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

Taiwan Electrical and Electronic Manufacturers' Association

November 2022

Table of contents

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. In the ICT supply chain, various hardware and software, applications and information services use technology components from external suppliers to some extent. 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, providing the necessary security services for ICT products to ensure the security of operating systems and software running on the chip layer. The system and software layers are also often the primary targets for hackers, who exploit remote and application interfaces to infiltrate and attack ICT products. 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 standard has been established.

The purpose of this standard is to assist ICT supply chain stakeholders in Taiwan to enhance the security protection capabilities of their ICT products, and to lead ICT and IoT application vendors to adopt 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

The level corresponding to this standard within the supply chain is shown in the red box in Figure 1 below. The roles of vendors applicable to this series of standards and their positions within the supply chain are as follows:

- System and software vendors: Responsible for developing operating systems (such as real-time operating systems, RTOS), communication modules, cryptographic libraries (crypto library), and application services required for products at the system and software layers, such as Apps. Their security is built upon a secure chip layer.
- OEMs: Conceive and develop product 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.

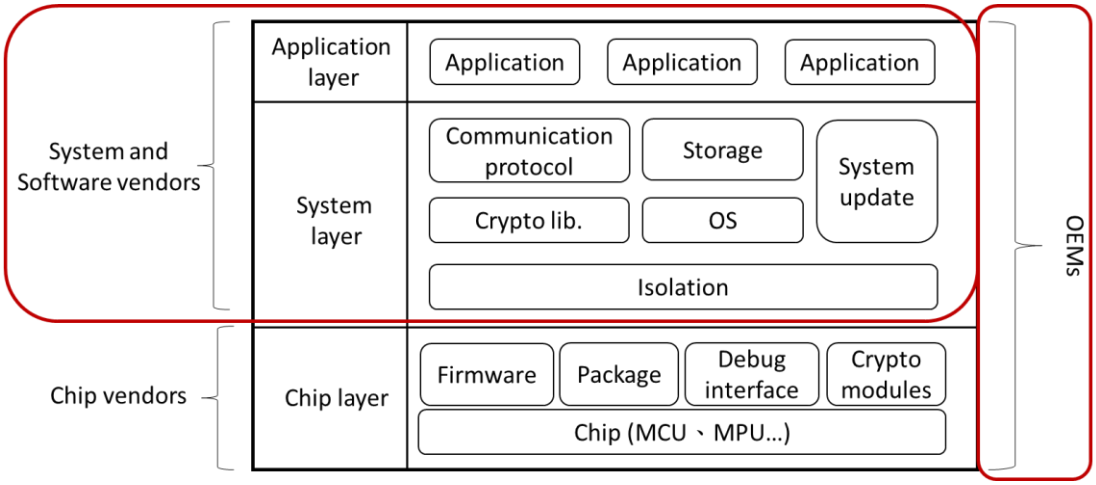

Figure 1 Scope of Part 2: System Software Security

This standard specifies the security requirements for the system layer and the software layer, including password security, storage security, communication security, and so on.

Since the operation of the system layer relies on a secure chip layer, the cybersecurity standard certification for the system layer shall be based on the chip layer that has been certified under the Part 1: Chip Security standard. For system and software layer vendors focusing on the development of their components (such as OS and Crypto library), if the components aim to be certified under this cybersecurity standard, they shall be based on both the certified chip layer.

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.

- Security Standard for ICT Product Supply Chain Part 1: Chip Security Standard V1.0

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 Part

Refers to a relatively independent component of an application, such as a module, process, applet, etc.

3.2 Only-increasing Counter

Refers to a component that stores the number of occurrences of specific events or processes and only increases over time.

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 security standards (such as SESIP) and lower the threshold of product security certification, this standard defines three security levels for the system software layer. Components on the system software 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 important security baselines for system software 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 the 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 demonstrate that components developed by system software vendors can meet the requirements of most products, allowing vendors to provide security assurances applicable to many mass-market solutions. Level 2 security involves an independent evaluation by a testing laboratory. Laboratory uses methods such as vulnerability scanning, vulnerability analysis, and penetration testing to confirm whether the components under test meet the standard requirements.
- Level 3: The Level 3 security standard caters to system software vendors developing high-value components that demand the highest level of trust. This rigorous standard instills confidence in OEMs by exceeding baseline security and demonstrating resilience against sophisticated hacking attempts. Through independent evaluation by accredited testing laboratories, Level 3 certification verifies the component's

advanced security features and its ability to withstand complex attacks. This includes neutralizing attempts to exploit component vulnerabilities as springboards for broader system compromise.

