# Developing Chip Security Standards for ICT Product Supply Chain in Taiwan

**Song-Kong Chong[1], Chuan-Kai Kao[1], Wei-Chun Tai[2]***

[1]Cybersecurity Technology Institute, Institute for Information Industry, Taiwan

[2]*Information Technology Services Division, Institute for Information Industry, Taiwan

*Corresponding Author: derricktai@gmail.com

DOI: https://doi.org/10.30211/JIC.202402.004

## ABSTRACT

Digital trust is essential for the reliable operation of society. Advances in semiconductor technology and the rapid miniaturization of electronic components have posed a major challenge to the security of digital technology. These potentially insecure chips could weaken digital trust, which could in turn affect the reliable operation of society. Since chip security is not only related to personal privacy, but also to national security and the stability of corporate operations, establishing trusted chip security standards is the cornerstone of ensuring digital trust, providing a guarantee for people to use digital technology with confidence. Recognizing the significant position of Taiwan's semiconductor industry in the global ICT supply chain, and with the support of the Taiwan Ministry of Digital Affairs, we have developed the Chip Security Standard for ICT Product Supply Chain. The standard encompasses 31 chip security requirements and has been released in Taiwan as an industry benchmark. This paper presents the background of the security standard development, the expert review process, the overview of the chip security standards and its impact on the industry. By establishing these standards, the work addresses vulnerabilities in semiconductor technology that arise from rapid miniaturization and advances, which could potentially compromise both personal privacy and national security. This standard serves as a benchmark for the industry in Taiwan, guiding the production and use of more secure digital technologies and reinforcing the overall reliability and security of the digital ecosystem.

Keywords: Chip, Security Standard, ICT Product Supply Chain.

## 1. Introduction

In an increasingly interconnected world, businesses, governments, and individuals who engage in cross-border transactions and collaborations, rely heavily on digital technologies and platforms to communicate, exchange data, and conduct commerce. Thus, digital trust plays a pivotal role in facilitating and sustaining globalization [1-2].

The digital trust is usually built upon hard security and soft security [3]. Hard security measures can help to prevent unauthorized access to a system or network, while soft security are non-technical measures that protect systems and data through user education, security policies, security evaluations, incident response plans and etc. The adoption of these security measures is additionally influenced by various psychological factors, including self-efficacy [4] and perceived risk [5]. Factors such as technology complexity, firm size, and competitive pressure, which are related to the internal organization and the external environment, also impact the adoption of security measures themselves [6].

In fact, hard security and soft security are complementary approaches to security because they address different aspects of the security challenge. If a product or service fails to operate in a predictable, reliable and secure manner, management will be difficult to achieve in such digital world. On the other hand, in order for business operations to proceed smoothly, management needs to trust the reliability of the product or service through certain methods [7]. Therefore, various security standards that can increase confidence and interoperability in the digital commerce ecosystem build the foundation of digital trust.

To protect against evolving security threats, maintain the integrity of products and services, and safeguard sensitive data and intellectual property, the security of the ICT (Information and Communication Technology) product supply chain is more important than ever. As ICT products are becoming increasingly complex with multiple hardware, firmware, and software components integrated into a single device, this complexity introduces a higher risk of vulnerabilities and potential security breaches. Ensuring the security of the supply chain helps mitigate these risks.

ICT products can usually be divided into the most basic chip (hardware) layer, and the system software layer that build on it. Over the years, significant advancements have been made in system software security. Operating systems, applications, and network infrastructure have become more robust in terms of vulnerability detection and patching. This progress has made it more challenging for attackers to exploit system software vulnerabilities directly. As a result, attackers are shifting their focus to the hardware layer, where attention and security measures may be relatively limited. Once a security issue arises, these hardware vulnerabilities can be challenging to remediate, thereby eroding the foundation of digital trust.

In the past 10 years, several significant developments and notable news events related to hardware attacks have taken place. Here are some prominent examples:

- Rowhammer (2015): Rowhammer [8-9] is a hardware vulnerability that targets dynamic random-access memory (DRAM) chips. By repeatedly accessing certain memory locations, an attacker can cause bit flips in neighboring memory cells, leading to unauthorized access or control of the affected system. Rowhammer attacks highlighted the potential security risks associated with hardware-level vulnerabilities in memory systems.
- Spectre and Meltdown (2018): Spectre [10] and Meltdown [11] were two major hardware vulnerabilities discovered in modern computer processors. They allowed attackers to exploit speculative execution to access sensitive data, including passwords and encryption keys [12].

These vulnerabilities affected a wide range of processors from various manufacturers, including Intel, AMD, and ARM.

