Security Standard for ICT Product Supply Chain

Part 1: Chip Security

V1.0

Taiwan Electrical and Electronic Manufacturers' Association

November 2022

Table of contents

ABSTRACT **2**

1. .SCOPE **4**

2. REFERENCE **6**

3. TERMS AND DEFINITIONS **7**

4. SECURITY LEVEL **12**

4.1 Overview of Security Levels 12

5. SECURITY REQUIREMENT **16**

5.1 Chip Security 16

5.2 Physical Interface Security 17

5.3 Hardware Components Security 17

5.4 Cryptographic Security 19

5.5 Firmware Security 20

REFERENCES **21**

VERSION REVISION HISTORY **22**

REVISION RECORD **23**

Abstract

With the development of semiconductor, electronic components are rapidly miniaturized and applied to various information and communication equipment, thereby enabling the rapid development of information and communication technology (ICT). ICT technology has become the basis for building a modern society, widely used in national defense and military systems, as well as key infrastructure related to the national economy and people's livelihood. For such applications, if their security is compromised, it may lead to serious loss of life and property issues, so ensuring information security is a prerequisite for the deployment of such ICT applications.

After decades of globalization, the ICT supply chain has gradually become globally dispersed, and this trend is particularly obvious in ICT products. Under the trend of globalization of ICT procurement, ensuring the security of the ICT industry supply chain has become a thorny issue. Typical ICT products are mainly composed of software and hardware components such as microcontrollers (MCUs) or microprocessors (MPUs), storage devices, communication modules/devices, operating systems, and applications. Vendors such as Original Equipment Manufacturers (OEMs) typically select the appropriate hardware and software components and build them into products that provide specific services.

In the ICT supply chain, various hardware and software, applications and information services use technology components from external suppliers to some extent. Since these hardware and software components are likely to come from different third-party suppliers, the related components in the supply chain may pose an information security threat to ICT products, thus making the security of the final product questionable. Because ICT product suppliers may not be able to effectively grasp the security of all external components, once hackers can attack a link in the supply chain, it will have a serious impact on the security of ICT products.

In ICT products, information security must be ensured through various security functions. Therefore, the security of chips responsible for various precision calculations has become a prerequisite for the normal operation of various key equipment. Since Taiwan’s semiconductor industry occupies an important position in the global ICT supply chain, how to ensure that the provided ICT products comply with certain security standards and regulations has become the focus of attention. Therefore, this standard was developed with the support of 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 standard aims to assist end users (such as local governments and other relevant units) to improve the information security protection capabilities of the ICT products that they purchase, and guide ICT and IoT related application vendors to introduce information security protection design concepts and technologies.

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

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

1. .Scope

ICT products can usually be divided into the most basic chip layer, as well as the system layer and software layer. Different vendors are responsible for developing the relevant components. According to the three layers of ICT products, their security requirements can be divided into "Part 1: Chip Security" and "Part 2: System Software Security" standards. This standard applies to various hardware components of ICT products that may pose potential security risks to the product.

Vendors covered by this standard and their roles in the supply chain are as follows:

- Chip vendors: focus on the research and development of chip layer chips, firmware and boot ROM, so this standard is applicable.
- OEMs: conceive and develop equipment according to this standard, such as selecting hardware that complies with this standard, selecting appropriate systems and software on the hardware, developing related applications or function libraries, etc., and assembling them into product that provides specific services. Since OEMs typically combine or integrate various hardware and software components, such as processors and software, into the solutions they sell, both the Part 1 and Part 2 security standards apply.

The scope of this standard is the chip layer of ICT products, and its corresponding layer in the supply chain is shown in the red box in Figure 1 below.

