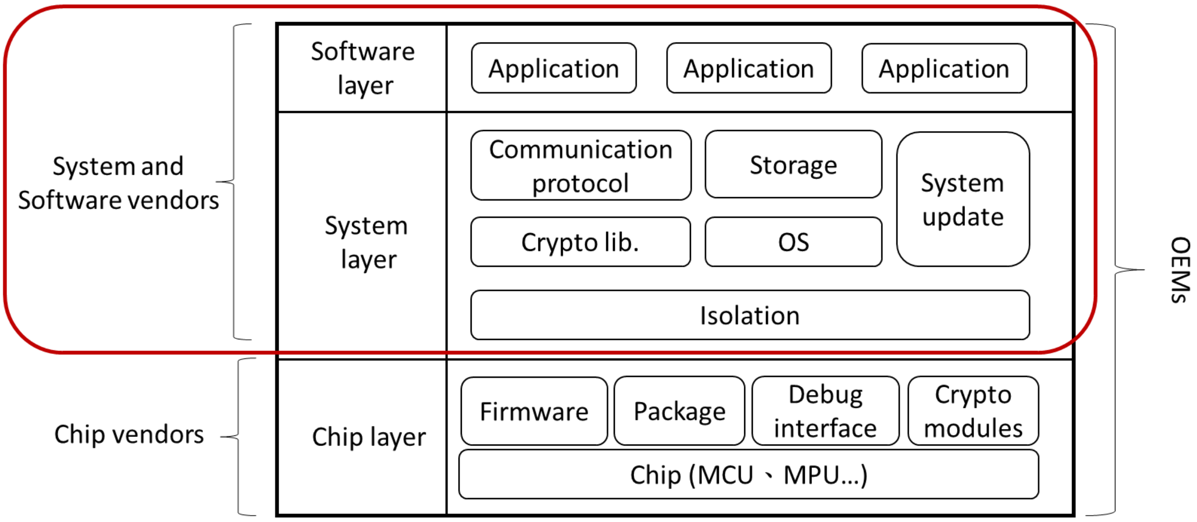

Figure 1 Scope of Testing Specification for System Software Security

The scope of applicability of this specification is explained in Table 1.

Table 1 Scope of application of this specification

Security Aspects	The Subject of Testing	The Applicable Scope
System Software Component Security	System Software Identity	The TOE provides system software identity verification.
	System Software Operating Status	The TOE provides secure running status of system software.
	Secure Update	The TOE provides update functionality.
Cryptographic Security	Cryptographic Algorithm Security	The TOE uses cryptographic algorithms.
	Key Security	The TOE uses cryptographic keys.
	Random Number Generator Security	The TOE uses random numbers.
Software Security	Isolation Security	The TOE provides software security isolation functionality.
	Security Status	The TOE provides specific operating states.
	Install/Update/Uninstall Security	The TOE provides on-site software installation/update/uninstallation functionality.
Storage Security	Data Protection	The TOE provides data storage.
	Secure Data Destruction	The TOE has data that shall be destructed and cannot be recovered.
	Log Preservation	The TOE provides event logging functionality.
	Only-Increasing Counter Preservation	The TOE provides generation and storage of reliable indicators.
Communication Security	Protocol Security	The TOE uses communication protocols for communication.
Firmware Security	Firmware Content Security	The TOE must ensure the security of the firmware content used.
	Firmware Protection	The TOE must ensure that the integrity and authenticity of the firmware used are protected.

2. Reference

The following documents are essential references for this specification. If a listed standard is marked with a year edition, only the standard for that year edition is cited. If the year is not marked, the latest version (including supplements) shall prevail.

[1] Security Standard for ICT Product Supply Chain Part 2: System Software Security V1.0, 2022

3. Terms and Definitions

Security Standard for ICT Product Supply Chain Part 2: System Software Security V1.0, and the following terms and definitions apply to this specification.

3.1 Software Instance

It refers to virtual devices or components within a product that have similar lifecycle characteristics. Typically, virtualization software is used to create an abstraction layer over computer hardware, allowing the hardware elements of a single computer, such as processors, memory, storage, etc., to be partitioned into multiple virtual devices.

4. Test Item Level

This section formulates the corresponding security testing items and test methods based on the Security Standard for ICT Product Supply Chain Part 2: System Software Security V1.0.

The summary table of testing standards is shown in Table 2. The first column represents the security testing aspects, including System Software Component Security, Cryptographic Security, Software Security, Storage Security, Communication Security, and Firmware Security. The second column lists the corresponding security testing items designed according to the security testing dimensions. The third column indicates the testing standards for each security testing item to assess the security level.

The security level is based on (1) the security requirements at the system software layer and (2) the complexity of security technology implementation, divided into three levels: Level 1, Level 2, and Level 3. Products must pass the tests of lower security levels before proceeding to the tests of higher security levels. The testing items in the security levels are divided into two categories: M and O, as described below:

- M: This item is a mandatory security requirement.
- O: Optional security requirements, which can be used to enhance the security of the product.

For products that implement the optional security requirements in the respective security levels, their security levels are 2+ and 3+ respectively.

Table 2 Summary Table of Test Specification Levels

Security Test Aspects	Security Test Items	Security Levels		
		Level 1	Level 2	Level 3
5.1 System Software Components Security	5.1.1 System Software Identity	The vendor conducts self-assessment and provides supporting evidence, which is then reviewed by the laboratory.	5.1.1.1 (M)	—
	5.1.2 System Software Operating Status		5.1.2.1 (M)	—
	5.1.3 Secure Update		5.1.3.1 (M)	—
5.2 Cryptographic Security	5.2.1 Cryptographic Algorithm Security		5.2.1.1 (M)	—
	5.2.2 Key Security		5.2.2.1 (M) 5.2.2.2 (M)	—
	5.2.3 Random Number Generator Security		5.2.3.1 (M)	—

Security Test Aspects	Security Test Items	Security Levels		
		Level 1	Level 2	Level 3
5.3 Software Security	5.3.1 Isolation Security		—	5.3.1.1 (M)
	5.3.2 Security Status		5.3.2.1 (M)	5.3.2.2 (O)
	5.3.3 Install/Update/Uninstall Security		5.3.3.1 (M) 5.3.3.2 (M) 5.3.3.3 (M)	—
5.4 Storage Security	5.4.1 Data Protection		5.4.1.1 (M) 5.4.1.2 (M) 5.4.1.3 (M)	—
	5.4.2 Data Secure Destruction		—	5.4.2.1 (M)
	5.4.3 Log Preservation		5.4.3.1 (M)	—
	5.4.4 Only-Increasing Counter Preservation		—	5.4.4.1 (O)
5.5 Communication Security	5.5.1 Protocol Security		5.5.1.1 (M) 5.5.1.2 (M) 5.5.1.3 (M)	—
5.6 Firmware Security	5.6.1 Firmware Content Security		5.6.1.1 (M) 5.6.1.2 (M)	5.6.1.3 (M)
	5.6.2 Firmware Protection		5.6.2.1 (M) 5.6.2.2 (M) 5.6.2.3 (M) 5.6.2.4 (M)	—

The Level 1 security level in this specification involves self-assessment by vendors for the TOE, with the relevant assessment items detailed in Appendix A. Levels 2 and 3 entail independent assessments conducted by laboratories on the TOEs submitted by vendors, with the corresponding testing specifications outlined in Chapter 5.

5. Security Test Specifications

5.1 System Software Components Security

5.1.1 System Software Identity

5.1.1.1 System Software Identity Verification

(a) Compliance:

Section 5.1.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2(M)

(c) Test purpose:

To verify the identity of TOE components and determine if they can be correctly recognized.

(d) Precondition:

None

(e) The vendors shall attach the following information:

(1) Explanation of the steps to view identification information for each TOE component.

(2) Declaration of the format for identifying information for each TOE component.

(3) Declaration of the naming convention for identification information.

(f) Test method:

(1) Inspect each TOE component to confirm the provision of identification information and ensure compliance with the declared naming convention.

