TEEMA

Industrial Standard

Security Testing Specification for ICT Product Supply Chain Part 1: Chip Security

V1.0

Taiwan Electrical and Electronic Manufacturers' Association

November 2022

Table of contents

Abstract

In light of the control requirements for modern national defense and various critical infrastructure related to civilian needs, support from Information and Communication Technology (ICT), including computers, electronic devices, and communication technologies, is essential. As the core of ICT, chips provide an unprecedented level of precision control for various digital devices, driving economic and scientific advancements. The security of chips, serving as the core for precise computation, is a prerequisite for the normal operation of various critical devices.

Taiwan semiconductor industry holds a significant position in the global ICT supply chain. Ensuring that the products provided meet certain safety standards has become a focal point of attention. Therefore, with the support of the Administration for Digital Industries of the Ministry of Digital Affairs, and the Department of Industrial Technology of Ministry of Economic Affairs, this specification is formulated. It explicitly outlines the testing items for chip-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 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.

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 specified in this specification are based on chip security, encompassing the security of the chip itself (e.g., resistance to side-channel attacks), chip design security (e.g., potential presence of suspicious logic gates in RTL circuits), robustness testing for chip cryptographic module protection, and testing for the integrity and authenticity of chip firmware. As chips require a printed circuit board (PCB) as a carrier for operation, this specification includes physical security as one of the testing items. It defines the security of debugging interfaces to reduce the likelihood of malicious actors compromising chip security through debugging interfaces. This specification does not exhaustively list all cybersecurity testing items, so users may need additional methods to ensure the security of their products.

The scope of this specification applies to the chip layer, corresponding to its level in the supply chain, as illustrated by the red box in Figure 1 below.

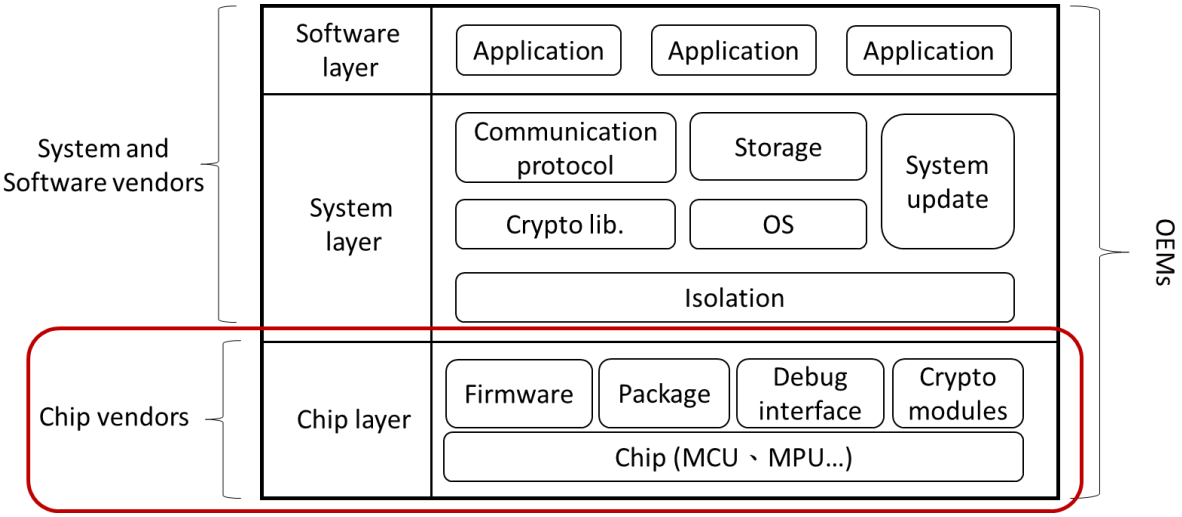

Figure 1 Scope of Testing Specification for Chip Security

The scope of applicability for this specification is delineated as illustrated in Table 1.

Table 1 Scope of application of this specification

Security Aspects	The Subject of Testing	The Applicable Scope
Chip Security	Chip Core	The TOE provides hardware cryptographic module.
	Chip Design	Netlist, RTL file
	Chip Security Module Protection	The TOE provides hardware cryptographic module.
Physical Interface Security	Debug Interface	The TOE provides debug interface.
	Functional Protection	The TOE provides security or basic functionality.
Hardware Components Security	Chip Identity	The TOE provides hardware identity verification.
	Hardware Operating Status	The TOE provides secure boot functionality.
	Secure Update	The TOE provides update function.
	Factory Reset	The TOE can be securely reset.
	Isolation Security	The TOE provides hardware security isolation functionality.
Cryptographic Security	Cryptographic Algorithm Security	T The OE uses encryption algorithm.
	Key Security	The TOE uses cryptographic keys.
	Random Number Generator Security	The TOE uses random numbers.
Firmware Security	Firmware Protection	The TOE contains firmware.

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 1: Chip Security V1.0, 2022

3. Terms and Definitions

Security Standard for ICT Product Supply Chain Part 1: Chip Security V1.0, and the following terms and definitions apply to this specification.

3.1 SNR (Signal-to-Noise Ratio)

SNR is a metric commonly used in science and engineering to compare the strength of the desired signal to the strength of background noise. It is defined as the ratio of signal power to noise power, expressed in decibels (dB). Generally, a higher SNR value indicates better signal quality. In this context, the term "signal" refers to the electronic signal that needs to be processed by a device, while "noise" refers to the irregular additional signals generated by the device, which did not exist in the original signal. Moreover, such signals do not vary with changes in the original signal.

3.2 EDC (Error detection code)

EDC is a technique for reliably transmitting digital data over an unreliable communication channel. Many communication channels are disturbed by channel noise, so error detection techniques are able to detect but not correct unintentional changes in data

3.3 Hash

A hash function, also known as a cryptographic hash algorithm, is a method of creating small digital "fingerprints" from any type of data. The collision-resistant hash function means that it is difficult to find different data that produces the same hash value, which can be used to confirm the integrity of the data.

3.4 MAC (Message Authentication Code)

MAC, also known as Keyed-hash Message Authentication Code, is a message authentication code generated by a special calculation method using a cryptographic hash function combined with an encryption key. It can be used to ensure the integrity of data and can be used as an authentication of messages.

3.5 DSA (Digital Signature Algorithm)

DSA is one of the US federal digital signature standards, based on the complexity of modular arithmetic and discrete logarithms. DSA is a variant of the Schnorr and ElGamal signature schemes. The security of the DSA algorithm is based on the modular arithmetic and the

discrete logarithm problem, which are considered intractable problems. The algorithm uses a key pair consisting of a public key and a private key. The private key is used to generate a digital signature of the message, which can be verified using the signer's corresponding public key. Digital signatures provide message authentication (the recipient can verify the origin of the message), integrity (the recipient can verify that the message has not been modified since it was signed), and non-repudiation (the sender cannot falsely claim that they did not sign the message).

3.6 TOE (Target of Evaluation)

According to Common Criteria, TOE refers to the information system, part of a system or product and all related documentation that is the subject of a security evaluation.

4. Test Item Level

This section formulates the corresponding security testing items and methods based on the Security Standard for ICT Product Supply Chain Part 1: Chip Security V1.0.

The overall table of testing specification levels, as shown in Table 2, includes the following columns: Security Testing Aspects (such as Chip Security, Physical Interface Security, Hardware Component Security, Cryptographic Security, and Firmware Security), Security Testing Items designed corresponding to the security testing aspects, and the Security Level based for each security testing item.