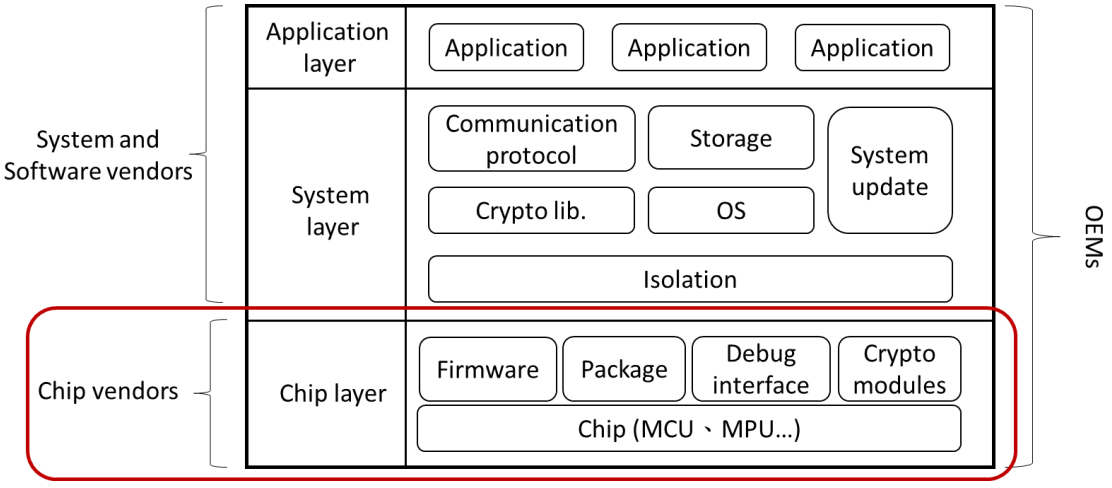

Figure 1 Scope of Part 1: Chip Security

Since the chip is the core of various operations, once a security problem occurs, it will directly affect the security of the upper-layer system software. Therefore, the Part 1: Chip Security standard, specifies the security requirements at the chip layer, including the microcontroller/microprocessor that performs the core operations. Chip designs should avoid suspicious circuits in the pre-silicon stage, prevent non-intrusive side-channel and fault injection attacks in the post-silicon stage. This standard also specifies security requirements related to chip packaging, firmware, and debug interfaces. Because the chip layer is the bottom layer of ICT products, it provides a basic security environment for the operation of upper-layer system software, so the Part 1: Chip Security standard can be independently certified.

2. Reference

The following documents are essential references for this standard. 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.

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

3. Terms and Definitions

The following terms and definitions apply to this standard.

3.1 Testing

Refers to testing in the testing laboratory in accordance with the standard procedures of testing specifications, issuing a formal testing report, and notifying customers of the testing results.

3.2 Certification

Recognition by an impartial third party that a product, component, process or service conforms to a standard.

3.3 Testing Laboratory

Refers to the testing laboratory (hereinafter referred to as the laboratory) certified by ISO/IEC 17025, which uses the test method defined in this standard to verify whether the object under test meets the defined passing criteria.

3.4 CSP (Critical Security Parameter)

Refers to security-related information that, if leaked or modified, may compromise the security of a cryptographic module, such as: secret keys, private keys, passwords, PINs (personal identification numbers), certificates, modes of operation, or other sensitive information.

3.5 Sensitive Data

Refers to sensitive documents (such as business information, etc.) generated when the user runs the object under test.

3.6 Personal Data

Refers to the natural person's name, date of birth, identity number, passport number, features, fingerprints, marriage, family, education, occupation, medical records, medical treatment, genetics, sex life, health examination, criminal record, contact information, financial status, social activities and etc. that can directly or indirectly identify an individual.

3.7 Key

In cryptography, keys such as: secret key, private key, and public key refer to the unique parameters used to perform encryption, decryption, integrity verification, digital signature and other cryptographic applications.

3.8 IC (Integrated Circuit/Chip)

A chip or integrated circuit (IC) is a very small electronic circuit designed to perform processing and/or storage functions.

3.9 Hardware Instance

Refers to a physical or virtual device or component in a product that has a similar life cycle, such as a chip that has a protected memory area in its flash memory and contains a 128-bit unique identifier ID, can be considered an instance. Secure World and Normal World in TrustZone are two different instances that can be switched between them as needed for the current session.

3.10 Physical Maintenance

When the user open the chip cover to remove the chip package, or debugs through physical interfaces such as JTAG, UART, and USB, it is regarded as physical maintenance of the chip.

3.11 TA (Timing Analysis)

Every logic operation in a chip takes time to execute or respond, depending on the input value. By accurately measuring the time taken for each operation, attackers can use this to break the cryptosystem and obtain the secret keys, private keys, passwords, PINs, etc. used by the encryption and decryption algorithms.