(2) Confirm whether the naming convention for identification information meets the requirement for (global) uniqueness.

(g) Pass criteria:

(1) Each TOE component provides identification information and adheres to the declared naming convention.

(2) The naming convention for identification information meets the requirement for (global) uniqueness.

(h) Value

The vendor can accurately provide unique identification information, thereby validating the security of the product in use and serving as the foundation for compliance checks.

5.1.2 System Software Operating Status

5.1.2.1 Secure Boot

(a) Compliance:

Section 5.1.2.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether the software has the capability to inspect software configuration and ensure the authenticity and integrity of its code during the boot process.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(3) Explanation of the TOE boot process.

(4) Declaration of the method used during the boot process to ensure the authenticity and integrity of TOE configuration and code.

(5) Declaration of the "controlled state list," outlining the states the TOE shall exhibit if authenticity or integrity cannot be ensured, and explanation of recognizable ways for controlled states (e.g., warning windows, indicator lights, and sounds). Controlled states include known operational states.

(6) Declaration of the conditions for TOE entry into the “controlled state list.”

(7) Explanation of the steps triggering changes in the controlled state.

(f) Test method:

(1) Trigger all conditions for changes in controlled states.

(2) Observe whether the system enters a recognizable controlled state.

(g) Pass criteria:

(1) The software enters a controlled state based on trigger conditions.

(2) The controlled state is recognizable.

(h) Value

Users can verify the security of the software boot process.

5.1.3 Secure Update

5.1.3.1 Software Secure Update

(a) Compliance:

Section 5.1.3.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To assess whether the software provides secure software update functionality in the user environment.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare the method to ensure the integrity, authenticity, and confidentiality of the software during user environment updates (offline and online).

(2) If data encryption is employed during online updates, declare the encryption algorithm.

(3) Declare methods to resist downgrade attacks.

(4) Provide the data to be attached by the test unit in <5.5.1.1 Communication Support>.

(5) Explain the steps for executing software offline and online updates.

(6) If the vendor provides a test private key, provide the mechanism for the digital signature of the TOE. Otherwise, the laboratory will use its self-signed public-private key for testing, and the vendor needs to assist in the test.

(7) Provide the update files used by the TOE.

(8) If the software cannot provide secure software update functionality in the user environment, the vendor should provide a reasoned analysis report explaining the reasons for the absence of software secure update functionality.

(f) Test method:

(1) Offline Update Test:

i. Execute an offline update using a newer version of update files.

ii. Observe if the installation is completed successfully and can be executed.

iii. Use the test method from <5.1.1.1 System Software Identity Authentication> to observe if the updated software has unique (global) identification information. iv. Execute an offline update using an older version of update files (older version test).

iv. Execute an offline update using an older version of update files (older version test).

v. Observe if the installation is completed successfully and can be executed.

vi. Tamper with the contents of the update files (integrity test).

vii. Execute an offline update.

viii. Observe if the installation is completed successfully and can be executed.

ix. If the vendor provides a test private key (non-originally signed private key) to the laboratory, the laboratory will sign the update file with its self-signed private key according to the vendor's provided original update file and signature method (authenticity test).

x. Execute an offline update.

xi. Observe if the installation is completed successfully and can be executed.

xii. If the laboratory provides a self-signed public-private key to the vendor, the vendor signs the update file using that private key (authenticity test).

xiii. Execute an offline update.

xiv. Observe if the installation is completed successfully and can be executed.

xv. Reverse engineer the update files (confidentiality test).

xvi. Check if the plaintext content of the update files can be viewed.

(2) Online Update Test:

i. Open a packet capture tool and capture packets.

ii. Execute an online update.

iii. Check if a secure channel is used or if data is encrypted.

iv. Observe if the installation is completed successfully and can be executed.

v. Use the test method from <5.1.1.1 System Software Identity Authentication> to observe if the updated software has unique (global) identification information.

(g) Pass criteria:

(1) Offline Update:

i. Successfully updated software possesses unique (global) identification information.

ii. The TOE refuses to install using older versions of update files.

iii. The TOE refuses to install using tampered update files.

iv. If the vendor provides a test private key to the laboratory, the TOE refuses to install using a tampered update file signed with a forged private key.

v. If the laboratory provides a self-signed public-private key to the vendor, the TOE accepts installation using update files signed with that private key.

vi. It is not possible to reverse engineer the update files.

(2) Online Update:

i. Successfully updated software possesses unique (global) identification information.

ii. If the TOE uses a secure channel, the communication protocol version and algorithm used comply with the requirements of Appendix B.

iii. If the TOE uses data encryption, the algorithm used complies with the requirements of Appendix B.

(h) Value:

Enhance the security of on-site update mechanisms, allowing users to confidently update software in real-time when security vulnerabilities, functional errors, or improvements are identified.

5.2 Cryptographic Security

5.2.1 Cryptographic Algorithm Security

5.2.1.1 Cryptographic Operation

(a) Compliance:

Section 5.2.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2(M)

(c) Test purpose:

To verify if the TOE (Target of Evaluation) uses password algorithms that comply with standard specifications.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare a "Password Operation List," listing the password operations used, such as encryption, decryption, hash value calculation, digital signature, and signature verification.

(2) Declare a "Password Algorithm List," listing the password algorithms used.

(3) Declare the supported key lengths for the password algorithms.

(4) Declare the supported operation modes for the password algorithms.

(5) Use a table to correspond the algorithms with their supported password operations, key lengths, and operation modes.

(6) Provide test keys and data to be encrypted by them.

(f) Test method:

(1) Using the test keys, attempt to encrypt plaintext and compare the result with the TOE's self-encrypted result.

(2) Confirm if the two encryption methods and results are consistent.

(3) Verify resistance to timing attacks.

(4) Verify resistance to padding oracle attacks.

(g) Pass criteria:

(1) The password operations, algorithms, key lengths, and operation modes used comply with the requirements of Appendix B.

(2) The application applies the password algorithms listed in the "Password Algorithm List."

(3) The TOE can resist timing and padding oracle attacks.

(h) Value:

By using password algorithms that comply with standard specifications, the TOE reduces the probability of data being compromised through decryption attempts.

5.2.2 Key Security

5.2.2.1 Key Generation

(a) Compliance:

Section 5.2.2.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To examine the TOE's key generation method for compliance with standard specifications.

(d) Precondition:

The TOE must provide key generation functionality.

(e) The vendors shall attach the following information:

(1) Declare the password algorithms used in the key generation method.

(2) Declare the supported key lengths for the password algorithms.

(3) Declare the supported operation modes for the password algorithms.

(4) Provide evidence that the generated keys comply with the declarations in (1) to (3)

(5) Use a table to correspond the algorithms with their supported key lengths and operation modes.

(f) Test method:

(1) Review the evidence provided by the vendor regarding the conformity of the generated keys and confirm that the TOE complies with this requirement.

(2) Confirm if the declared password algorithms, key lengths, and operation modes comply with the requirements of Appendix B.

(g) Pass criteria:

(1) The password algorithms, operation modes, and key lengths used in the key generation method comply with the requirements of Appendix B.

(h) Value

By using a key generation method that complies with standard specifications, the TOE reduces the probability of key compromise.

5.2.2.2 Key Storage

(a) Compliance:

Section 5.2.2.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test Purpose:

To ensure that the CSP (Cryptographic Service Provider) stored in KeyStore is not compromised, thereby safeguarding the authenticity, integrity, and confidentiality of the data.

(d) Precondition:

The TOE must contain a CSP.

(e) The vendors shall attach the following information:

(1) Declare the types of assets to be protected by KeyStore.

(2) Declare the method for ensuring the authenticity, integrity, and confidentiality of KeyStore data.

(3) Declare an "Operation List," listing the operations that the application can perform on the CSP stored in KeyStore without obtaining the CSP.

(4) Explain the steps for storing CSP through the application into KeyStore.

(5) Explain the steps for opening KeyStore and viewing its contents.