- Thunderclap (2019): Thunderclap [13] refers to a set of vulnerabilities affecting Thunderbolt interfaces, which can be exploited to gain unauthorized access to a system's memory. These vulnerabilities demonstrated the potential for direct memory access (DMA) attacks through hardware interfaces, highlighting the need for robust hardware-based security measures.
- Vulnerabilities in Wi-Fi and Bluetooth Chips (2020): Researchers [14] have discovered multiple security vulnerabilities in existing Wi-Fi and Bluetooth chips. These vulnerabilities allowed attackers to execute remote code execution attacks, enabling them to take control of the affected devices, which can lead hackers to use them to steal device passwords and various data.

These examples illustrate the evolving landscape of hardware attacks and the continuous discovery of vulnerabilities in various hardware components. These developments have spurred increased attention and efforts to improve hardware security, and the resilience of systems against hardware-based threats. Providing a secure hardware foundation for digital systems and services is critical to the effective and efficient delivery of ICT products.

Due to the increasing severity of security threats targeting chips, Taiwan, which holds a significant position in the global ICT supply chain, has decided to enhance the security of the ICT product supply chain (especially chip security) through standardization work. This is to demonstrate its commitment to supply chain security, and to ensure and promote the implementation of the most fundamental digital trust.

Starting in 2021, the Taiwan government has initiated its 6th National Cyber Security Action Plan, emphasizes the security of ICT chip products, focusing on the following key aspects: (1) Research and development of chip security analysis tools to address underlying security risks associated with chips; (2) Establishment of an internationally recognized chip security testing laboratory to bridge the gap in domestic chip testing technology and the testing environment ecosystem, thereby reducing security compliance barriers for domestically exported products. These initiatives have been integrated into national policies, with allocated resources to support the overall advancement of chip security. The Institute for Information Industry (III), a think tank under the supervision of the Taiwan Ministry of Digital Affairs, is in charge of executing the project.

After two years of diligent effort, III has formulated relevant supply chain security standards, and officially released them as the industry standard through the Taiwan Electrical and Electronic Manufacturers' Association (TEEMA), the most important industry association in Taiwan with more than 3,000 members. These standards are as follows:

- Security Standard for ICT Product Supply Chain, Part 1: Chip Security
- Security Standard for ICT Product Supply Chain, Part 2: System Software Security

Due to space constraints, this paper primarily focuses on introducing research related to chip security standard, specifically Part 1 of the Security Standard for ICT Product Supply Chain, which pertains to chip security and has several key impacts and contributions to the semiconductor industry within the domain:

- Enhanced Security and Trust: By implementing specific security standards for semiconductor chips, Taiwan's industry can bolster the overall trust in its products. This is crucial given the sensitive nature of many applications that rely on these components, from personal devices to critical national infrastructure.
- Competitive Advantage: Establishing rigorous standards can give Taiwanese semiconductor manufacturers a competitive edge in international markets. Companies adhering to high security standards may be preferred by customers concerned about security, which is increasingly becoming a critical criterion in supplier selection.
- Regulatory Compliance: With cybersecurity threats evolving, governments and industries worldwide are tightening regulations. Having a robust standard in place can help local companies ensure compliance with both domestic and international regulations, which can be pivotal for maintaining access to global markets.
- Innovation and Research: The focus on chip security can spur innovation and research within the industry. Companies and academic institutions may invest more in developing new technologies that enhance chip security, leading to advancements in the field.
- Risk Mitigation: For the semiconductor industry, which is foundational to virtually all modern electronic devices, any security breach can have catastrophic consequences. These standards help in mitigating risks associated with security vulnerabilities.

## 2. Literature Review

### 2.1 PSA and SESIP

The Internet of Things (IoT) is revolutionizing the supply chain by introducing new levels of connectivity, automation, and data-driven insights. To ensure the security and trustworthiness of IoT devices and platforms within the supply chain, the relevant security standards are PSA (Platform Security Architecture) and SESIP (Secure Evaluation Scheme for IoT Platforms).

The PSA [15] is a certification program designed for ensuring the security of IoT hardware, software, and devices. It encompasses two key components: the security certification (PSA Certified Level 1/2/3) and the functional API certification (PSA Certified Functional API). At its core, PSA defines threat models specific to different device types, enabling manufacturers to identify potential security risks and design appropriate countermeasures. The framework emphasizes the concept of a Root of Trust (RoT), which provides a secure foundation within devices, ensuring the authenticity, integrity, and confidentiality of data and software. PSA also provides a set of security components that manufacturers can incorporate, such as secure storage, communication protocols, trusted execution environments, and secure update mechanisms, enhancing IoT device security and protecting against common attack vectors. Over time, this certification scheme has gained significant adoption among chip manufacturers, system/software developers, and OEMs (Original Equipment Manufacturers).