Since the operation of the system software layer relies on a secure chip layer, the system software layer shall use the same security level or a higher level of chip layer. In other words, the security level of the chip layer shall be at least equal to or greater than the security level the system software layer aims to achieve. For example, if the system software layer aims to achieve Level 2 security certification, the underlying chip layer shall have achieved Level 2 or Level 3 security certification. If the chip layer associated with the system software layer has only achieved Level 2 security certification, the system software layer shall only be able to obtain Level 2 security certification and cannot achieve Level 3 security certification.

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 System Software Security Requirements Levels

<table>
<tr><th rowspan="2">Security Aspects</th><th rowspan="2">Security Requirements 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 System Software Component Security</td><td>5.1.1 System Software Identity</td><td rowspan="9">The vendor conducts self-assessment and provides supporting evidence, which is then evaluated by the laboratory</td><td>5.1.1.1 (M)</td><td></td></tr>
<tr><td>5.1.2 System Software Operating Status</td><td>5.1.2.1 (M)</td><td></td></tr>
<tr><td>5.1.3 Secure Update</td><td>5.1.3.1 (M)</td><td></td></tr>
<tr><td rowspan="3">5.2 Cryptography Security</td><td>5.2.1 Cryptographic Algorithm Security</td><td>5.2.1.1 (M)</td><td>—</td></tr>
<tr><td>5.2.2 Key Security</td><td>5.2.2.1 (M)
5.2.2.2 (M)</td><td></td></tr>
<tr><td>5.2.3 Random Number Generator Security</td><td>5.2.3.1 (M)</td><td></td></tr>
<tr><td rowspan="2">5.3 Software Security</td><td>5.3.1 Isolation Security</td><td></td><td>5.3.1.1 (M)</td></tr>
<tr><td>5.3.2 Security Status</td><td>5.3.2.1 (M)</td><td>5.3.2.2 (O)</td></tr>
</table>

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

Source: Prepared by this project

Table 1 summarizes the overall security levels, with the first column outlining key security aspects such as system software component security and cryptography security. The second column outlines corresponding security requirements for each aspect. The third column specifies the respective security levels. Evaluation results for each security requirement will be used to determine the overall security level. This security level summary table shall comply with the technical specifications in Sections 5.1 to 5.6 of this standard.

4.1.1 Security Aspects

(a) 5.1 System Software Component Security: The component's unique identification information shall be able to be correctly identified, and shall be able to update securely.

(b) 5.2 Cryptography Security: The cryptography algorithm, keys, and random number generator used by the component shall possess sufficient security strength.

(c) 5.3 Software Security: The application programs shall have security protection mechanisms.

(d) 5.4 Storage Security: The component shall guarantee the authenticity, integrity, and confidentiality of all stored data, with provisions for secure destruction when required.
(e) 5.5 Communication Security: The component shall use secure communication protocols and protection measures that comply with cybersecurity standards.
(f) 5.6 Firmware Security: The component's firmware shall uphold confidentiality, authenticity, and integrity while explicitly disallowing access to exploitable vulnerabilities.

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 system software layer shall have, and (2) the complexity of the technology implementation.

The pertinent list constitutes a subset of security requirements, delineating both mandatory and optional compliance. Numerical categorization of security levels serves to indicate their relative prominence. Attaining higher-level security prerequisites necessitates prior fulfillment of all mandatory security standards for lower-tier security levels. In cases where the provider incorporates one or more optional security provisions from levels 2 and 3, the resulting safety designation is denoted as 2+ and 3+, respectively. Should the provider meet level 3+ security requirements grounded in level 2, adherence to level 2 requirements is also affirmed.