(f) Test method:

(1) If KeyStore can be opened and viewed:

i. Attempt to store a key through the application.

ii. Open KeyStore to confirm if it is stored correctly.

iii. Try to add a key to KeyStore by impersonating another application (A) through application (B).

iv. Try to tamper with the contents of KeyStore by manipulating the KeyStore through application (A).

v. Confirm whether successful addition (authenticity) and tampering (integrity) can be achieved.

vi. Confirm whether KeyStore content is encrypted or protected using permission-bound isolation.

(2) If KeyStore cannot be opened and viewed:

i. Perform black box testing.

ii. Confirm the authenticity, integrity, and confidentiality of KeyStore data.

iii. Review the evidence provided by the vendor regarding the conformity of the generated keys.

(g) Pass criteria:

(1) The application cannot compromise the authenticity, integrity, and confidentiality of the CSP stored in KeyStore.

(h) Value

KeyStore provides protection for authenticity, integrity, and confidentiality, preventing improper disclosure of CSP.

5.2.3 Random Number Generator Security

5.2.3.1 Random Number Generator

(a) Compliance:

Section 5.2.3.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test Purpose:

To verify if the random number generation algorithm conforms to standard specifications.

(d) Precondition:

The TOE must provide random number generation functionality.

(e) The vendors shall attach the following information:

(1) Declare the password algorithm used for generating random numbers.

(2) Declare an "Entropy Source List," listing the sources from which random numbers are generated from physical and computational resources.

(3) Provide evidence that the random number generation of the TOE conforms to the declarations in (1) and (2).

(4) Provide proof that the random numbers generated by the random number generation algorithm pass the NIST SP 800-22 randomness test.

(f) Test method:

(1) Review the compliance evidence for random number generation.

(2) Confirm if the random number generation algorithm complies with the requirements of Appendix B.

(3) Confirm if the entropy sources for random number generation comply with the requirements of Appendix B.

(4) Confirm if the random numbers generated by the random number generation algorithm pass the NIST SP 800-22 randomness test.

(g) Pass criteria:

(1) The compliance evidence for random number generation meets this requirement.

(2) The random number generation algorithm complies with the requirements of Appendix B.

(3) The entropy sources for random number generation comply with the requirements of Appendix B.

(4) The random numbers generated by the random number generation algorithm pass the NIST SP 800-22 randomness test.

(h) Value:

Conforming to the standard specifications for random number generation ensures that the TOE produces more secure random numbers for use in cryptographic algorithms.

5.3 Software Security

5.3.1 Isolation Security

5.3.1.1 Application Component Isolation

(a) Compliance:

Section 5.3.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

To verify the functionality of application component isolation and its ability to provide secure isolation.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare the "Application Component List," listing the components that make up the application, such as modules, processes, applets, etc.

(2) Declare the "Critical Assets List," listing the sensitive data and personal information that should be protected within the application.

(3) Declare the method of isolating each component of the application.

(4) Provide proof of isolation for each component of the application.

(f) Test method:

(1) Review the isolation proofs for each component of the application.

(2) Confirm if the proof meets the security requirements.

(g) Pass criteria:

(1) The isolation proofs for each component of the application meet the security requirements.

(2) Sensitive data and personal information are protected by the application component isolation functionality.

(h) Value

The product provides isolation for each component of the application, ensuring that even if an attacker can execute malicious actions on one component of the application, they cannot compromise the confidentiality and integrity of other components of the application.

5.3.2 Security Status

5.3.2.1 Application Authenticity

(a) Compliance:

Section 5.3.2.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify the ability of the TOE to authenticate the application's authenticity.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare the methods to prevent the application from being copied (e.g., signatures, whitelist registration).

(2) Declare the actions taken upon detecting changes to the application.

(f) Test method:

(1) Using the mechanisms provided by the vendor to protect the authenticity of the application, attempt to compromise the authenticity of the application (e.g., using laboratory testing to sign the application with a test private key).

(2) Observe whether the TOE detects changes to the application.

(g) Pass criteria:

The application cannot be modified or copied without detection.

(h) Value

Users can ensure they have a genuine (secure) product rather than an insecure/incomplete clone.

5.3.2.2 Application State Attestation

(a) Compliance:

Section 5.3.2.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 3 (O)

(c) Test purpose:

Verify whether the TOE provides an identifiable known operating state.

(d) Precondition:

Pass the test of <5.3.2.1 Application Authenticity> .

(e) The vendors shall attach the following information:

(1) Declare the "Specific Operational State List" of the application, listing various specific operational states of the application, and only use the information provided by the application (e.g., the application's static code, configuration, and other

management-related information such as the application lifecycle status) to represent the current state of the application.

(2) Describe the steps to view the application's operational state.

(3) Declare the conditions for specific state changes of the application.

(4) Explain the steps to trigger specific state changes.

(f) Test method:

(1) Check if the information used in the "Specific Operational State List" is limited to the information provided by the application.

(2) Trigger all conditions for specific state changes.

(3) Observe if identifiable specific states are entered.

(g) Pass criteria:

(1) The state proof information of the application is limited to the information provided by the application.

(2) The application enters the specific operational state based on the trigger of specific operational states.

(3) Specific operational states are identifiable.

(h) Value

Users can verify the specific operational state of the application at any time.

5.3.3 Install/Update/Uninstall Security

5.3.3.1 Application Secure Installation

(a) Compliance:

Section 5.3.3.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify if the TOE provides secure application installation functionality in user environments and insecure product manufacturing sites.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare methods to check the integrity and authenticity of the application.

(2) Provide the application installation file.

(3) Provide an application installation file that is incompatible with the operational environment.

(4) Declare methods to check compatibility between the application and the operational environment.

(5) Explain the steps to install the application.

(6) Explain the steps to uninstall the application.

(f) Test method:

(1) Compatibility Testing

i. Attempt to install application installation files that are incompatible with the installation and operating environment.

ii. Observe if the installation can be completed successfully and if the application can run.

iii. Attempt to install application installation files that are compatible with the installation and operating environment.

(2) Integrity Testing

i. Tamper with the content of the application installation files.

ii. Execute the application installation files.

iii. Observe if the application can be installed and executed.

(3) Authenticity Testing

i. Re-sign the application installation files using laboratory test keys..

ii. Execute the application installation files.

iii. Observe if the application can be installed and executed.

(g) Pass criteria:

(1) The installation mechanism ensures that the application is compatible with the current operating environment before installation.

(2) The TOE rejects the use of tampered installation files for installation.

(3) The TOE rejects the use of counterfeit installation files for installation.

(h) Value

Ensuring the security of on-site application installation.

5.3.3.2 Application Secure Update

(a) Compliance:

Section 5.3.3.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2(M)

(c) Test purpose:

To verify if the TOE provides secure application update functionality in the user environment.

(d) Precondition:

None

(e) The vendors shall attach the following information:

(1) Declaration of methods to maintain the integrity, authenticity, and confidentiality of the application during updates in the user environment.

(2) Declaration of encryption algorithms used if data encryption is performed during online updates.

(3) Declaration of methods to resist downgrade attacks.

(4) Explanation of the operational steps for executing offline and online updates of the application.

(5) Provide the documentation required by the submitting unit in section <5.5.1.1 Communication support>.

(f) Test method:

(1) Offline Update Testing

i. Execute an offline update using an older version of the update file. (Downgrade installation test)

ii. Observe if the installation can be completed successfully and the application can run.

iii. Execute an offline update using a newer version of the update file. (New version installation test)

iv. Observe if the installation can be completed successfully and the application can run.

v. Tamper with the content of the update file. (Integrity test)

vi. Execute the offline update.

vii. Observe if the installation can be completed successfully and the application can run.

viii. Re-sign the update file using laboratory test keys. (Authenticity test)

ix. Execute the offline update.

x. Observe if the installation can be completed successfully and the application can run.

xi. Reverse engineer the update file. (Confidentiality test)

xii. Check if the plaintext content of the update file can be viewed.