The SESIP [16] is a comprehensive framework that aims to ensure the security and trustworthiness of IoT platforms. It provides guidelines, specifications, and evaluation criteria for assessing the security posture of IoT platforms. It focuses on key security aspects, including physical attack resistance, device identity, secure updates, secure communication, data protection, and et al. By defining these security requirements, SESIP establishes a standardized framework for evaluating the security features and capabilities of IoT platforms. SESIP plays a critical role in establishing a strong security foundation for IoT platforms, enhancing their security posture, and ensuring that they meet the stringent security requirements of today's connected world. Through SESIP evaluations, organizations can assess the effectiveness of security measures implemented in IoT platforms, ensuring they meet industry-standard security requirements. This evaluation process helps identify any vulnerabilities or weaknesses in the platform's security architecture and enables organizations to take appropriate measures to address them. SESIP promotes the adoption of secure and trustworthy IoT platforms by providing a recognized and standardized approach to evaluating security. It contributes to the overall security and resilience of the IoT ecosystem, fostering a more secure and more reliable environment for IoT deployments.

## 2.2 FIPS 140, ISO/IEC 24759, and ISO/IEC 17825

Security requirements, test requirements and test methods for cryptographic modules include FIPS (Federal Information Processing Standard) 140, ISO/IEC 24759, and ISO/IEC 17825.

FIPS 140 [17] is a security standard established by the U.S. government. It establishes stipulations for cryptographic modules employed in safeguarding sensitive information, serving as a compulsory standard for the protection of valuable or sensitive data within Federal systems. FIPS 140 specifies guidelines for the design, implementation, and testing of these modules. The standard defines four security levels, each representing different levels of security offered by the cryptographic module. Compliance with FIPS 140 is often mandated for cryptographic modules used by government agencies and organizations handling sensitive data. It ensures that these modules meet rigorous security standards and undergo thorough testing and validation. Adhering to FIPS 140 helps organizations enhance the security of their cryptographic systems and demonstrates their compliance with government regulations.

ISO/IEC 24759 [18] defines the testing methodologies to be employed by testing laboratories in assessing the compliance of cryptographic modules with the stipulations outlined in ISO/IEC 19790:2012 [19]. These methodologies are designed to ensure a high level of objectivity throughout the testing process and to establish uniformity across different testing laboratories. Furthermore, this standard outlines the prerequisites for information that vendors must provide to testing laboratories as supporting evidence to substantiate the conformity of their cryptographic modules with the requirements specified in ISO/IEC 19790:2012. Vendors can utilize this document as a reference to validate whether their cryptographic modules meet the requirements outlined in ISO/IEC 19790:2012 before initiating the testing procedure with the laboratory.

ISO/IEC 17825:2016 [20] outlines the non-invasive attack mitigation test metrics utilized to assess compliance with the requirements specified in ISO/IEC 19790:2012 [19] for Security Levels 3 and 4. These test metrics are specifically linked to the security functions outlined in ISO/IEC 19790.

The testing process is carried out at the designated boundary of the cryptographic module, considering the available inputs and outputs within that boundary. The test methods employed by testing laboratories to determine conformity of the cryptographic module with the requirements of ISO/IEC 19790, along with the specified test metrics outlined in this International Standard for each of the associated security functions as defined in ISO/IEC 19790, are documented in ISO/IEC 24759. This International Standard utilizes an efficient "push-button" test approach, ensuring technically sound, repeatable tests that incur moderate costs. The testing methodology adheres to industry best practices and provides a practical and effective means of evaluating the cryptographic module's performance against specified security requirements.

### 2.3 ISO/IEC 15408

ISO/IEC 15408 [21-23], also known as the Common Criteria for Information Technology Security Evaluation, is a standard that encompasses a comprehensive set of requirements for the security functions of IT products and systems, as well as the assurance measures applied during security evaluations. The standard is divided into three parts, each serving a specific purpose:

a) Part 1, Introduction and general model [21], provides an introduction to ISO/IEC 15408 and establishes fundamental concepts and principles for IT security evaluation. It presents a general evaluation model and offers constructs for expressing IT security objectives, defining security requirements, and creating high-level specifications for products and systems.

b) Part 2, Security functional requirements [22], defines a standardized approach for expressing functional requirements for Targets of Evaluation (TOEs). It catalogs a comprehensive set of functional components, families, and classes that serve as a basis for specifying functional requirements.

c) Part 3, Security assurance requirements, establishes a standardized framework for expressing assurance requirements for TOEs. It catalogs a range of assurance components, families, and classes. Part 3 also defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs) and introduces Evaluation Assurance Levels (EALs), which represent predefined scales for rating assurance levels for TOEs.

ISO/IEC 15408 provides a structured and standardized framework for evaluating the security functions and assurance levels of IT products and systems, ensuring consistency and reliability in security evaluations.