3.12 SPA (Simple Power Analysis)

When each instruction running on the cryptographic module is executed sequentially, by monitoring the power consumption changes during the execution of the cryptographic module, the instruction execution or logic circuit activity patterns can be directly analyzed. If the instruction sequence is related to the key, the waveform changes caused by these instructions may lead to security problems such as key leakage. SPA only needs a small amount of power consumption traces to attack.

3.13 SEMA (Simple Electromagnetic Analysis)

SEMA uses the same method as SPA to estimate the key by observing changes in the electromagnetic radiation traces (i.e., EM traces). Encryption algorithms that perform different operations depending on whether the key bits are 0 or 1 are vulnerable to SEMA attacks. An attacker can deduce the key by observing the entire encryption process.

3.14 DPA (Differential Power Analysis)

DPA requires a large number of voltages change traces to compare power consumption and data dependency. DPA does not require much detailed knowledge of the object under test, even if the recorded traces contain noise, once enough power consumption traces are collected, an attacker can use multiple power traces for both sets of data, and then the difference between the averages is calculated and used to remove noise to find the key.

3.15 Differential Electromagnetic Analysis (DEMA)

DEMA is an advanced attack that uses multiple traces of electromagnetic radiation to improve the fidelity of the captured signal. Suitable for situations where simple electromagnetic analysis attacks are not possible or provided sufficient information is not enough. DEMA attacks are more complex than simple electromagnetic analysis attacks, but can effectively analyze side-channel weaknesses in cryptosystems without much knowledge of the object under test.

3.16 Dependency

Dependency is a measure of the degree to which two variables influence each other. For example, when the input value bit "0" is encountered, the encryption time will be shortened, and conversely, when the input value bit "1" is encountered, the encryption time will be slightly extended. By analyzing the different input values of the encryption module, it can be determined whether the chip has protection against timing attacks on the encryption module at the beginning of the design. This prevents an attacker from inferring from timing side channel information that the cryptographic module is currently computing a bit "0" or "1".

3.17 Semiconductor Package

A semiconductor package (hereinafter referred to as a package) is a carrier/enclosure for containing and encapsulating one or more semiconductor components or integrated circuits. The material of the enclosure can be metal, plastic, glass or ceramic. The package provides the following capabilities for die: (1) Provide certain impact/scratch protection; (2) Provide

pins or contacts for connection with external circuits; (3) Take away the heat generated by the die.

3.18 Pre-silicon

Chip designers describe the chip circuit through a hardware description language (HDL, such as Verilog or VHDL), and use a hardware description language simulator to confirm the correctness of circuit functions. After that, the designers transform HDL code into a netlist describing the hardware (e.g., the logic gates and the wires connecting them) through logic synthesis tool. After placement and routing, the GDSII file is generated for fabrication.

3.19 Post-silicon

In the post-silicon stage, chip designers submit chip layout designs (e.g., GDSII) to chip manufacturers or foundries to manufacture chips. The foundry will actually transfer the designed circuit diagram to the semiconductor wafer. Through a series of processes, integrated circuits (ICs) are formed on the surface of the wafer, which are then diced into dies, and packaged to form the final chip.

3.20 Coating

Refers to the passivation technology of semiconductor packaging, using materials such as organic polymers to form a conformal coating or seal coating to prevent damage to the chip from environmental or other physical damage.

3.21 DFA (Differential Fault Analysis)

During the encryption and decryption process, the attacker selects the appropriate time and position to perform error injection (such as changing the voltage of the chip), interferes with the encryption and decryption operation, and causes the temporary register in the chip to generate errors during the encryption and decryption process. By comparing the difference between the correct ciphertext output and the incorrect ciphertext output, the attacker may obtain sensitive information inside the chip, such as keys, etc.

3.22 EMFI (Electromagnetic Fault Injection)

EMFI is a localized, high-precision attack method. The attacker places the electromagnetic probe near the encrypted circuit, and generates a pulse signal in time to interfere with the key signal circuit inside the chip, causing the circuit to work abnormally, for example, causing the register to occur bit flips to produce desired effects, such as skipping

authentication steps, bypassing secure boot, escalating privileges or changing the output of password operations, etc.