According to (1) the security requirements that the chip layer should have, and (2) the complexity of security technology implementation, the security level is divided into three levels: Level 1, Level 2, and Level 3. The component shall pass the test of the lower security level before proceeding to the test of the advanced level. The test items in the security levels can be divided into two categories: M and O, as follows:

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

For component 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

<table>
<tr><th rowspan="2">Security Testing Aspects</th><th rowspan="2">Security Testing Items</th><th colspan="3">Security Levels</th></tr>
<tr><th>Level 1</th><th>Level 2</th><th>Level 3</th></tr>
<tr><td rowspan="3">5.1 Chip Security</td><td>5.1.1 Chip Core</td><td rowspan="5">The vendor conducts self-assessment and provides supporting evidence, which is then evaluated by the laboratory</td><td>—</td><td>5.1.1.1 (M)
5.1.1.2 (M)
5.1.1.3 (O)
5.1.1.4 (O)</td></tr>
<tr><td>5.1.2 Chip Design</td><td>—</td><td>5.1.2.1 (O)</td></tr>
<tr><td>5.1.3 Chip Security Module Protection</td><td>—</td><td>5.1.3.1 (M)
5.1.3.2 (M)
5.1.3.3 (O)</td></tr>
<tr><td rowspan="2">5.2 Physical Interface Security</td><td>5.2.1 Debug Interface</td><td>5.2.1.1 (M)
5.2.1.2 (O)</td><td>—</td></tr>
<tr><td>5.2.2 Functional Protection</td><td>—</td><td>5.2.2.1 (M)</td></tr>
</table>

Security Testing Aspects	Security Testing Items	Security Levels		
		Level 1	Level 2	Level 3
5.3 Hardware Components Security	5.3.1 Chip Identity		5.3.1.1 (M) 5.3.1.2 (M) 5.3.1.3 (M)	—
	5.3.2 Hardware Operating Status		5.3.2.1 (M) 5.3.2.2 (M)	—
	5.3.3 Secure Update		5.3.3.1 (M)	—
	5.3.4 Factory Reset		5.3.4.1 (M) 5.3.4.2 (O) 5.3.4.3 (O)	—
	5.3.5 Isolation Security		5.3.5.1 (M)	5.3.5.2 (M)
5.4 Cryptographic Security	5.4.1 Cryptographic Algorithm Security		5.4.1.1 (M)	—
	5.4.2 Key Security		5.4.2.1 (M) 5.4.2.2 (M)	—
	5.4.3 Random Number Generator Security		5.4.3.1 (M)	—
5.5 Firmware Security	5.5.1 Firmware Protection		5.5.1.2 (M) 5.5.1.3 (M) 5.5.1.4 (M) 5.5.1.5 (M)	5.5.1.1 (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

The defined testing items in this specification are primarily formulated by referencing international standards and industry standard specifications. These encompass various threats that the chip layer may encounter. Therefore, to meet the security functionalities required by the Security Standard for ICT Product Supply Chain Part 1: Chip Security, components shall undergo testing in accordance with the specified testing specifications outlined in this section, tailored to different levels.

5.1 Chip Security

5.1.1 Chip Core

5.1.1.1 TA

(a) Compliance:

Section 5.1.1.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3(M)

(c) Test purpose:

Verify whether variations in CSPs during the execution of cryptographic operations result in different processing times, thereby making it susceptible to TA.

(d) Precondition:

The TOE provides a hardware cryptographic module.

(e) The vendor shall attach the following information:

(1) The cryptographic algorithms used.

(2) Declarations outlining the mechanisms protecting the CSP and cryptographic algorithms against TA attacks.

(3) Declarations specifying conditions/modes in which the TOE is susceptible to side-channel analysis.

(4) Explanation of the steps to trigger and determine the start and stop of cryptographic operations to obtain optimal synchronization signals. For example, in test mode, the component can offer an external trigger point to indicate the start and stop of cryptographic operations.

(5) Explanation of the steps to modify CSP and ciphertext for conducting side-channel attack tests.

(f) Test method:

(1) Calibrate the signal for initiating and stopping cryptographic operations.

(2) Execute 1,000 timing measurements using a random CSP and a fixed plaintext string, respectively.

(3) Perform statistical analysis on the timing measurement results, examining execution times and the utilized CSP.

(4) If unable to clearly identify each round's peak, incrementally increase the number of measurements in stages until reaching 10,000.

(5) Using a specific time unit (e.g., microseconds, milliseconds), as a reference, statistically analyze the execution times of all samples. Calculate the dependence between the execution time and CSP within the sample set, determining if it is ≥5%. If it exceeds the threshold, the test does not pass; otherwise, continue with the following steps.

(6) Execute 1,000 timing measurements using a random plaintext string and a fixed CSP, respectively.

(7) If unable to clearly identify each round's peak, incrementally increase the number of measurements in stages until reaching 10,000.

(8) Using a specific time unit (e.g., microseconds, milliseconds) as a reference, statistically analyze the execution times of all samples. Calculate the dependence between the execution time and the plaintext within the sample set, determining if it is ≥5%.

If the execution times in steps (4) and (6) are challenging to measure (e.g., due to noise or delay), use the clock cycle of the TOE as the tolerance value (ε) and perform the following test:

i. Perform test method steps (2) and (6) separately, averaging the execution times of the results to obtain T1 and T1'.

ii. Perform test method steps (2) and (6) separately again, averaging the execution times of the results to obtain T2 and T2'.

iii. Calculate |T1 - T2| = r1, and |T1' - T2'| = r2, respectively verify if r1 and r2 < ε.

(g) Pass criteria:

(1) Unable to perform signal alignment.

(2) The dependency between execution time and CSP is <5%, and the dependency between execution time and plaintext is <5%.

(3) r1 < ε and r2 < ε.

Any one of the results from (1) to (3) is considered satisfactory.

(h) Value:

TA vulnerabilities are often overlooked during the design phase since timing weaknesses only manifest during the implementation stage and may inadvertently be introduced during compiler optimizations. The passing of this test indicates that the chip, through the implemented mitigations during design or implementation, has enhanced its ability to resist Timing Analysis side-channel attacks.

5.1.1.2 SPA/SEMA

(a) Compliance:

Section 5.1.1.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify whether it is possible to identify the execution sequence of cryptographic operations, and consequently discern the corresponding cryptographic algorithm, by collecting a small amount of power consumption or electromagnetic radiation records from the TOE.

(d) Precondition:

(1) The TOE provides a hardware cryptographic module.

(2) Pass the test of <5.1.1.1 TA>.

(e) The vendor shall attach the following information:

(1) The cryptographic algorithm used.

(2) Declarations outlining mechanisms protecting the CSP and cryptographic algorithms against side-channel attacks.

(3) Declarations specifying conditions/modes in which the TOE is susceptible to side-channel analysis.

(4) Explanation of the steps to trigger and determine the start and stop of cryptographic operations to obtain optimal synchronization signals. For example, in test mode, the TOE can provide an external trigger to indicate the start and stop of cryptographic operations.

(5) Explanation of the steps to modify the CSP and plaintext for conducting side-channel attack tests.

(f) Test method:

(1) Calibrate power consumption or electromagnetic radiation signals for initiating and stopping cryptographic operations.

(2) Collect 6 sets of waveforms generated using the following data formats, each waveform containing the Cryptographic Service Provider (CSP) and plaintext:

i. Set 1: Waveform generated with 1 CSP and 1 pre-determined plaintext string;

ii. Set 2: Waveform generated with 1 pre-determined CSP and 1 plaintext string;

iii. Sets 3-6: Four waveforms generated with pairs of 4 random CSPs and 4 random plaintext strings.

(3) For each time period corresponding to each CSP bit, sample at least 100 points for each waveform resolution.

(4) For each collected waveform, calculate the cross-correlation between them, identify similar segments, and discover potential execution sequences corresponding to the cryptographic algorithm.

(g) Pass criteria:

(1) Unable to perform signal alignment.

(2) Unable to calibrate power consumption or electromagnetic radiation signals for initiating and stopping cryptographic operations.

(3) If, during the relevance analysis (through visual or statistical inspection) of all collected waveforms, no irregular execution sequence related to the CSP is identified, then the test is considered passed.

Any one of the results from (1) to (3) is considered satisfactory.

(h) Value

SPA/SEMA can be applicable to most cryptographic algorithms, posing a potential risk in the majority of encryption chips. The passing of this test indicates that the chip, through the implemented mitigations during design or implementation, has enhanced its ability to resist SPA/SEMA side-channel analysis attacks.

5.1.1.3 DPA/DEMA

(a) Compliance:

Section 5.1.1.3 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (O)

(c) Test purpose:

Verify whether it is possible to identify the CSP used by the TOE through DPA/DEMA analysis.

(d) Precondition:

(1) The TOE provides a hardware cryptographic module.

(2) Pass the test of <5.1.1.2 SPA/SEMA>.

(e) The vendor shall attach the following information:

(1) The cryptographic algorithm used.

(2) Declarations outlining mechanisms protecting the CSP and cryptographic algorithms against side-channel attacks.

(3) Declarations specifying conditions/modes in which the TOE is susceptible to side-channel analysis.

(4) Explanation of the steps to trigger and determine the start and stop of cryptographic operations to obtain optimal synchronization signals. For example, in test mode, the TOE can provide an external trigger to indicate the start and stop of cryptographic operations.

(5) Explanation of the steps to modify the CSP and plaintext for conducting side-channel attack tests

(f) Test method:

(1) Using a specified set of CSP provided by the vendor, collect 10,000 waveforms for each CSP using a designated subset A and subset B of test vectors (e.g., TVLA t-test).