(2) Online Update Testing

i. Open a packet-sniffing tool to capture packets.

ii. Execute the online update.

iii. Check if a secure channel is used or if the data is encrypted.

iv. Observe if the installation can be completed successfully and the application can run.

(g) Pass criteria:

(1) Offline Update Testing

i. The TOE uses a newer version of the update file for installation.

ii. The TOE refuses to use an older version of the update file for installation.

iii. The TOE refuses to use a tampered update file for installation.

iv. The TOE refuses to use a counterfeit update file for installation.

v. It is not possible to reverse engineer the update file.

(2) Online Update Testing

i. If the TOE uses a secure channel, the communication protocol version and algorithm used comply with the requirements in Appendix B.

ii. If the TOE uses data encryption, the algorithm used complies with the requirements in Appendix B.

(h) Value

Enhance the security of on-site update mechanisms. When an application encounters security flaws, functional errors, or requires improvements, users can confidently update the application in real-time.

5.3.3.3 Application Secure Uninstallation

(a) Compliance:

Section 5.3.3.3 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2(M)

(c) Test purpose:

To verify the TOE's secure uninstallation functionality to ensure that application data is destroyed to prevent potential attackers from obtaining sensitive and personal data through physical contact.

(d) Precondition:

None

(e) The vendors shall attach the following information:

(1) Explanation of the steps to uninstall the application.

(2) Declaration of the "Objects Not Destroyed List," listing the data that will not be destroyed during application uninstallation, along with explanations of the data's purpose and why it does not need to be destroyed.

(3) Declaration of the method used to destroy application data after uninstallation.

(4) Explanation of the steps to render the application inoperable.

(f) Test method:

(1) Review the "Objects Not Destroyed List" explanation for reasonableness.

(2) Correctness test of the "Objects Not Destroyed List":

i. Uninstall the application.

ii. Through the system interface, observe whether the application and its data have been wiped (excluding items on the "Objects Not Destroyed List").

(3) Application data recovery test:

i. Uninstall the application.

ii. Export the contents of non-volatile memory.

iii. Confirm whether the application data has been destroyed (excluding items on the "Objects Not Destroyed List").

(4) Data recovery test:

i. Store user data such as personal information, credentials, or configuration settings in the application.

ii. Execute steps to trigger errors in the application and confirm if successful.

iii. Execute the application uninstallation function.

iv. Through the system interface, check if the application data has been deleted.

v. Export the contents of non-volatile memory.

vi. Confirm that the application data has been destroyed.

(g) Pass criteria:

(1) The explanation of the "Objects Not Destroyed List" is reasonable.

(2) All application data generated after installing the application is destroyed upon uninstallation.

(3) All application data not explicitly marked as exempt from uninstallation is destroyed upon uninstallation.

(4) In the event of application issues, the application can still be securely uninstalled and sensitive and personal data cannot be recovered.

(h) Value

Users can use this feature to destroy application data, preventing potential attackers from obtaining sensitive and personal data through physical contact.

5.4 Storage Security

5.4.1 Data Protection

5.4.1.1 Data Storage Authenticity and Integrity

(a) Compliance:

Section 5.4.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether all data stored by the application is protected in terms of authenticity and integrity.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declaration of the "All Stored Data List" by the application, along with explanations of the categories of data stored in plaintext and their reasons.

(2) Declaration of the cryptographic algorithms used.

(3) Declaration of the key length used in the cryptographic algorithms.

(4) Proof of the uniqueness of keys used in software instances (i.e., no key sharing).

(5) A set of keys used by a software instance.

(f) Test method:

(1) Review the "All Stored Data List" to confirm its reasonableness.

(2) Review the proof of key uniqueness to ensure compliance with the specification requirements.

(3) Confirm whether the cryptographic algorithms and key lengths used meet the requirements of Appendix B.

(4) Attempt to add and tamper with data stored by Application B using the keys provided by the vendor, assuming the identity of A.

(5) Confirm whether it is possible to successfully add and tamper with data stored by other applications.

(6) If successful in tampering with data stored by other applications, confirm whether there are notifications or records of the identity and content of A.

(7) If the data storage device of the TOE (e.g., hard drive, SD card) is removable, attempt to add and tamper with the content of the storage device using other appropriate devices.

(8) Reinstall the storage device into the TOE.

(9) Confirm whether there are notifications or records of unauthorized actions.

(g) Pass criteria:

(1) The "All Stored Data List" is reasonable.

(2) Keys meet the uniqueness requirements.

(3) The password algorithms and key lengths used comply with the requirements of Appendix B.

(4) A cannot use its identity to add, tamper with, or delete data stored by other applications, or there are notifications or records of A's identity and content by the TOE.

(5) If the data storage device is removable, it shall not add or tamper with data stored by the application without being detected.

(h) Value

The TOE demonstrates the ability to protect the authenticity and integrity of application data.

5.4.1.2 Data Storage Confidentiality

(a) Compliance:

Section 5.4.1.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify if the cryptographic algorithm used can protect the confidentiality and integrity of stored data.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declaration of the "All Stored Data List" by the application, explaining the types of data stored in plaintext and the reasons for storing them as plaintext.

(2) Declaration of the cryptographic algorithm used by the encryption.

(3) Declaration of the key length used in the cryptographic algorithm.

(4) Provide a method and proof of generating unique keys.

(5) Provide proof of key uniqueness for software instances (i.e., no key sharing).

(6) Explanation of all data stored by the application, their storage locations, and viewing methods.

(7) Provide a set of encryption keys used by a product software instance.

(f) Test method:

(1) Review the explanation of the " All Stored Data List" to assess its reasonableness.

(2) Review the proof of key uniqueness to ensure compliance with this standard requirement.

(3) Access the data storage location.

(4) Verify if the data is encrypted.

(5) Confirm if the keys meet the declared specifications and provide sufficient strength for data confidentiality protection.

(g) Pass criteria:

(1) The explanation of the " All Stored Data List" is reasonable.

(1) The keys meet the uniqueness requirement.

(2) The cryptographic algorithm and key length used comply with the requirements of Appendix B.

(3) Data other than those listed in the " All Stored Data List" are encrypted.

(h) Value

The TOE demonstrates the ability to protect the confidentiality and integrity of application data.

5.4.1.3 External Storage

(a) Compliance:

Section 5.4.1.3 of “Security Standard for ICT Product Supply Chain Part 2: System Software Security”.

(b) Security level:

Level 2(M)

(c) Test purpose:

Verify if all data stored outside the control of the TOE is adequately protected.

(d) Precondition:

Data of the TOE stored externally.

(e) The vendors shall attach the following information:

(1) Explanation of the location and access method of data stored outside the control of the TOE.

(2) Declaration of security elements for protected data, such as authenticity, integrity, confidentiality, software instance binding (e.g., external storage space bound to the TOE), and version control.

(3) Declaration of the "External Storage Exception Data List," listing data stored outside the direct control of the TOE but not protected, along with reasons why the data does not need protection.

(4) Provide login credentials for external data storage space.

(5) If data is protected using cryptographic algorithms, declare:

i. The cryptographic algorithm used for data encryption.

ii. The key length supported by the cryptographic algorithm for data encryption.

(f) Test method:

(1) Review the explanation of the "External Storage Exception Data List" for reasonableness.

(2) Authenticity Test:

i. Attempt to add data with another application identity via the application.

ii. Verify if the operation is successful.

(3) Integrity Test:

i. Attempt to tamper with data stored by another application via the application.

ii. Verify if the operation is successful.

(4) Confidentiality Test:

i. Attempt to access data stored outside the control of the TOE using another identity and view the data.

ii. Confirm if plaintext is visible.

iii. Attempt to intercept while accessing external storage data through the application.

iv. Examine the intercepted content to confirm the use of secure channels or content encryption.

(5) Software Instance Binding Test:

i. Attempt to access external storage data of Product B using the identity of Product A.

ii. Verify if the operation is successful.

(6) Version Control Test:

i. Check if versions exist at the external storage location and attempt to change versions via the application.

ii. Verify if the operation is successful.