4. Security level

Security level is a measure of the ability of a component to withstand information security threats. It is achieved by combining the most appropriate security measures to ensure that the component meets security requirements.

4.1 Overview of Security Levels

Each component has unique features and security requirements. In order to connect with international information security standards (such as SESIP) and lower the threshold of product security certification, this standard defines three security levels for the chip layer. Components on the chip layer must first meet the requirements of the lower security level before they can enter the higher level of testing.

Each security level is described as follows:

- Level 1: The Level 1 security standard brings together the most security baselines for chip level and protects against some of the most common security breaches. The vendor fills in the questionnaire according to the security function of the components, so that an accredited testing laboratory can evaluate whether the components meet the requirements of the baseline security standard through the questionnaire and attachments filled in by the vendor.
- Level 2: The Level 2 security standard is used to prove that components are protected from remote cyber-attacks, that an attacker cannot perform a large-scale repeated attack on a component until it is detected. As a result, the scope of damage to components from physical attack is limited, allowing vendors to provide security guarantees that apply to many mass-market solutions. Level 2 security involves an independent evaluation by accredited testing laboratories. Laboratory uses methods such as vulnerability analysis and penetration testing to confirm that the components under test meet the standard requirements.
- Level 3: The Level 3 security standard is designed for chip vendors who wish to independently evaluate the high-value components. This level of security allows OEMs to trust that the component has native protection from hackers against local attacks. This level is independently evaluated by an accredited testing laboratory to

ensure that the component is protected against complex hardware attacks, such as hackers having physical access to the component.

Table 1 is the summary of chip security requirements, in which the security requirements in the third column of the security level 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.

Table 1 Summary of Chip Security Requirements Levels

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

Security Aspects	Security Requirements Items	Security Levels		
		Level 1	Level 2	Level 3
	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)

Source: Prepared by this project

This table summarizes key security considerations, outlined in the first column (e.g., chip security, physical interface security). The second column specifies corresponding security requirements for each aspect. The third column defines assigned security levels. Evaluation results for each requirement directly contribute to determining the overall security level. This summary table shall adhere to the detailed technical specifications provided in Sections 5.1 to 5.5 of this standard.

4.1.1 **Security Aspects**

(a) 5.1 Chip Security: The component should have the ability to detect and resist intrusion. Additionally, secure chip design and robust packaging materials should be considered as the subject of chip security requirements.

(b) 5.2 Physical Interface Security: The debugging interface provided by the component should have sufficient security protection.

(c) 5.3 Hardware Component Security: The identity of the hardware components shall be properly identified (authenticated) and can be securely updated and factory reset.

(d) 5.4 Cryptographic Security: The cryptographic algorithms, keys and random number generators used in the component should have sufficient security strength.

(e) 5.5 Firmware Security: Firmware used in component shall ensure its confidentiality, authenticity and integrity.

4.1.2 **Security Requirements Items**

Each security requirement item includes one or more security requirements according to the security requirements specified in the security aspect.

4.1.3 **Security Levels**

The security level is divided into 3 levels: Level 1, Level 2 and Level 3, according to (1) the security requirements that the chip layer shall have, and (2) the complexity of the technology implementation.

The number of the security level represents the level of the security level. To satisfy higher level security requirements, all mandatory security requirements for lower security levels are first met. If the vendor implements one or more optional security requirements at levels 2 and 3, the security levels are 2+ and 3+, respectively. If the vendor meets the security requirements of level 3+ on the basis of level 2, it shall also be considered as level 2.

5. Security Requirement

This section details the common methods that the component shall take to meet the security functions. The corresponding security level of the component shall meet the security requirements of this section.

5.1 Chip Security

5.1.1 Chip Core

5.1.1.1 During the cryptographic operation, the component shall not cause differences in processing time due to different CSP values, so as to prevent the discovery of the dependency between execution time and CSP through timing analysis. (Level 3)

5.1.1.2 During the cryptographic operation, the component shall prevent attackers from finding out the operation sequence of cryptographic operations through simple power analysis or simple electromagnetic analysis. (Level 3)

5.1.1.3 The traces of the component during the encryption operation shall prevent attackers from discovering the CSP used by the component through differential power analysis or differential electromagnetic analysis. (Level 3)