(2) Utilize the calibration function of the testing equipment to perform both static and dynamic calibration of the waveforms and calculate SNR.

(3) If the SNR value is sufficient, the laboratory can proceed to the next testing step. Otherwise, methods to enhance measurement quality shall be identified before conducting the test.

(4) Calculate intermediate values of the security function (e.g., AES's SBOX).

(5) For the calibrated and/or pre-processed waveforms, use Welch’s t-test statistical testing to analyze the leaked values C of the CSP.

(g) Pass criteria:

(1) The signal cannot undergo static and dynamic alignment.

(2) In Welch’s t-test, if the values of C for all subsets A and subsets B do not exceed +4.5 or -4.5, then the test is considered passed.

Any one of the results from (1) to (2) is considered satisfactory.

(h) Value

The passing of this test for the chip indicates that the mitigations implemented during the design or implementation stages enhance the chip's resistance to DPA/DEMA side-channel analysis attacks.

5.1.1.4 DFA/EMFI

(a) Compliance:

Section 5.1.1.4 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (O)

(c) Test purpose:

Verify Check whether it is possible to induce stable abnormal outputs in the TOE or potential CSP leakage issues through DFA/EMFI attacks.

(d) Precondition:

The TOE provides a hardware cryptographic module.

(e) The vendor shall attach the following information:

(1) The cryptographic algorithm used.

(2) Declarations outlining mechanisms protecting the CSP and cryptographic algorithms against DFA/EMFI attacks.

(3) Explanation of the steps to trigger and determine the start and stop of cryptographic operations to obtain optimal synchronization signals. For example, in test mode, the TOE can provide an external trigger to indicate the start and stop of cryptographic operations.

(4) Explanation of the steps to modify the CSP and plaintext for conducting the test.

(f) Test method:

(1) Perform calibration of power consumption or electromagnetic radiation signals for initiating and stopping cryptographic operations.

(2) Execute multiple encryption operations using different CSP and plaintexts, simultaneously collecting waveforms and recording output values.

(3) After processing the waveforms (e.g., applying low-pass filtering, signal alignment), identify the waveform for each round of encryption operations.

(4) Set fault injection parameters and perform encryption operations again, injecting faults during the encryption process.

(5) Confirm whether the output values in step (4) match the results from step (2) and repeat step (4) until a stable fault causing output errors is identified. Ensure that this fault does not result in the restart, destruction, or halt of the TOE.

(6) Confirm the relevance and regularity of each set of error output results with their corresponding CSP and plaintext combinations.

(g) Pass criteria:

(1) The signal cannot undergo static and dynamic alignment.

(2) Unable to identify a fault injection that can consistently cause output errors.

(3) No apparent correlation or regularity found between each set of error output results and their corresponding CSP and plaintext combinations.

Any one of the results from (1) to (3) is considered satisfactory.

(h) Value

The passing of this test for the chip indicates that the mitigations implemented during the design or implementation stages enhance the chip's ability to resist DFA/EMFI attacks.

5.1.2 Chip Design

5.1.2.1 Suspicious Circuit Testing

(a) Compliance:

Section 5.1.2.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (O)

(c) Test purpose:

Verify whether there is a suspected hardware Trojan circuit design in the chip.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) The vendor is required to provide a report file containing the results after executing the suspicious circuit detection tool on the chip.

(f) Test method:

(1) Execute the suspicious circuit detection tool.

(2) Select the target RTL code or netlist file for analysis.

(3) Send the execution result report to the laboratory for analysis.

(g) Pass criteria:

(1) No suspicious circuit found in the execution result report.

(h) Value

Reduce the risk of hardware Trojan implantation during the chip design process.

5.1.3 Chip Security Module Protection

5.1.3.1 General Protection of Chip Cryptographic Module

(a) Compliance:

Section 5.1.3.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify the chip's cryptographic module to determine if it employs more secure materials and coatings, and assess the potential risk of leakage during physical maintenance.

(d) Precondition:

The TOE provides a hardware cryptographic module.

(e) The vendor shall attach the following information:

(1) Provide evidence that the cryptographic module is of production-grade quality.

(2) Provide evidence of the cryptographic module having a covering passivation material (e.g., applying conformal or sealing coating on the chip's cryptographic module).

(3) Declare the mechanism for zeroing the cryptographic module.

(4) Declare the included CSP in the cryptographic module.

(5) Explain the steps to review all plaintext CSP.

(6) Describe the steps for physical maintenance.

(f) Test method:

(1) Review the supporting documents to verify if the TOE is composed of production-grade components that include standard passivation technology.

(2) After performing physical maintenance, verify whether zeroing has been carried out or if it is required according to the procedure before viewing and using the TOE.

(g) Pass criteria:

(1) The cryptographic module shall be composed of production-grade components.

(2) The cryptographic module components shall have a covering passivation coating.

(3) During physical maintenance, all CSP contained in the cryptographic module shall be zeroed by the operator following the procedure or automatically by the cryptographic module itself.

(h) Value

Mitigate the probability of CSP leakage during the access of the cryptographic module through physical maintenance procedures.

5.1.3.2 Basic Protection of Chip Cryptographic Module

(a) Compliance:

Section 5.1.3.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify whether evidence of tampering or removal is retained when the chip's cryptographic module is subjected to alteration or removal.

(d) Precondition:

(1) The TOE provide a hardware cryptographic module.

(2) Pass the test of <5.1.3.1 General Protection of Chip Cryptographic Module>.

(e) The vendor shall attach the following information:

(1) Provide the documentation required for testing in <5.1.3.1 General Protection of Chip Cryptographic Module>.

(2) Provide evidence of the use of tamper-evident and opaque hard coating materials (e.g., corrosion-resistant coating, tinted coating, and hard opaque epoxy resin with passivation layer) on the chip password module.

(3) Declare the mechanism for preserving evidence when the chip cryptographic module is tampered with or removed.

(f) Test method:

(1) Review the proof documents.

(2) Confirm whether the proof documents comply with the requirements of this test item.

(3) Attempt to tamper with or remove the module through physical means, such as trying to peel, pry, or chemically corrode the protective material on the module.

(4) Confirm whether there is evidence of tampering or removal being preserved.

(g) Pass criteria:

(1) The cryptographic module is covered with anti-tamper and opaque hard anti-tamper coating or encapsulating material, and evidence of tampering or removal of the module is retained.

(h) Value

When the chip cryptographic module is tampered with or removed, retaining evidence of tampering or removal can enhance user awareness.

5.1.3.3 Advanced Protection of Chip Cryptographic Module

(a) Compliance:

Section 5.1.3.3 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (O)

(c) Test purpose:

When the chip cryptographic module is subjected to physical attacks, it should have a mechanism to record tampering responses.

(d) Precondition:

(1) The TOE provides a hardware cryptographic module.

(2) Pass the test of <5.1.3.2 Basic Protection of Chip Cryptographic Module>.

(e) The vendor shall attach the following information:

(1) Provide the documentation required for testing in <5.1.3.2 Basic Protection of Chip Cryptographic Module>.

(2) Declare the mechanism for tamper response, such as log records, alert notifications, and triggering conditions.

(f) Test method:

(1) Attempt to access the module physically.

(2) Confirm if there is a tamper response after the attempt.

(g) Pass criteria:

(1) There is a response after the chip's cryptographic module has been tampered with.

(h) Value

Users can obtain anomaly notifications or records through the tamper response log mechanism of the chip's cryptographic module.

5.2 Physical Interface Security

5.2.1 Debug Interface

5.2.1.1 Secure Debugging

(a) Compliance:

Section 5.2.1.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2(M)

(c) Test purpose:

Verify whether the services provided by the debugging interface are prone to abuse.

(d) Precondition:

The TOE provides a debugging interface.

(e) The vendor shall attach the following information:

(1) A “Debugging Interfaces List,” which describes each debugging interface's purpose and necessity.

(2) The authentication mechanism of the debugging interfaces and the used cryptographic algorithm (please refer to Appendix B).

(3) An "Exception Data List," which lists the data not protected during the debugging period, and describes why the data is not necessary to be protected. These exception data shall not include application data that can identify the user's data.

(4) The login CSP (such as password) used by the authentication mechanism.

(f) Test method:

(1) Review whether the description of the “Debugging Interfaces List” is reasonable.

(2) Review whether the description of the “Exception Data List” is reasonable.

(3) Inspect the appearance of the TOE.

(4) Attempt to access the debug interface using both non-authenticated and failed authentication methods for the identified debug interfaces.

(5) Confirm whether the access is successful.