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 System Software Component Security

5.1.1 System Software Identity

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

5.1.2 System Software Operating Status

5.1.2.1 The component shall provide recognizable known operating states. (Level 2)

5.1.3 Secure Update

5.1.3.1 The component shall offer a secure component update functionality in the user environment. (Level 2)

5.2 Cryptography Security

5.2.1 Cryptographic Algorithm Security

5.2.1.1 The component shall use cryptography algorithms that comply with international standard requirements or widely accepted security industry practices, such as security algorithms approved by NIST SP 800-140C or higher. (Level 2)

5.2.2 Key Security

5.2.2.1 The key generation algorithm used by the component shall use a cryptographic algorithm that meets the requirements of international standards, such as NIST SP 800-133 Rev. 2. (Level 2)

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

5.2.3 Random Number Generator Security

5.2.3.1 The random number generation algorithm used in the component shall comply with the requirements of international standards, or meet the recognized industry practices in the field of information security, such as NIST SP 800-90A, NIST SP 800-90B or a cryptographic algorithm of equal or higher level approved by AIS31, and also the generated random numbers shall pass the NIST SP 800-22 randomness test. (Level 2)

5.3 Software Security

5.3.1 Isolation Security

5.3.1.1 The component shall provide an effective isolation functionality for application components, ensuring that even if an attacker can execute malicious actions on a specific application part, they cannot compromise the confidentiality and integrity of other parts of the application. (Level 3)

5.3.2 Security Status

5.3.2.1 The component shall have the capability to verify the authenticity of application. (Level 2)

5.3.2.2 The component shall provide recognizable known operational states for applications, such as indicators, warning messages, icons, etc. (Level 3)

5.3.3 Install/Update/Uninstall Security

5.3.3.1 The component shall deliver secure application installation functionality within user environments and also in potentially insecure manufacturing sites. (Level 2)

5.3.3.2 The component shall offer secure application update functionality in user environments. (Level 2)

5.3.3.3 The component shall provide secure uninstallation functionality, destroying application data to prevent potential attackers from gaining sensitive and personal information through physical contact. (Level 2)

5.4 Storage Security

5.4.1 Data Protection

5.4.1.1 All data stored by the application shall be protected for authenticity and integrity. (Level 2)

5.4.1.2 The component shall use encryption to protect the confidentiality and integrity of stored data. (Level 2)

5.4.1.3 Data stored outside the direct control of the component and not included in the exception list shall be protected. (Level 2)

5.4.2 Secure Data Destruction

5.4.2.1 Data deleted from memory shall be securely erased and irrecoverable. (Level 3)

5.4.3 Log Preservation

5.4.3.1 The component shall provide a secure method for log generation and storage. (Level 2)

5.4.4 Only-Increasing Counter Preservation

5.4.4.1 The component shall provide a reliable only-increasing counter and prevent tampering or deletion of counter values. (Level 3)

5.5 Communication Security

5.5.1 Protocol Security

5.5.1.1 The secure channel protocol used by the component shall comply with security standards, such as TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384 of TLS 1.2, etc. (Level 2)

5.5.1.2 The communication protocol implemented by the component shall match the declaration. (Level 2)

5.5.1.3 The component shall only provide the necessary network services required for operation. (Level 2)

5.6 Firmware Security

5.6.1 Firmware Content Security

5.6.1.1 The firmware shall not contain plaintext CSP, undisclosed IP, URL, and email. (Level 2)

5.6.1.2 The firmware shall not have vulnerabilities assessed in the Common Vulnerability Scoring System (CVSS) v3 with a severity rating of high for cybersecurity risk vulnerabilities. (Level 2)

5.6.1.3 After executing reverse engineering, the firmware shall not have source code, object code, or just-in-time compiled code. (Level 3)

5.6.2 Firmware Protection

5.6.2.1 The firmware shall have an integrity verification mechanism, and the algorithms used shall adhere to international standard requirements or the best practices of recognized security industry conventions. (Level 2)

5.6.2.2 The firmware shall have an authenticity verification mechanism, and the keys used for authenticity shall be protected. (Level 2)

5.6.2.3 The firmware shall have an integrity protection mechanism to prevent users from updating tampered firmware. (Level 2)

5.6.2.4 The firmware shall have an authenticity protection mechanism to prevent users from updating forged 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.

Version Revision History

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

Revision Record

Amended Clause	Current Clause