5.1.1.4 During the cryptographic operation, the component shall prevent attackers from generating stable abnormal output through differential fault analysis or electromagnetic fault injection, or causing potential CSP leakage problems. (Level 3)

5.1.2 Chip Design

5.1.2.1 The component shall not be suspected of being a hardware Trojan in the circuit design. (Level 3)

5.1.3 Chip Security Module Protection

5.1.3.1 The cryptographic module components shall consist of production-grade components that include standard passivation technology, and the plaintext CSP will not be leaked during physical maintenance. (Level 3)

5.1.3.2 The cryptographic module components shall be covered with opaque, hard tamper-evident coating or packaging material, and shall retain evidence of tampering or removal when tampered with. (Level 3)

5.1.3.3 Cryptographic module components shall have a tampered response mechanism. (Level 3)

5.2 Physical Interface Security

5.2.1 Debug Interface

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. (Level 2)

5.2.1.2 The identity authentication function of the debugging interface shall have the corresponding identity/role permissions design, and cannot use illegal means to escalate the privilege. (Level 2)

5.2.2 Functional Protection

5.2.2.1 The component shall have the ability to detect or prevent physical attacks, and avoid necessary functional abnormalities in non-security functions (such as: network time protocol cannot work, power indicator lights are abnormal, etc.). (Level 3)

5.3 Hardware Components Security

5.3.1Chip Identity

5.3.1.1 The component shall have unique identification information and be correctly identified. (Level 2)

5.3.1.2 The hardware instance shall have unique identification information and can be correctly identified. (Level 2)

5.3.1.3 The component shall provide a mechanism to verify its authenticity to ensure that it is not an illegal clone. (Level 2)

5.3.2 Hardware Operating Status

5.3.2.1 The authenticity and integrity of the component shall be verified during start-up. (Level 2)

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. (Level 2)

5.3.3 Secure Update

5.3.3.1 The component shall provide a secure firmware update capability in the user environment. (Level 2)

5.3.4 Factory Reset

5.3.4.1 The component shall provide a factory reset function to destroy user data stored in the product. (Level 2)

5.3.4.2 The component shall provide decommissioning capabilities to destroy applications, sensitive data, and personal data in the product, rendering the product unusable. (Level 2)

5.3.4.3 In the event of a failure requiring repair, the component shall provide the ability to return the product to the vendor, destroy sensitive data and personal data in the product, and make it impossible for the vendor to recover the destroyed data. (Level 2)

5.3.5 Isolation Security

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. (Level 2)

5.3.5.2 The component shall provide effective isolation between hardware components, preventing weak components from becoming an attack agent that cause damage to other components. (Level 3)

5.4 Cryptographic Security

5.4.1 Cryptographic Algorithm Security

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. (Level 2)

5.4.2 Key Security

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. (Level 2)

5.4.2.2 CSPs stored in KeyStore shall protect their authenticity, integrity and confidentiality. (Level 2)

5.4.3 Random Number Generator Security

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. (Level 2)

5.5 Firmware Security

5.5.1 Firmware Protection

5.5.1.1 Firmware shall not be extracted to analyze CSPs in plaintext. (Level 3)

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. (Level 2)

5.5.1.3 Firmware shall have an authenticity check mechanism, and the keys used for authenticity check shall be protected. (Level 2)

5.5.1.4 Firmware shall have an integrity check mechanism to prevent users from updating with tampered firmware. (Level 2)

5.5.1.5 Firmware shall have an authenticity check mechanism to prevent users from updating with fake firmware. (Level 2)

References

(1) Arm Limited, Platform Security Model v1.1 (JSADEN014), Jan. 2021.
(2) Arm Limited, PSA Certified Level 1 Questionnaire version 2.1 (JSADEN001), Oct. 2020.
(3) GlobalPlatform Technology, SESIP Profile for Secure MCUs and MPUs v0.0.0.7 (GPT_SPE_150), Jun. 2021.
(4) Security Evaluation Standard for IoT Platforms (SESIP) v1.0 (GP_FST_070)
(5) FIPS 140-3 Security Requirements for Cryptographic Modules
(6) ISO/IEC 15408:2008 Information technology — Security techniques — Evaluation criteria for IT security
(7) ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules

Version Revision History

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

Revision Record

Amended Clause	Current Clause