(6) Access the debug interface after normal authentication and attempt to access application data beyond the “Exception Data List.”

(7) Confirm whether successful access is possible.

(g) Pass criteria:

(1) The description of the “Debugging Interfaces List” is reasonable.

(2) The description of the "Exception Data List" is reasonable.

(3) The debugging interface contains only the authentication mechanism announced by the vendor, and the debugging functions support identity authentication.

(4) In debug mode, all data stored in the application (except the "Exception Data List") cannot be accessed.

(h) Value

The debug interface has identity verification and can only access data within the "Exception Data List."

5.2.1.2 Secure Debugging Authentication

(a) Compliance:

Section 5.2.1.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (O)

(c) Test purpose:

Verify the security of the authentication function used by the secure debugging interface.

(d) Precondition:

The TOE provides a debugging interface.

(e) The vendor shall attach the following information:

(1) Provide the documentation required for testing in <5.2.1.1 Secure Debugging>.

(2) Declare the “Identity Role Permissions List” and provide explanations for the content, purposes, and necessity of the identity role permissions.

(3) A “Accessible Data List” corresponding to “Identity Role Permissions List,” explain the reasons for authorizing access to that data.

(f) Test method:

(1) Review whether the description of the “Identity Role Permissions List” is reasonable.

(2) Review whether the description of “Accessible Data List" is reasonable.

(3) Enter debug mode according to the debugging interface operation method.

(4) Complete identity authentication.

(5) Confirm that the “Accessible Data List” is consistent with “Identity Role Permissions List.”

(6) Attempt to access “Accessible Data List” that does not match “Identity Role Permissions List.”

(7) Attempt to obtain identities with higher privileges.

(8) Confirm whether the debug mode of the identity can be entered.

(g) Pass criteria:

(1) The description of “Identity Role Permissions List” is reasonable.

(2) The description of “Accessible Data List” is reasonable.

(3) The “Identity Role Permissions List” under debug mode is consistent with the announcement of “Accessible Data List.”

(4) Unable to enter debug mode with identities with higher privileges.

(5) Unable to access data lists that do not match the identity role permissions.

(h) Value

Secure authentication can reduce the risk of sensitive data leakage through the debugging interface.

5.2.2 Functional Protection

5.2.2.1 Security and Essential Function Protection

(a) Compliance:

Section 5.2.2.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify whether the TOE can detect or prevent anomalies in security functions or essential functions caused by attackers.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) A list of security functions that may expose CSP.

(2) Identity the functions required to operate the TOE.

(3) A list of physical access interfaces (JTAG, UART, USB, SD card, etc.) of the TOE.

(4) The steps to use each access interface.

(5) A data sheet that includes the specification of the TOE.

(6) The operational environment of the TOE and the physical attacks that may occur.

(7) The security mechanism that the TOE detects or prevents physical access from attackers.

(f) Test method:

(1) Perform <5.2.1.1 Secure debugging> and <5.2.1.2 Secure Debugging Authentication> testing.

(2) Verify whether the TOE can detect or prevent anomalies in security functions when an attacker with physical access launches an attack.

(g) Pass criteria:

(1) The TOE is capable of detecting or preventing attacks that could potentially cause anomalies in security functions or essential functions.

(h) Value

The TOE possesses the capability to resist physical attacks.

5.3 Hardware Components Security

5.3.1 Chip Identity

5.3.1.1 Chip Identity Verification

(a) Compliance:

Section 5.3.1.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

The TOE's identity can be accurately recognized through testing.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Explain the steps to view the TOE identification information.

(2) Declare the format of the TOE identification information.

(3) Declare the naming convention for the identification information.

(f) Test method:

(1) Examine the TOE to confirm the presence of identification information and verify if it adheres to the declared naming convention.

(2) Confirm whether the naming convention of the identification information satisfies the requirement for uniqueness (globally).

(g) Pass criteria:

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

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

(h) Value

The TOE can accurately provide unique identification information, thereby verifying that the product used is secure, forming the foundation for compliance checks.

5.3.1.2 Chip Instance Identity Verification

(a) Compliance:

Section 5.3.1.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify if the identity of the hardware instances provided by the TOE, such as "secure" and "non-secure" physical address spaces, can be correctly identified.

(d) Precondition:

The TOE provides hardware instance functionality.

(e) The vendor shall attach the following information:

(1) Explain the steps to view instance identification information.

(2) Declare the format of instance identification information.

(3) Declare the naming convention for identification information.

(f) Test method:

(1) Examine the instances to confirm if identification information is provided and conforms to the declared naming convention.

(2) Confirm if the naming convention for identification information satisfies the requirement for uniqueness (globally).

(g) Pass criteria:

(1) Each instance provides identification information and conforms to the declared naming convention.

(2) The naming convention for identification information satisfies the requirement for uniqueness (globally).

(h) Value

The TOE can accurately provide unique identification information, thereby verifying that the product in use is secure.

5.3.1.3 Chip Genuineness Attestation

(a) Compliance:

Section 5.3.1.3 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Examine the verification method provided by the TOE to determine if it can be used to check the genuineness.

(d) Precondition:

Pass the tests of <5.3.1.1 Chip Identity Verification> and <5.3.1.2 Chip Instance Identity Verification>.

(e) The vendor shall attach the following information:

(1) Provide two TOEs.

(2) Declare methods to prevent TOE identity replication.

(3) Declare actions taken upon discovering a changed identity.

(f) Test method:

(1) Log in to the product management interface and attempt to modify the TOE identity field.

(2) Confirm if modifications can be made without being detected.

(3) If modifications can be made without detection, attempt to copy the TOE identity of Item A to Item B.

(4) Confirm if Item B can operate normally using the identity of Item A.

(5) Import the firmware of Item A into Item B.

(6) Confirm if Item B can operate normally using the identity of Item A.

(g) Pass criteria:

(1) The TOE identity field cannot be modified or modified without detection.

(2) The TOE identity cannot be copied or impersonated.

(h) Value

Users can verify that they possess a genuinely secure product, avoiding insecure or incomplete replicas (clones).

5.3.2 Hardware Operating Status

5.3.2.1 Secure Boot

(a) Compliance:

Section 5.3.2.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the TOE has the ability to check the authenticity and integrity of hardware configurations during initialization (e.g., startup) and the loading of other configurations required for the Operating System (OS) kernel.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Explain the process of TOE initialization.

(2) Declare the method by which the TOE ensures the authenticity and integrity of hardware configurations during initialization and the loading of other configurations required for OS kernel.

(3) Declare the “controlled state list,” listing the states the chip should exhibit when it cannot guarantee the authenticity or integrity of the hardware configuration, and explain how controlled states can be recognized (e.g., warning windows, lights, sounds). Controlled states include known operational states.

(4) Provide detailed explanations for each state in the “controlled state list,” justifying the types of states (e.g., dividing them into three categories) and ensuring coverage of all possible scenarios.

(5) Declare the conditions under which the TOE enters the “controlled state list.”

(6) Explain the steps to trigger a change in the controlled state.

(f) Test method:

(1) Trigger all conditions for changing controlled states.

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

(g) Pass criteria:

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

(2) The controlled state is recognizable

(h) Value

Users can verify the security of the chip's initialization process.

5.3.2.2 Chip State Attestation

(a) Compliance:

Section 5.3.2.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the TOE provides an identifiable known operating state.

(d) Precondition:

Pass the tests of <5.3.1.3 Chip Genuineness Attestation> and <5.3.2.1 Secure Boot>.

(e) The vendor shall attach the following information:

(1) Declare the “Known Operational State List” of the TOE, listing various known operational states of the TOE.

(2) Explain the steps to check the operational state of the TOE.

(3) Declare the conditions triggering all known operational states of the TOE, potentially including logical and physical aspects.

(4) Explain the steps for triggering all known operational states of the TOE.

(f) Test method:

(1) Trigger all conditions for changing controlled states.

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

(g) Pass criteria:

(1) The chip enters the specified known operational state based on the trigger conditions.

(2) The known operational state is recognizable.

(h) Value

Users can verify the chip's operational state at any given time.

5.3.3 Secure update

5.3.3.1 Chip Secure Update

(a) Compliance:

Section 5.3.3.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the TOE provides a secure firmware update function in user environment.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

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

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

(3) Declaration of methods to resist downgrade attacks.

(4) An "Endpoint and Protocol Correspondence Table" in table format, listing all default open communication interfaces, services, and port numbers. Declare the corresponding communication protocols and supported algorithms, such as TLS 1.2 with TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8, or IPSEC, etc. Sufficient information should be provided to accurately describe the quality of the cryptographic algorithms used.