(7) Confirm that the security elements of the data to be protected have been ensured as declared by the vendor.

(g) Pass criteria:

(1) The explanation of the "External Storage Exception Data List" is reasonable.

(2) If data is protected using cryptographic algorithms, the cryptographic algorithm used complies with the requirements of Appendix B.

(3) All data stored outside the direct control of the TOE, except those declared in the "External Storage Exception Data List," has been protected.

(4) The security of the data to be protected is ensured as declared by the vendor.

(h) Value

Protection of data stored outside the direct control of the TOE reduces the likelihood of data modification or leakage.

5.4.2 Secure Data Destruction

5.4.2.1 Data Sanitization

(a) Compliance:

Section 5.4.2.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether valuable information that may remain in deleted data in memory is also cleared and cannot be recovered.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) If encryption algorithms are used to clear data, declare the encryption algorithm.

(2) Declare the "Data not Automatically Cleared List" and explain why the data does not need to be automatically cleared.

(3) Declare the programming language used by the application.

(4) If the programming language does not have an automatic clearing function, provide proof of code containing memory-clearing instructions.

(5) Explain the steps for executing memory-clearing instructions in the application.

(f) Test method:

(1) Review the explanation of the "Data not Automatically Cleared List" for reasonableness.

(2) If the programming language used does not have an automatic clearing function, review the proof of code containing memory-clearing instructions.

(3) Confirm that the memory clearing instructions can completely clear the data.

(4) Use the application to execute memory-clearing instructions to clear data other than those listed in the data list.

(5) Export the contents of the memory (memory dump).

(6) Analyze and attempt to recover the contents of the memory.

(g) Pass criteria:

(1) The explanation of the "Data Not Automatically Cleared List" is reasonable.

(2) If the TOE uses encryption methods to clear data from memory, the encryption algorithm should comply with the requirements of Appendix B.

(3) The TOE completely clears data other than those listed in the "Data not Automatically Cleared List."

(4) The cleared data cannot be recovered.

(h) Value

Reducing the opportunity for attackers to obtain valuable residual information through physical access methods.

5.4.3 Log Preservation

5.4.3.1 Audit Log Generation and Storage

(a) Compliance:

Section 5.4.3.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify the security of the generation and storage methods of audit logs.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Declare the "Security Event List," marking important and minor security events, and explain the reasons for marking minor security events.

(2) Declare the identities with access to the audit logs and their corresponding permissions.

(3) Explain the steps for accessing the audit logs.

(4) Declare the conditions and methods for triggering the generation of important security events by the TOE.

(f) Test method:

(1) Review the explanation of the "Security Event List" for reasonableness.

(2) Trigger the conditions for generating important security events.

(3) Authorize users to access the audit logs.

(4) Confirm whether corresponding audit logs are generated and recorded.

(5) Attempt to access the audit logs as an unauthorized user.

(6) Confirm whether unauthorized access is successful。

(g) Pass criteria:

(1) The explanation of the "Security Event List" is reasonable.

(2) The TOE can generate and record audit logs for the important security events listed in the Security Event List.

(3) Authorized users accessing the audit logs comply with their permission settings.

(h) Value

The method used for generating and storing audit logs meets security requirements and enables the detection of attempted attacks on the TOE.

5.4.4 Only-Increasing Counter Preservation

5.4.4.1 Reliable Indicator

(a) Compliance:

Section 5.4.4.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether the indicator of the only-increasing counter is susceptible to tampering or deletion.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Explanation of the operational steps for viewing the growth record.

(2) Declaration of the computing unit for the growth record.

(f) Test method:

(1) Start the TOE and check the growth record.

(2) Attempt to tamper with and delete the growth record.

(3) Attempt to execute <5.3.4.1 Hardware Factory Reset> of “Security Standard for ICT Product Supply Chain Part 1: Chip Security.

(4) Confirm whether the growth record has been reset.

(5) According to the declaration, after using the TOE for a certain computing unit, check the growth record.

(6) Confirm whether the growth record has increased corresponding to the computing unit.

(g) Pass criteria:

(7) The growth record cannot be tampered with or deleted.

(8) Even if a hardware factory reset occurs, the system does not allow the growth record to be reset.

(h) Value

The growth counter is important data for confirming the usage status of the TOE, hence protecting this indicator from harm is essential.

5.5 Communication Security

5.5.1 Protocol Security

5.5.1.1 Communication Support

(a) Compliance:

Section 5.5.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Review whether the security protocols and measures used between products and products, or between users and products, comply with security specifications.

(d) Precondition:

The TOE supports network communication interfaces.

(e) The vendors shall attach the following information:

(1) Declare the "Endpoint and Protocol Measures Correspondence Table" in tabular form, listing all default open communication interfaces, services, and port numbers, and declare the corresponding communication protocols and supported algorithms, such as: TLS 1.2 with TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, or IPSEC. The test unit should provide sufficient information to accurately describe the quality of the cryptographic algorithms used.

(f) Test method:

(1) Review whether the "Endpoint and Protocol Measures Correspondence Table" lists all default open communication interfaces, services, and port numbers in tabular form, and declares the corresponding communication protocols and supported algorithms.

(2) Confirm that the communication protocols and supported algorithms used in the "Endpoint and Protocol Measures Correspondence Table" comply with the requirements of Appendix B.

(g) Pass criteria:

(1) The information provided in the "Endpoint and Protocol Measures Correspondence Table" is sufficient to identify all used communication interfaces, services, and port numbers, along with the corresponding communication protocols and supported algorithms.

(2) The communication protocols and supported algorithms used in the "Endpoint and Protocol Measures Correspondence Table" comply with the requirements of Appendix B.

(h) Value

The TOE uses protocols and measures that comply with security specifications to protect communication between products and products, or between users and products.

5.5.1.2 Communication Enhancement

(a) Compliance:

Section 5.4.4.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether the protocols and measures used by the TOE are correctly implemented.

(d) Precondition:

The TOE supports network communication interfaces.

(e) The vendors shall attach the following information:

(1) Provide the documentation required for testing as specified in Section <5.5.1.1 Communication Support>.

(f) Test method:

(1) Scan the services and port numbers provided by the TOE.

(2) Confirm whether the results match the services and port numbers declared in the "Endpoint and Protocol Measures Correspondence Table."

(3) Activate packet-sniffing tools.

(4) Access the TOE's network communication interface via the network.

(5) Verify if the communication protocols and cryptographic algorithms used in transmission match those declared in the "Endpoint and Protocol Measures Correspondence Table."

(g) Pass criteria:

(1) The scan results match the services and port numbers declared in the "Endpoint and Protocol Measures Correspondence Table."

(2) The communication protocols and algorithms used in transmission match those declared in the "Endpoint and Protocol Measures Correspondence Table."

(h) Value

The TOE implements communication protection using protocols and measures that comply with security standards.

5.5.1.3 Service Minimization

(a) Compliance:

Section 5.4.4.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To examine whether all network services provided by the TOE are necessary.

(d) Precondition:

The TOE supports network communication services.

(e) The vendors shall attach the following information:

(1) Declare the "All Network Services List" and explain the purpose of each service and its necessity.

(2) Describe the steps to enable all network services.

(f) Test method:

(1) Review the explanation provided in the "All Network Services List" to determine its reasonableness.

(2) Enable all network services.

(3) Perform a network service scan.

(4) Verify if the scan results match the "All Network Services List."

(5) Based on the scan results, compare if the provided service versions have any known security vulnerabilities.

(g) Pass criteria:

(1) The explanation provided in the "All Network Services List" is reasonable. For instance, if the test subject provides RDP (Remote Desktop Protocol) service without the need for remote desktop functionality, it would be deemed unreasonable.

(2) The scan results match the "All Network Services List."

(3) The provided service versions do not have any known security vulnerabilities.

(h) Value

By offering only essential network services, the test subject can reduce the attack surface for potential attackers.