(5) Explanation of the operational steps for performing firmware offline and online updates.

(6) If the vendor provides a test private key, provide the mechanism for digital signatures on the TOE, or else use the lab's self-signed public-private key for testing with the vendor's assistance.

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

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

(f) Test method:

(1) Offline update test

i. Use a newer version of the firmware update file and perform an offline update.

ii. Observe if the installation can be completed successfully.

iii. Observe if the TOE possesses a globally unique identification after the update, using the test method from <5.3.1.1 Chip Identity Verification>.

iv. Use an older version of the firmware update file and perform an offline update (Older version test).

v. Observe if the installation can be completed successfully.

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

vii. Perform an offline update.

viii. Observe if the installation can be completed successfully.

ix. If the vendor provides a test private key (non-original signing key), the lab will use a self-signed private key to sign the update file according to the original signing method provided by the vendor.

x. Perform an offline update.

xi. Observe if the installation can be completed successfully.

xii. If the lab provides a self-signed public-private key to the vendor, the vendor uses that private key to sign the update file (Authenticity test).

xiii. Perform an offline update.

xiv. Observe if the installation can be completed successfully.

xv. Reverse engineer the firmware update file (Confidentiality test).

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

(2) Online update test

i. Execute a packet sniffer tool for packet sniffing.

ii. Perform an online update.

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

iv. Observe if the firmware can be successfully installed and executed.

v. Observe if the TOE possesses a globally unique identification after the update, using the test method from <5.3.1.1 Chip Identity Verification>.

(g) Pass criteria:

(1) Offline update

i. The TOE possesses a globally unique identification after a successful update.

ii. The TOE rejects the installation of older version update files.

iii. The TOE rejects the installation of tampered update files.

iv. If the vendor provides a test private key, the TOE rejects the installation of falsified update files using the self-signed private key provided by the lab.

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

vi. The firmware update file cannot be reverse engineered.

(2) Online update

i. The TOE possesses a globally unique identification after a successful update.

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

iii. 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, allowing users to confidently update firmware instantly when security flaws, functional errors, or improvements are needed.

5.3.4 Factory Reset

5.3.4.1 Hardware Factory Reset

(a) Compliance:

Section 5.3.4.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify if the hardware's factory reset function can destruct user data stored in the product, preventing potential attackers from obtaining sensitive and personal information through physical contact.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Explanation of the steps for using the hardware reset function.

(2) Declaration that after performing the reset function, any "Retained Data List" necessary for the continued operation of the product, such as data needed for <5.3.1.3 Chip Genuineness Attestation> and <5.3.2.2 Chip State Attestation>, will still be retained. Provide a reasoned analysis statement on the list.

(3) Declaration of the data destruction method.

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

(f) Test Method:

(1) Hardware Reset Test:

i. Perform a hardware reset before storing any user data.

ii. Restart the hardware and observe if the product can still operate normally.

(2) Data Recovery Test:

i. Store user data, such as personal information, certificates, or configuration settings, on the product.

ii. Execute steps to trigger an application error and confirm if successful.

iii. Perform a hardware reset.

iv. Check through the system interface if user data has been deleted.

v. Observe if parameters set by applications have been initialized.

vi. Export the contents of non-volatile memory.

vii. Confirm that user data has been destroyed.

(g) Pass criteria:

(1) The product can still operate normally after restoring factory settings, and parameters set by applications are initialized.

(2) In case of application issues, the product can undergo a factory reset, and sensitive and personal data cannot be recovered.

(h) Value:

When disposing of the product (e.g., donation, resale), users can use the hardware factory reset function to destruct sensitive and personal data stored on the product, preventing potential attackers from obtaining sensitive information through physical contact.

5.3.4.2 Hardware Decommission

(a) Compliance:

Section 5.3.4.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (O)

(c) Test purpose:

Verify if the hardware decommission function can destruct applications, sensitive data, and personal information in the product, rendering the product unusable.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Explanation of the steps for using the hardware decommission function.

(2) Declaration of the "Applications Exempt from Decommission Destruction List" and provide a reasoned analysis statement on the list.

(3) Declaration of the data destruction mechanism.

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

(f) Test method:

(1) Store user data, such as personal information, certificates, or configuration settings, on the product.

(2) Execute steps to trigger an application error and confirm if successful.

(3) Execute the hardware decommissioning function and observe if the product can still operate normally.

(4) Export the contents of non-volatile memory.

(5) Confirm if data has been destructed.

(g) Pass criteria:

(1) The TOE provides a decommission function.

(2) The product cannot operate after executing the hardware decommission.

(3) After decommissioning, all applications not marked for exemption are destructed.

(4) In case of application issues, the hardware decommission function can still be executed.

(h) Value

Ensures that after executing the hardware decommission function, applications, sensitive data, and personal information in the product are destructed, and the product is rendered unusable.

5.3.4.3 Hardware Field Return

(a) Compliance:

Section 5.3.4.3 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (O)

(c) Test purpose:

Verify if the field return function can destruct sensitive data and personal information in the product, making it irretrievable by the vendor.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Explanation of the steps for using the hardware return function.

(2) Declaration of the "Data Retained List" after hardware return to vendor, and provide a reasoned analysis statement on the list.

(3) Declaration of the data destruction mechanism.

(f) Test method:

(1) Store sensitive data and personal information on the product.

(2) Execute the field return function.

(3) Export the contents of non-volatile memory.

(4) Confirm if user data has been destructed.

(g) Pass criteria:

(1) Sensitive data and personal information received by the user after executing the field return function are destructed.

(h) Value

Allows users to destruct sensitive data and personal information before returning the product to the supplier, preventing potential attackers and the vendor from accessing such information.

5.3.5 Isolation Security

5.3.5.1 Hardware Isolation

(a) Compliance:

Section 5.3.5.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the hardware isolation function provided by the TOE can isolate applications and hardware security functions.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Declaration of the method for isolating hardware security functions and applications.

(2) Declaration of different modes of permissions.

(3) Declaration of permission modes for all applications.

(4) Explanation of the steps to view application permission modes.

(f) Test method:

(1) View the permission modes of applications.

(2) Confirm whether the permissions of all applications are isolated from hardware security functions.

(g) Pass criteria:

(1) The TOE uses an operating system with kernel-user mode separation or another industry-recognized isolation mode.

(h) Value

The product provides isolation between applications and hardware security functions, preventing attackers from compromising other security functions of the product even if they can perform malicious actions on applications.

5.3.5.2 Hardware Part Isolation

(a) Compliance:

Section 5.3.5.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify whether the hardware part isolation function provided by the TOE can securely isolate hardware part from each other.

(d) Precondition:

The TOE may have potential attack vectors.

(e) The vendor shall attach the following information:

(1) If there are no vulnerable hardware parts, provide a reasonable analysis statement for the list. Otherwise, declare the "Vulnerable Hardware Parts List," listing potential attack vectors, such as network modules, communication modules, memory modules, etc.

(2) Declare the "Protected Hardware Parts List," listing the parts that need protection.

(3) Declare the method of isolating each hardware part.

(4) Provide isolation proofs for each hardware part.

(f) Test method:

(1) Review the isolation proofs for each hardware part.

(2) Confirm whether the proofs meet security requirements.

(3) Attempt to view and tamper with protected hardware parts through vulnerable hardware components.

(4) Confirm if plaintext content can be viewed.

(5) Confirm if tampering can be successful.

(g) Pass criteria:

(1) The isolation proofs for each hardware part meet security requirements.

(2) It is not possible to view or tamper with protected hardware parts through vulnerable hardware parts, ensuring the confidentiality and integrity of protected hardware parts.

(h) Value

The isolation feature provided by the product protects the integrity and confidentiality of parts, reducing the probability of parts being damaged by other parts.

5.4 Cryptographic Security

5.4.1 Cryptographic Algorithm Security

5.4.1.1 Cryptographic Operation

(a) Compliance:

Section 5.4.1.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the TOE uses cryptographic algorithms that comply with standard specifications.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) Declare the “Cryptographic Operation List,” listing the cryptographic operations used, such as encryption, decryption, hash, digital signature, and signature verification.

(2) Declare the “Cryptographic Algorithm List,” listing the cryptographic algorithms used.

(3) Declare the key lengths supported by the cryptographic algorithm.

(4) Declare the operation modes supported by the cryptographic algorithm.

(5) Use a table to list the corresponding algorithms and their supported operations, key lengths, and operation modes for (1) to (4) above.

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

(f) Test method:

(1) Review the attached documents to confirm if the cryptographic operations, algorithms, key lengths, and operation modes used comply with the requirements of Appendix B.

(2) Attempt to encrypt plaintext using the test keys and compare the results with the encryption performed by the TOE.

(3) Confirm whether the two encryption methods and results are consistent.

(g) Pass criteria:

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

(2) The application applies the cryptographic algorithms listed in the “Cryptographic Algorithm List.”

(h) Value

The TOE’s use of cryptographic algorithms that comply with standard specifications reduces the likelihood of data being compromised.

5.4.2 Key Security

5.4.2.1 Key Generation

(a) Compliance:

Section 5.4.2.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify whether the key generation method of the TOE complies with standard specifications.

(d) Precondition:

The TOE provides key generation functionality.

(e) The vendor shall attach the following information:

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

(2) Declare the key lengths supported by the cryptographic algorithm.

(3) Declare the operation modes supported by the cryptographic algorithm.

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

(5) Use a table to correspond algorithms with supported key lengths and operation modes for (1) to (3) above.

(f) Test method:

(1) Review the evidence provided by the vendor to confirm that the generated keys comply with the requirements.

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

(3) Check for the presence of the ROCA (The Return of Coppersmith's Attack) vulnerability in the TOE.

(g) Pass criteria:

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

(2) The TOE does not have the ROCA vulnerability.

(h) Value

The TOE’s use of key generation methods that comply with standard specifications reduces the likelihood of key compromise.

5.4.2.2 Key Storage

(a) Compliance:

Section 5.4.2.2 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Ensure the authenticity, integrity, and confidentiality of the CSP stored in the key storage.

(d) Precondition:

The TOE contains a CSP.

(e) The vendor shall attach the following information:

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

(2) Declare the method used by the key storage to protect CSP (e.g., eFuse, Mask ROM, anti-fuse OTP, etc.).

(3) Declare the method of ensuring the authenticity, integrity, and confidentiality of the key storage.

(4) Explain the access control and permission management mechanism of the key storage.

(5) Provide authorized secure operation permissions for the key storage.

(6) Explain the steps to open the key storage and view its contents.

(f) Test method:

(1) Examine the method used by the key storage to protect CSP to ensure there are no design flaws that could lead to plaintext leakage of CSP.

(2) Examine the packaging used by the key storage to determine if it has anti-tampering design.

(3) Attempt to view the CSP stored in the key storage through authorized secure operation permissions.

(4) Attempt to view the CSP stored in the key storage without authorized secure operation permissions.

(5) Attempt to extract the CSP stored in the key storage through side-channel attack methods (e.g., <5.1.1.3 DPA/DEMA>).

(g) Pass criteria:

(1) The key storage uses a secure storage method to protect CSP.

(2) The packaging used by the key storage has anti-tampering design.

(3) The key storage has a secure access control and permission management mechanism.

(4) The CSP stored in the key storage is protected in ciphertext.

(5) The CSP stored in the key storage cannot be extracted through side-channel attack methods.

(h) Value

The key storage provides protection for the authenticity, integrity, and confidentiality of CSP, preventing unauthorized leakage.

5.4.3 Random Number Generator Security

5.4.3.1 Random Number Generator

(a) Compliance:

Section 5.4.3.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

Verify if the random number generation algorithm complies with standard specifications.

(d) Precondition:

The TOE provides the functionality of random number generation.

(e) The vendor shall attach the following information:

(1) Declaration of the cryptographic algorithm used for random number generation.

(2) Declaration of the “Entropy Source List,” outlining the sources from physical and computational resources for generating random numbers.

(3) Submission of evidence that the random numbers generated by the vendor adhere to the declarations in (1) and (2).

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

(f) Test method:

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

(6) Confirm whether the random number generation algorithm adheres to the requirements in Appendix B.

(7) Verify if the entropy sources for random number generation comply with the requirements in Appendix B.

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

(g) Pass criteria:

(1) The compliance evidence for random number generation meets the specified requirements.

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

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

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

(h) Value

Ensuring that the random number generation method aligns with standard specifications guarantees the generation of more secure random numbers by the TOE, suitable for use in cryptographic algorithms.

5.5 Firmware Security

5.5.1 Firmware Protection

5.5.1.1 Firmware Extraction Protection

(a) Compliance:

Section 5.5.1.1 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 3 (M)

(c) Test purpose:

Verify whether the firmware used in the chip can be extracted for analysis.

(d) Precondition:

None.

(e) The vendor shall attach the following information:

(1) If programming pins exist, provide the operational tools for firmware programming interfaces.

(2) If programming pins exist, explain the steps for reading the firmware.

(f) Test method:

(1) Visually inspect whether programming pins for the chip exist.

(2) If programming pins exist, attempt to extract the firmware using the programming interface tools provided by the vendor.

(3) If the firmware can be extracted, use tools with binary file string search functionality to determine if plaintext CSP is present.

(4) If the firmware can be extracted, use tools with firmware disassembly functionality to dissect the TOE's firmware.

(5) Examine whether the firmware update file can be parsed to reveal file system directories and check for plaintext CSP.

(g) Pass criteria:

(1) The chip does not have programmable pins for firmware programming.

(2) It is not possible to extract the firmware through the programming pins.

(3) The extracted firmware does not contain plaintext CSP.

Any one of the above (1), (2), or (3) meeting the criteria.

(h) Value

Prevention of firmware extraction and analysis by potential attackers, mitigating potential security risks.

5.5.1.2 Integrity Mechanism Review

(a) Compliance:

Section 5.5.1.2 of Security Standard for ICT Product Supply Chain Part 1: Chip 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 vendor 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. 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.

5.5.1.3 Authenticity Mechanism Review

(a) Compliance:

Section 5.5.1.3 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify whether the firmware used by chips implements the protection mechanism of authenticity.

(d) Precondition:

None.

(e) The vendor 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.

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

(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.

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

(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.

5.5.1.4 Integrity Mechanism Protection

(a) Compliance:

Section 5.5.1.4 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

To verify if the firmware used in the chip has implemented an integrity mechanism.

(d) Precondition:

Pass the test of <5.5.1.2 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:

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

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

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

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

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

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

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

(8) 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.

5.5.1.5 Authenticity Mechanism Protection

(a) Compliance:

Section 5.5.1.5 of Security Standard for ICT Product Supply Chain Part 1: Chip Security

(b) Security level:

Level 2 (M)

(c) Test purpose:

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

(d) Precondition:

Pass the test of <5.5.1.3 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 1: Chip 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
5.2.1.1	The debugging interface shall have the authentication function and cannot be abused (such as accessing data other than the user's identity authority), to ensure the security of the data.			
	(Describe the procedure and provide supporting evidence.)			
5.3.1.1	The component shall have unique identification information and be correctly identified.			
	(Describe the procedure and provide supporting evidence.)			
5.3.1.2	The hardware instance shall have unique identification information and can be correctly identified.			
	(Describe the procedure and provide supporting evidence.)			
5.3.1.3	The component shall provide a mechanism to verify its authenticity to ensure that it is not an illegal clone.			
	(Describe the procedure and provide supporting evidence.)			
5.3.2.1	The authenticity and integrity of the component shall be verified during start-up.			
	(Describe the procedure and provide supporting evidence.)			
5.3.2.2	The component shall provide an identifiable known operating state so that the user can check whether the current operating state of the component is secure at any time.			
	(Describe the procedure and provide supporting evidence.)			
5.3.3.1	The component shall provide a secure firmware update capability in the user environment.			
	(Describe the procedure and provide supporting evidence.)			
5.3.4.1	The component shall provide a factory reset function to destroy user data stored in the product.			
	(Describe the procedure and provide supporting evidence.)			