5.6 Firmware Security

5.6.1 Firmware Content Security

5.6.1.1 Sensitive Content Protection

(a) Compliance:

Section 5.6.1.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

To verify the cryptographic algorithms and CSP security used in firmware and to check for undisclosed links.

(d) Precondition:

Firmware is not encrypted.

(e) The vendors shall attach the following information:

(1) Provide firmware files.

(2) Declare the cryptographic algorithms used in the firmware.

(3) Declare the IP, URL, and email contained within the firmware.

(f) Test method:

(1) Use tools with binary string search capabilities to search for plaintext CSP in the firmware.

(2) Use tools with firmware disassembly capabilities to dissect the firmware of the product.

(3) Check if the firmware can be parsed for file system directories.

(4) Search for plaintext CSP in the file system.

(5) Review written documentation that can demonstrate the cryptographic algorithms used.

(6) Verify whether the cryptographic algorithm used to protect the keys in the firmware is one of the hash functions approved in Appendix B.

(7) Confirm whether there are undisclosed IP addresses, URLs, and email addresses in the firmware.

(g) Pass criteria:

(1) There are no plaintext CSPs in the firmware, or the CSPs have been properly protected.

(2) The IP, URL, and email addresses contained in the firmware are consistent with the declarations provided by the vendor.

(3) The cryptographic algorithms used to protect the keys in the firmware adhere to the cryptographic algorithms approved in Appendix B。

(h) Value

By only containing declared IP, URL, and email addresses in the firmware, and ensuring proper protection of CSPs, the probability of including malicious links and the risk of CSP leakage are reduced.

5.6.1.2 Firmware Vulnerability Detection

(a) Compliance:

Section 5.6.1.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To detect whether the firmware contains significant cybersecurity risks.

(d) Precondition:

Firmware is not encrypted.

(e) The vendors shall attach the following information:

(1) Provide firmware files。

(f) Test method:

(1) Use firmware disassembly software to dissect the submitted firmware.

(2) Perform vulnerability scanning on the firmware (e.g., checking for known vulnerabilities in the current version.)

(g) Pass criteria:

(1) The firmware does not contain any cybersecurity risk vulnerabilities with a CVSS v3.0 (or newer version) score of 7.0 or higher.

(h) Value

The firmware does not pose significant cybersecurity risks.

5.6.1.3 Firmware Source Code Protection

(a) Compliance:

Section 5.6.1.3 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether the firmware contains only executable form of code.

(d) Precondition:

The firmware is in executable format (e.g., EXE).

(e) The vendors shall attach the following information:

(1) Provide the firmware in executable format.

(2) Declare the format of the firmware after packaging.

(f) Test method:

(1) Attempt reverse engineering on the firmware file.

(2) Verify if the disassembled file contains source code, object code, or just-in-time compiled code.

(g) Pass criteria:

(1) The firmware contains only executable form of code, and does not include source code, object code, or just-in-time compiled code.

(h) Value

Ensures the security of source code, object code, or just-in-time compiled code, preventing unauthorized disclosure.

5.6.2 Firmware Protection

5.6.2.1 Integrity Mechanism Review

(a) Compliance:

Section 5.6.2.1 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To review the documentation provided by the vendor for compliance with integrity mechanism requirements.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Firmware integrity specification:

i. Declare whether the integrity mechanism is implemented internally or by another chip. If implemented by another chip, provide proof of its integrity testing.

ii. Declare the integrity mechanism used (e.g., EDC, hash, MAC, DSA), and if EDC is used, additional declarations are required:

1. Length of EDC.
2. Declare the EDC algorithm used.

3. Describe the calculation method of EDC.

iii. Explain the verification process and content for the following of the TOE:

1. Recalculate the check value when starting the integrity check.

2. Compare the stored check value with the recalculated check value.

3. Expected outputs when integrity check succeeds or fails.

(2) Firmware integrity proof:

i. Provide proof that integrity technology has been applied to the firmware.

(f) Test method:

(1) If EDC is used, verify that the EDC length is at least 16 bits.

(2) If EDC is used, confirm that the provided specification includes the following information:

i. The EDC algorithm used.

ii. The verification process and content of EDC.

(3) If EDC is not used, confirm that the algorithm used complies with the requirements of Appendix B.

(4) Verify that the provided specification meets this requirement.

(5) Ensure that the provided test report is sufficient to demonstrate the application of integrity technology to firmware protection.

(g) Pass criteria:

(1) If EDC is used, the EDC length is at least 16 bits.

(2) If EDC is used, the provided specification includes the following information:

i. The EDC algorithm used.

ii. The verification process and content of EDC.

(3) If EDC is not used, the algorithm used complies with the requirements of Appendix B.

(4) The provided specification meets this requirement.

(5) The provided proof of integrity is sufficient to demonstrate its application to firmware.

(h) Value

The integrity mechanism of the firmware complies with the standard.

5.6.2.2 Authenticity Mechanism Review

(a) Compliance:

Section 5.6.2.2 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To review the documentation provided by the vendor for compliance with authenticity mechanism requirements.

(d) Precondition:

None.

(e) The vendors shall attach the following information:

(1) Firmware authenticity specification:

i. Declare the method by which firmware ensures its security:

1. Single MAC or DSA.

2. Multiple disjoint MACs or DSAs.

ii. Declare whether the authenticity mechanism is implemented internally or by another chip. If implemented by another chip, provide proof of its authenticity testing.

(2) Firmware authenticity proof:

i. Provide the proof that the authenticity mechanism has been applied to the firmware.

(3) If implementing MAC, additionally provide the following specifications:

i. Storage location of the encryption key used by the authenticity technology.

ii. Comprehensive explanation of MAC calculation and verification processes.

(4) If implementing DSA, additionally provide the following specifications:

i. Storage location of the encryption key used by the authenticity technology.

ii. Comprehensive explanation of DSA calculation and verification processes.

iii. Declaration of the storage location of the key used for digital signatures.

(f) Test method:

(1) If the authenticity technology of the firmware is MAC, the testing method is as follows:

i. Verify that the provided specification includes a comprehensive explanation of the MAC calculation and verification processes.

ii. Verify that the key used by the authenticity technology is stored in the key storage or encrypted.

iii. Verify that the provided specification meets this requirement.

iv. Verify that the provided proof is sufficient to demonstrate the application of authenticity technology to firmware.

(2) If the authenticity technology of the firmware is DSA, the testing method is as follows:

i. Verify that the provided specification includes a comprehensive explanation of the DSA calculation and verification processes.

ii. Verify that the key used by the authenticity technology and the key used for digital signatures are stored in the key storage or encrypted.

iii. Verify that the provided specification meets this requirement.

iv. Verify that the provided proof is sufficient to demonstrate the application of authenticity technology to firmware.

(3) Verify that the algorithm used complies with the requirements of Appendix B.

(g) Pass criteria:

(1) If the authenticity technology of the firmware is MAC, the pass criteria are as follows:

   i. The provided specification includes a comprehensive explanation of the MAC calculation and verification processes.

   ii. The key used by the authenticity technology is stored in the key storage or encrypted.

   iii. The provided specification meets this requirement.

   iv. The provided proof is sufficient to demonstrate the application of authenticity technology to firmware.

   v. The MAC algorithm used complies with the requirements of Appendix B.

(2) If the authenticity technology of the firmware is DSA, the pass criteria are as follows:

   i. The provided specification includes a comprehensive explanation of the DSA calculation and verification processes.

   ii. The key used by the authenticity technology and the key used for digital signatures are stored in the key storage or encrypted.

   iii. The provided specification meets this requirement.

   iv. The provided proof is sufficient to demonstrate the application of authenticity technology to firmware.

   v. The DSA algorithm used complies with the requirements of Appendix B.

(h) Value

The TOE can verify the authenticity of the firmware, preventing it from being counterfeited.

5.6.2.3 Integrity Mechanism Protection

(a) Compliance:

Section 5.6.2.3 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify if the firmware has implemented an integrity mechanism.

(d) Precondition:

Pass the test of <5.6.2.1 Integrity Mechanism Review>.

(e) The vendor shall attach the following information:

(1) Updatable firmware files.

(2) Declaration of the expected output of the integrity check, indicating success or failure.

(3) Proof of the generation of a temporary value reset during the integrity check.

(f) Test method:

(4) If using EDC, check if the EDC length of the firmware is at least 16 bits.

(5) Tamper with the firmware file and perform a firmware update.

(6) Verify if the update is successful and if the output matches the declaration by the vendor.

(7) Use the updatable firmware file provided by the vendor and perform a firmware update.

(8) Verify if the output of a successful update matches the declaration by the vendor.

(9) Verify the effectiveness of the proof of resetting the temporary value.

(10) Tamper with the pre-stored checksum values (e.g., EDC, hash, MAC, DSA) of the firmware and perform a firmware update.

(11) Verify if tampering with the stored checksum values is detected or if tampering is prevented.

(g) Pass criteria:

(1) If using EDC, the EDC length is at least 16 bits.

(2) Tampered firmware cannot be successfully updated.

(3) Detection of tampering with stored checksum values or prevention of tampering with stored checksum values.

(4) Firmware update results, both success and failure, match the declaration by the vendor.

(5) Use effective methods to reset temporary values.

(h) Value

The firmware used in the TOE implements a mechanism for protecting its integrity, preventing users from inadvertently using tampered firmware.

5.6.2.4 Authenticity Mechanism Protection

(a) Compliance:

Section 5.6.2.4 of Security Standard for ICT Product Supply Chain Part 2: System Software Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify if the firmware has implemented an authenticity protection mechanism.

(d) Precondition:

Pass the test of <5.6.2.2 Authenticity Mechanism Review >.

(e) The vendor shall attach the following information:

(1) Updatable firmware files.

(2) Declaration of the expected state in case of authenticity check failure.

(3) Proof of the generation of a temporary value reset during the authenticity check.

(f) Test method:

(1) If the firmware's authenticity technology is MAC, the test method is as follows:

i. Tamper with the firmware file and perform a firmware update.

ii. Verify if the update can be successfully completed. If the update fails, check if the expected state matches the declaration by the vendor.

iii. Verify the effectiveness of the proof of resetting the temporary value.

(2) If the firmware's authenticity technology is DSA, the test method is as follows:

i. Verify if the firmware performs DSA signing.

ii. Tamper with the firmware file and perform a firmware update.

iii. Verify if the update can be successfully completed. If the update fails, check if the expected state matches the declaration by the vendor.

iv. Verify the effectiveness of the proof of resetting the temporary value.

(g) Pass criteria:

(1) If the firmware's authenticity technology is MAC, the pass criteria are as follows:

i. Tampered firmware cannot be successfully updated.

ii. The expected state in case of authenticity check failure matches the declaration by the vendor.

iii. Use effective methods to reset temporary values.

(2) If the firmware's authenticity technology is DSA, the pass criteria are as follows:

i. The firmware performs DSA signing.

ii. Tampered firmware cannot be successfully updated.

iii. The expected state in case of authenticity check failure matches the declaration by the vendor.

iv. Use effective methods to reset temporary values.

(h) Value

Prevent users from updating the firmware with forged versions.

Appendix A: Self-Assessment Items (Level 1)

Level 1 self-assessment is based on the corresponding self-assessment items developed according to the "Security Standard for ICT Product Supply Chain Part 2: System Software Security". Assessment items should be truthfully filled out by the vendor based on the security features provided by the TOE.

Table 3. Level 1 Self-Assessment Form for Vendor

Standard Requirements Items	Standard Requirements	Meet or not		
		Yes	Partial	No
5.1.1.1	The component shall have unique identification information and be correctly identified.			
	(Describe the procedure and provide supporting evidence.)			
5.1.2.1	The component shall provide recognizable known operating states.			
	(Describe the procedure and provide supporting evidence.)			
5.1.3.1	The component shall offer a secure component update functionality in the user environment.			
	(Describe the procedure and provide supporting evidence)			
5.2.1.1	The component shall use cryptography algorithms that comply with international standard requirements or widely accepted security industry practices, such as security algorithms approved by NIST SP 800-140C or higher.			
	(Describe the procedure and provide supporting evidence.)			
5.2.2.1	The key generation algorithm used by the component shall use a cryptographic algorithm that meets the requirements of international standards, such as NIST SP 800-133 Rev. 2.			
	(Describe the procedure and provide supporting evidence.)			
5.2.2.2	CSPs stored in KeyStore shall protect their authenticity, integrity and confidentiality.			
	(Describe the procedure and provide supporting evidence.)			
5.2.3.1	The random number generation algorithm used in the component shall comply with the requirements of international standards, or meet the recognized industry practices in the field of information security, such as NIST SP 800-90A, NIST SP 800-90B or a cryptographic algorithm of equal or higher level approved by AIS31, and also the generated random numbers shall pass the NIST SP 800-22 randomness test.			

Standard Requirements Items	Standard Requirements	Meet or not		
		Yes	Partial	No
	(Describe the procedure and provide supporting evidence.)			
5.3.2.1	The component shall have the capability to verify the authenticity of application.			
	(Describe the procedure and provide supporting evidence.)			
5.3.3.1	The component shall deliver secure application installation functionality within user environments and also in potentially insecure manufacturing sites.			
	(Describe the procedure and provide supporting evidence.)			
5.3.3.2	The component shall offer secure application update functionality in user environments.			
	(Describe the procedure and provide supporting evidence.)			
5.3.3.3	The component shall provide secure uninstallation functionality, destroying application data to prevent potential attackers from gaining sensitive and personal information through physical contact.			
	(Describe the procedure and provide supporting evidence.)			
5.4.1.1	All data stored by the application shall be protected for authenticity and integrity.			
	(Describe the procedure and provide supporting evidence.)			
5.4.1.2	The component shall use encryption to protect the confidentiality and integrity of stored data.			
	(Describe the procedure and provide supporting evidence.)			
5.4.1.3	Data stored outside the direct control of the component and not included in the exception list shall be protected.			
	(Describe the procedure and provide supporting evidence.)			
5.4.3.1	The component shall provide a secure method for log generation and storage.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.1	The secure channel protocol used by the component shall comply with security standards, such as TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384 of TLS 1.2, etc.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.2	The communication protocol implemented by the component shall match the declaration.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.3	The component shall only provide the necessary network services required for operation.			
	(Describe the procedure and provide supporting evidence.)			

Standard Requirements Items	Standard Requirements	Meet or not		
		Yes	Partial	No
5.6.1.1	The firmware shall not contain plaintext CSP, undisclosed IP, URL, and email.			
	(Describe the procedure and provide supporting evidence.)			
5.6.1.2	The firmware shall not have vulnerabilities assessed in the Common Vulnerability Scoring System (CVSS) v3 with a severity rating of high for cybersecurity risk vulnerabilities.			
	(Describe the procedure and provide supporting evidence.)			
5.6.2.1	The firmware shall have an integrity verification mechanism, and the algorithms used shall adhere to international standard requirements or the best practices of recognized security industry conventions.			
	(Describe the procedure and provide supporting evidence.)			
5.6.2.2	The firmware shall have an authenticity verification mechanism, and the keys used for authenticity shall be protected.			
	(Describe the procedure and provide supporting evidence.)			
5.6.2.3	The firmware shall have an integrity protection mechanism to prevent users from updating tampered firmware			
	(Describe the procedure and provide supporting evidence.)			
5.6.2.4	The firmware shall have an authenticity protection mechanism to prevent users from updating forged firmware.			
	(Describe the procedure and provide supporting evidence.)			

Appendix B: Applicable cryptographic algorithms and suites

The cryptographic algorithms and suites used in this specification shall adhere to the following requirements (choose one):

- NIST Special Publication 800-140C, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759
- NIST Special Publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generatio
- NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- BSI AIS31, A proposal for: Functionality clases for random number generators
- GlobalPlatform Technology, Cryptographic Algorithm Recommendations Version 2.0, Public Release, June 2021, Document Reference: GP_TEN_053

The cryptographic suites selected for the secure channel (TLS) should adhere to the following requirements:

- TLSv1.2
  - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
  - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
  - TLS_ECDHE_RSA_WITH_AES256_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
  - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

Appendix C: The interrelation among each test item

The interrelation among each test item is as shown in Table 4.