Standard Requirements Items	Standard Requirements	Meet or not		
		Yes	Partial	No
5.3.5.1	The component shall provide an effective isolation mechanism between the application and hardware security functions to prevent attackers from maliciously manipulating the application and destroying other security functions of the product.			
	(Describe the procedure and provide supporting evidence.)			
5.4.1.1	Various cryptographic operations used by the component, such as encryption, decryption, digital signature, etc., should use cryptographic algorithms that comply with international standards, or cryptographic algorithms conventionally used in the security industry, such as an equivalent or higher encryption algorithm approved by NIST SP 800-140C.			
	(Describe the procedure and provide supporting evidence.)			
5.4.2.1	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.)			
5.4.2.2	CSPs stored in KeyStore shall protect their authenticity, integrity and confidentiality.			
	(Describe the procedure and provide supporting evidence.)			
5.4.3.1	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.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.2	The firmware shall have an integrity check mechanism, and the algorithms used shall comply with the requirements of international standards, or use the algorithms that are generally accepted as security industry practices.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.3	Firmware shall have an authenticity check mechanism, and the keys used for authenticity check shall be protected.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.4	Firmware shall have an integrity check mechanism to prevent users from updating with			

Standard Requirements Items	Standard Requirements	Meet or not		
		Yes	Partial	No
	tampered firmware.			
	(Describe the procedure and provide supporting evidence.)			
5.5.1.5	Firmware shall have an authenticity check mechanism to prevent users from updating with fake 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 Generation
- NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- BSI AIS31, A Proposal for Functionality Classes 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: Chip Core Testing Procedure

The purpose of attacking the chip core is to test the cryptographic modules that support attack mitigation techniques to resist side-channel attacks. Currently, there are no standardized testing methods that can guarantee complete resistance to side-channel attacks. However, effective testing methods can verify whether the chip has taken sufficient precautions in designing and implementing attack mitigation measures to withstand side-channel attacks.

Side-channel attacks exploit hidden biases in physical measurements on the chip or its surroundings (such as electromagnetic fields, power consumption, and computation timing) to attempt to extract CSP information such as keys. These biases may be subtle but are typically persistent, making them a prime target for attackers. In this specification, if experimental evidence indicates that leaked information exceeds the allowed threshold, the chip may fail one or more tests, indicating potential vulnerabilities in confidentiality protection.

The TOE in Section 5.1 involves collecting and analyzing measured values within the scope of the test restrictions, such as maximum waveforms collected and test duration, to determine the extent of CSP leakage. Thus, test restrictions and leakage thresholds serve as the basis for passing or failing this test.

According to the requirements of this chip core testing specification, the testing laboratory should collect sufficient measurement data from the chip, analyze the collected data using a set of statistical methods, and conduct security testing for CSP categories for individual security functions (such as cryptographic algorithms). CSP categories include encryption keys, biometric data, or PIN codes, among others. If certain security functions use multiple CSPs, security analysis shall be performed for each applicable CSP for each security function. The testing method shall detect all CSP categories included in the test chip until the first test failure occurs or until all CSP categories have passed. If the test chip limits the number of repeated operations, rendering the test unable to continue, the result should be considered a pass, and the test will proceed to the next CSP category. The testing procedure is illustrated in Figure Figure 2.

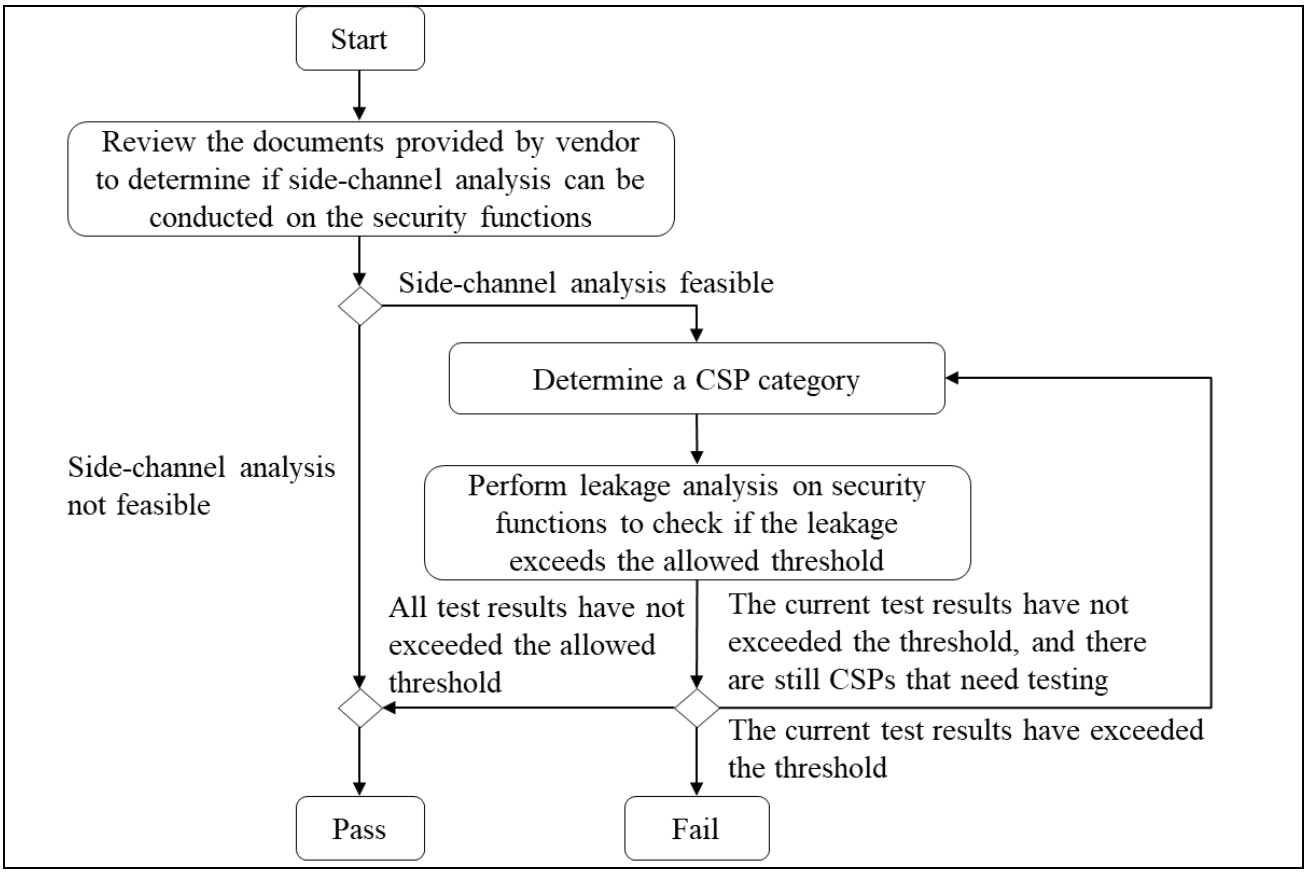

Figure 2 Chip Core Testing Procedure

The laboratory shall test the security of the chip against the three common types of side-channel attacks defined in this specification (i.e. TA, SPA/SEMA, and DPA/DEMA), following the testing sequence as depicted in Figure 3. The laboratory shall adhere to the testing sequence, for example: the TA test shall be conducted first, and only when the test chip passes the TA test shall the SPA/SEMA test be executed, and so forth. The TA, SPA/SEMA, and DPA/DEMA test methods specified in this specification do not require the laboratory to fully extract CSP through side-channel attacks as the basis for determining whether a test item passes or fails. If it can be demonstrated that CSP or cryptographic algorithm execution sequences leak beyond the threshold value, the test may fail.