Table 4. The correlation between test items

Test Item Name	Test Precondition
5.1.1.1 System Software Identity Verification	—
5.1.2.1 Secure Boot	—
5.1.3.1 Software Security Update	—
5.2.1.1 Cryptographic Operation	—
5.2.2.1 Key Generation	—
5.2.2.2 Key Storage	—
5.2.3.1 Random Number Generator	—
5.3.1.1 Application Component Isolation	—
5.3.2.1 Application Authenticity	—
5.3.2.2 Application State Attestation	Pass the test of <5.3.2.1 Application Authenticity>
5.3.3.1 Application Secure Installation	—
5.3.3.2 Application Secure Update	—
5.3.3.3 Application Secure Uninstallation	—
5.4.1.1 Data Storage Authenticity and Integrity	—
5.4.1.2 Data Storage Confidentiality	—
5.4.1.3 External Storage	—
5.4.2.1 Data Sanitization	—
5.4.3.1 Audit Log Generation and Storage	—
5.4.4.1 Reliable Indicators	—
5.5.1.1 Communication Support	—
5.5.1.2 Communication Enhancement	—
5.5.1.3 Service Minimization	—
5.6.1.1 Sensitive Content Protection	—
5.6.1.2 Firmware Vulnerability Detection	—
5.6.1.3 Firmware Source Code Protection	—
5.6.2.1 Integrity Mechanism Review	—
5.6.2.2 Authenticity Mechanism Review	—
5.6.2.3 Integrity Mechanism Protection	Pass the test of <5.6.2.1 Integrity Mechanism Review>
5.6.2.4 Authenticity Mechanism Protection	Pass the test of <5.6.2.2 Authenticity Mechanism Review >

Appendix E: The correspondence between this specification and SESIP

The security assurance requirements (Security Assurance Requirements) of SESIP are divided into 5 levels: SESIP1, SESIP2, SESIP3, SESIP4, and SESIP5. SESIP1 requires the vendor to conduct self-assessment on the TOE and provide supporting evidence, which is then reviewed by the laboratory. SESIP2 involves black-box testing conducted by the laboratory on the TOE. SESIP3 involves white-box testing conducted by the laboratory on the TOE. SESIP4 and SESIP5 aim to allow authorized laboratories to reuse products certified by SOG-IS/EUCC. As Taiwan is not a member of the European Union, it cannot benefit from the Mutual Recognition Agreement (MRA), which enables the mutual recognition of verification of relevant ICT products between regions participating in the union. Therefore, the alignment between the security requirements of this standard and SESIP is limited to SESIP1 to SESIP3.

The level 1 of this testing specification involves self-assessment by the vendor and providing supporting evidence, which is then reviewed by the laboratory and verified by the Certification Body (CB). It aligns with SESIP1. To enhance the testing efficiency of laboratories and the visibility into products, all relevant test items in this testing specification are conducted as white-box tests. Therefore, products compliant with this standard can skip SESIP2 and directly align with SESIP3 for white-box testing.

The corresponding table between the relevant test items of this testing specification and SESIP Security Functional Requirements (SFR) and SESIP Security Assurance Requirements (SAR) is presented in Table 5 as follows.

Table 5. The correspondence between test items and SESIP

Security Testing Aspects	Security Testing Items	Security Test Specifications	SESIP SFR	SESIP SAR
5.1 System Software Components Security	5.1.1 System Software Identity	5.1.1.1 System Software Identity Verification	3.1.1 Verification of Platform Identity	SESIP1 SESIP3
	5.1.2 System Software Operating Status	5.1.2.1 Secure Boot	3.1.4 Secure Initialization of Platform	SESIP1 SESIP3
	5.1.3 Secure Update	5.1.3.1 Software Secure Update	3.2.4 Secure Update of Application	SESIP1 SESIP3

Security Testing Aspects	Security Testing Items	Security Test Specifications	SESIP SFR	SESIP SAR
5.2 Cryptographic Security	5.2.1 Cryptographic Algorithm Security	5.2.1.1 Cryptographic Operation	3.5.1 Cryptographic Operation	SESIP1 SESIP3
	5.2.2 Key Security	5.2.2.1 Key Generation	3.5.2 Cryptographic Key Generation	SESIP1 SESIP3
		5.2.2.2 Key Storage	3.5.3 Cryptographic KeyStore	SESIP1 SESIP3
	5.2.3 Random Number Generator Security	5.2.3.1 Random Number Generator	3.5.4 Cryptographic Random Number Generation	SESIP1 SESIP3
5.3 Software Security	5.3.1 Isolation Security	5.3.1.1 Application Component Isolation	3.4.5 Software Attacker Resistance: Isolation of Application Parts	SESIP3
	5.3.2 Security Status	5.3.2.1 Application Authenticity	3.1.6 Attestation of Application Genuineness	SESIP1 SESIP3
		5.3.2.2 Application State Attestation	3.1.7 Attestation of Application State	SESIP3
	5.3.3 Install/Update/Uninstall Security	5.3.3.1 Application Secure Installation	3.2.2 Secure Install of Application	SESIP1 SESIP3
		5.3.3.2 Application Secure Update	3.2.4 Secure Update of Application	SESIP1 SESIP3
		5.3.3.3 Application Secure Uninstallation	3.2.5 Secure Uninstall of Application	SESIP1 SESIP3
5.4 Storage Security	5.4.1 Data Protection	5.4.1.1 Data Storage Authenticity and Integrity	3.6.1 Secure Storage	SESIP1 SESIP3
		5.4.1.2 Data Storage Confidentiality	3.6.2 Secure Encrypted Storage	SESIP1 SESIP3
		5.4.1.3 External Storage	3.6.3 Secure External Storage	SESIP1 SESIP3
	5.4.2 Secure Data Destruction	5.4.2.1 Data Sanitization	3.6.4 Residual Information Purging	SESIP3

Security Testing Aspects	Security Testing Items	Security Test Specifications	SESIP SFR	SESIP SAR
	5.4.3 Log Preservation	5.4.3.1 Audit Log Generation and Storage	3.6.5 Audit Log Generation and Storage	SESIP1 SESIP3
	5.4.4 Only-Increasing Counter Preservation	5.4.4.1 Reliable Indicators	3.6.6 Reliable Index	SESIP3
5.5 Communication Security	5.5.1 Protocol Security	5.5.1.1 Communication Support	3.3.1 Secure Communication Support	SESIP1 SESIP3
		5.5.1.2 Communication Enhancement	3.3.2 Secure Communication Enforcement	SESIP1 SESIP3
		5.5.1.3 Service Minimization	—	—
5.6 Firmware Security	5.6.1 Firmware Content Security	5.6.1.1 Sensitive Content Protection	—	—
		5.6.1.2 Firmware Vulnerability Detection	—	—
		5.6.1.3 Firmware Source Code Protection	—	—
	5.6.2 Firmware Protection	5.6.2.1 Integrity Mechanism Review	—	—
		5.6.2.2 Authenticity Mechanism Review	—	—
		5.6.2.3 Integrity Mechanism Protection	—	—
		5.6.2.4 Authenticity Mechanism Protection	—	—

Reference

(1) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions

(2) Security Evaluation Standard for IoT Platforms (SESIP) v1.0 (GP_FST_070)

(3) FIPS 140-3 Security Requirements for Cryptographic Modules

(4) ISO/IEC 15408:2008 Information technology — Security techniques — Evaluation criteria for IT security

(5) ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules

(6) ISO/IEC 17825:2016 Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

(7) Serge Vaudenay. “Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS...”, EUROCRYPT ’02: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 534-546, May 2002

Version Revision History

Version	Date	Summary
V1.0	2022/07/25	First edition