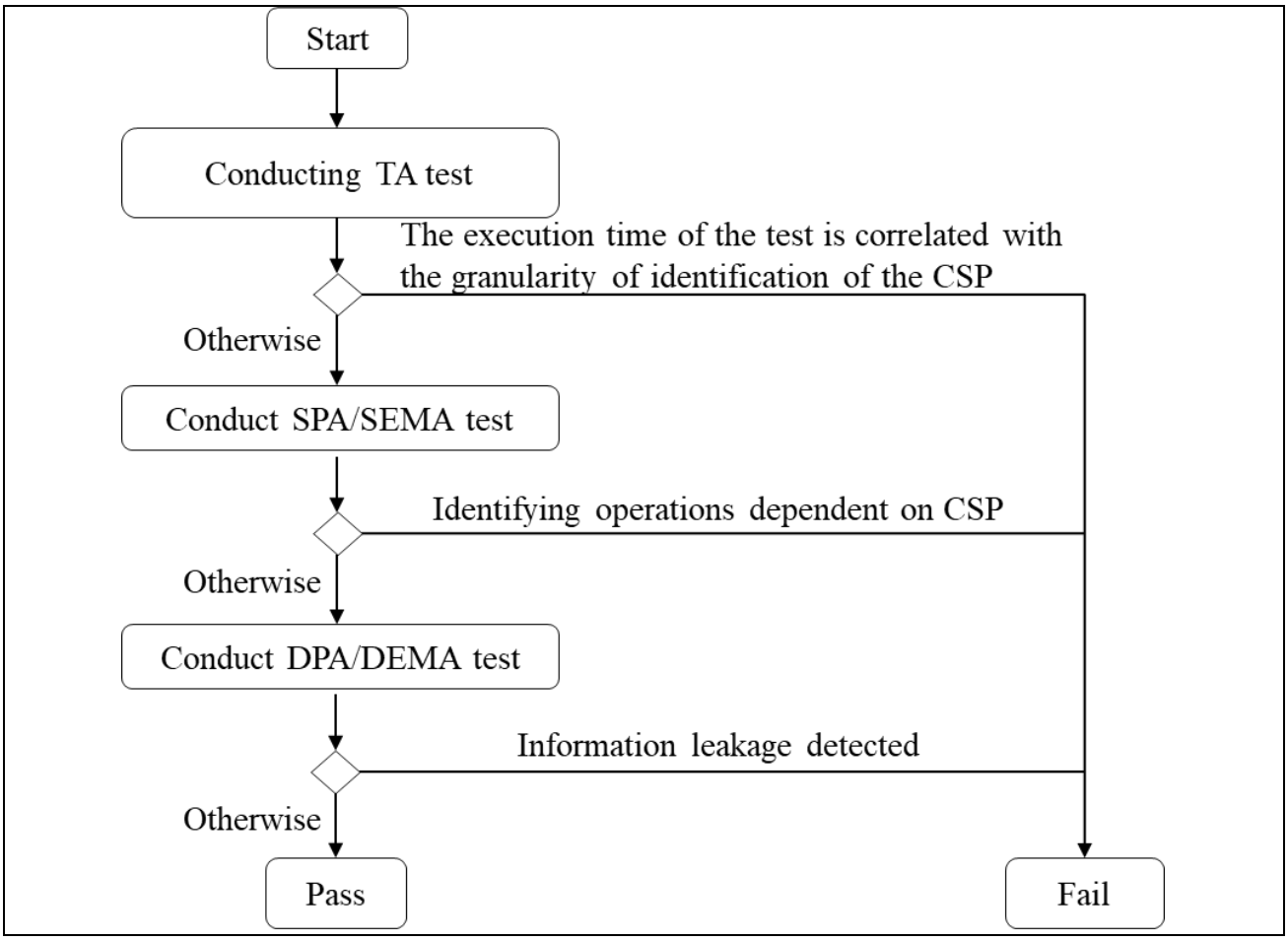

Figure 3 The testing sequence for TA, SPA/SEMA, and DPA/DEMA

Appendix D: 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 TA	—
5.1.1.2 SPA/SEMA	Pass the test of <5.1.1.1 TA>
5.1.1.3 DPA/DEMA	Pass the test of <5.1.1.2 SPA/SEMA>
5.1.1.4 DFA/EMFI	
5.1.2.1 Suspicious Circuit Testing	—
5.1.3.1 General Protection of Chip Cryptographic Module	—
5.1.3.2 Basic Protection of Chip Cryptographic Module	Pass the test of <5.1.3.1 General Protection of Chip Cryptographic Module>
5.1.3.3 Advanced Protection of Chip Cryptographic Module	Pass the test of <5.1.3.2 Basic Protection of Chip Cryptographic Module>
5.2.1.1 Secure Debugging	—
5.2.1.2 Secure Debugging Authentication	—
5.2.2.1 Security and Essential Function Protection	—
5.3.1.1 Chip Identity Verification	—
5.3.1.2 Chip Instance Identity Verification	—
5.3.1.3 Chip Genuineness Attestation	Pass the test of <5.3.1.1 Chip Identity Verification> and <5.3.1.2 Chip Instance Identity Verification >
5.3.2.1 Secure Boot	—
5.3.2.2 Chip State Attestation	Pass the tests of <5.3.1.3 Chip Genuineness Attestation> and <5.3.2.1 Secure Boot>
5.3.3.1 Chip Secure Update	—
5.3.4.1 Hardware Factory Reset	—
5.3.4.2 Hardware Decommission	—
5.3.4.3 Hardware Field Return	—
5.3.5.1 Hardware Isolation	—
5.3.5.2 Hardware Part Isolation	—
5.4.1.1 Cryptographic Operation	—
5.4.2.1 Key Generation	—
5.4.2.2 Key Storage	—
5.4.3.1 Random Number Generator	—
5.5.1.1 Firmware Extraction Protection	—
5.5.1.2 Integrity Mechanism Review	—
5.5.1.3 Authenticity Mechanism	—

Test Item Name	Test Precondition
Review	
5.5.1.4 Integrity Mechanism Protection	Pass the test of <5.5.1.2 Integrity Mechanism Review>
5.5.1.5 Authenticity Mechanism Protection	Pass the test of <5.5.1.3 Authenticity Mechanism Review>

Appendix E: The correspondence between this testing 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 Chip Security	5.1.1 Chip Core	5.1.1.1 TA	—	—
		5.1.1.2 SPA/SEMA	—	—
		5.1.1.3 DPA/DEMA	—	—
		5.1.1.4 DFA/EMFI	—	—
	5.1.2 Chip Design	5.1.2.1 Suspicious Circuit Testing	—	—
	5.1.3 Chip Security Module Protection	5.1.3.1 General Protection of Chip Cryptographic Module	—	—

Security Testing Aspects	Security Testing Items	Security Test Specifications	SESIP SFR	SESIP SAR
		5.1.3.2 Basic Protection of Chip Cryptographic Module	—	—
		5.1.3.3 Advanced Protection of Chip Cryptographic Module	—	—
5.2 Physical Interface Security	5.2.1 Debug Interface	5.2.1.1 Secure Debugging	3.6.7 Secure Debugging	SESIP1 SESIP3
		5.2.1.2 Secure Debugging Authentication	—	—
	5.2.2 Functional Protection	5.2.2.1 Security and Essential Function Protection	3.4.1 Limited Physical Attacker Resistance 3.4.2 Physical Attacker Resistance	SESIP3
5.3 Hardware Components Security	5.3.1 Chip Identity	5.3.1.1 Chip Identity Verification	3.1.1 Verification of Platform Identity	SESIP1 SESIP3
		5.3.1.2 Chip Instance Identity Verification	3.1.2 Verification of Platform Instance Identity	SESIP1 SESIP3
		5.3.1.3 Chip Genuineness Attestation	3.1.3 Attestation of Platform Genuineness	SESIP1 SESIP3
	5.3.2 Hardware Operating Status	5.3.2.1 Secure Boot	3.1.4 Secure Initialization of Platform	SESIP1 SESIP3
		5.3.2.2 Chip State Attestation	3.1.5 Attestation of Platform State	SESIP1 SESIP3
	5.3.3 Secure Update	5.3.3.1 Chip Secure Update	3.2.3 Secure Update of Platform	SESIP1 SESIP3
	5.3.4 Factory Reset	5.3.4.1 Hardware Factory Reset	3.2.1 Factory Reset of Platform	SESIP1 SESIP3
		5.3.4.2 Hardware Decommission	3.2.6 Decommission of Platform	SESIP1 SESIP3
		5.3.4.3 Hardware Field Return	3.2.7 Field Return of Platform	SESIP1 SESIP3

Security Testing Aspects	Security Testing Items	Security Test Specifications	SESIP SFR	SESIP SAR
	5.3.5 Isolation Security	5.3.5.1 Hardware Isolation	3.4.3 Software Attacker Resistance: Isolation of Platform	SESIP1 SESIP3
		5.3.5.2 Hardware Part Isolation	3.4.4 Software Attacker Resistance: Isolation of Platform Parts	SESIP3
5.4 Cryptographic Security	5.4.1 Cryptographic Algorithm Security	5.4.1.1 Cryptographic Operation	3.5.1 Cryptographic Operation	SESIP1 SESIP3
	5.4.2 Key Security	5.4.2.1 Key Generation	3.5.2 Cryptographic Key Generation	SESIP1 SESIP3
		5.4.2.2 Key Storage	3.5.3 Cryptographic KeyStore	SESIP1 SESIP3
	5.4.3 Random Number Generator Security	5.4.3.1 Random Number Generator	3.5.4 Cryptographic Random Number Generation	SESIP1 SESIP3
5.5 Firmware Security	5.5.1 Firmware Protection	5.5.1.1 Firmware Extraction Protection	—	—
		5.5.1.2 Integrity Mechanism Review	—	—
		5.5.1.3 Authenticity Mechanism Review	—	—
		5.5.1.4 Integrity Mechanism Protection	—	—
		5.5.1.5 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) Welch, B. L. "The generalization of "Student's" problem when several different population variances are involved". Biometrika. Vol. 34, No.1/2, pp. 28–35, Jan. 1947.

Version Revision History

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

TAIWAN ELECTRICAL AND ELECTRONIC MANUFACTURERS' ASSOCIATION
Tel：886-2-87926666 Fax：886-2-87926088
http://www.teema.org.tw