Due to the presence of multiple security standards for IoT devices, IT products, and systems, as well as the related security requirements, test requirements, and test methods for cryptographic modules, along with hardware vulnerability information from the CWE database [24], there is a need for a method to establish chip security standards that meet the requirements of the Taiwanese industry.

## 3. The Proposed Chip Security Standard for ICT Product Supply Chain

In the past, III has assisted the industry in developing multiple security standards, such as the Cybersecurity Standard for Video Surveillance System and its Test Specification [25-32], which has been published as the national standard of the Republic of China under the designation CNS16120.

Additionally, III has contributed to the establishment of Security Standard and Test Specification for the Intelligent Bus Telematics System [33-38], and Cybersecurity Standard and Test Specification for Intelligent Streetlight System [39-40]. These initiatives have also facilitated the creation of a related security ecosystem in Taiwan, allowing participating testing laboratories and third-party certification bodies to operate autonomously.

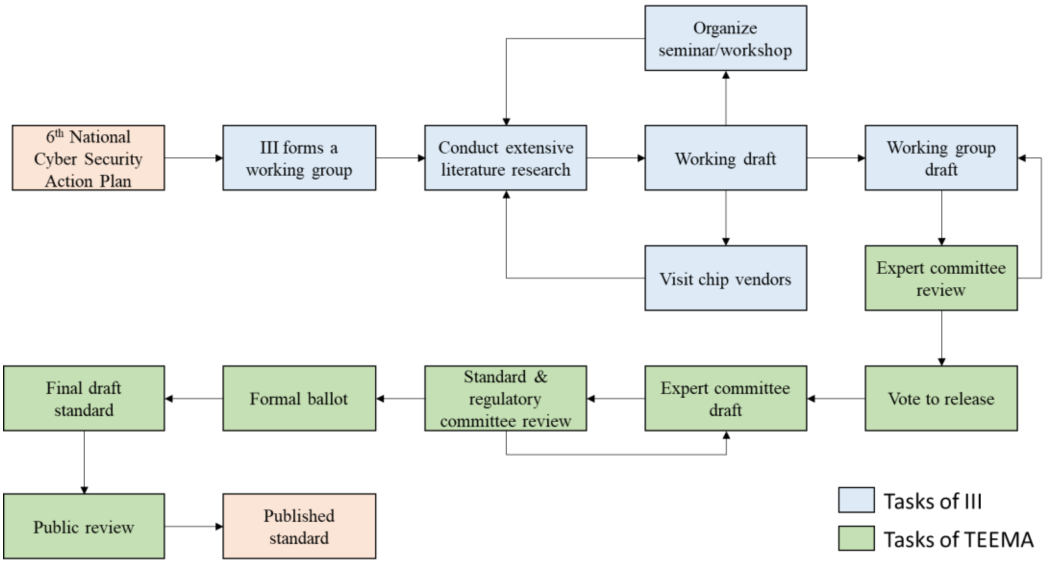


Figure 1. Chip Security Standard Development Process

To establish a chip security standard for ICT product supply chain, following the standards development process suggested by [41-42], III adopted the methodology depicted in Figure 1 and described as follows.

### 3.1 Tasks of III

In accordance with the 6th National Cyber Security Action Plan launched by the Taiwan government, III organized a standards development working group of 6-8 people to conduct extensive research on various security standards and testing specifications, including PSA, SESIP, FIPS 140 and others as mentioned in Section II. The working group's key mission is to develop security standards for trusted chips that can be used by domestic and foreign vendors to promote the trustworthiness of the semiconductor supply chain.

In order to avoid working in isolation, since the first quarter of 2021, III has conducted visits to several key chip vendors in Taiwan to gain insights into their perspectives and requirements regarding the establishment of chip security standards. Due to the short life cycle of many ICT products, a primary requirement from the vendors is to adopt a modular approach. Stakeholders emphasize the need for security standards that are applicable to individual ICT components, such as microprocessors and flash memory, rather than solely focusing on entire ICT products commonly seen in Taiwan. This modular approach enables rapid responsiveness to market demands, provided that the security standard is reasonable, concise, and aligns with existing security standards.

Aligning with existing security standards has been a key focus for III during the process of developing chip security standards. To achieve this, researchers continue extensively studied various security standards related to chip security and cryptographic modules, aiming to meet the expectations of chip manufacturers.

Concurrently, to promote international certification for chip security in Taiwan, III, in collaboration with Brightsight and Winbond, co-organized the "IoT International and Taiwan Security Certification Standards Seminar" in May 2021, attracting a total of 30 participating companies. Additionally, to introduce SESIP certification and the CB accreditation system, III, together with Winbond, Brightsight, and GlobalPlatform, also jointly held the "SESIP Lab and CB Accreditation Workshop" in June 2021, to provide an overview of the program to five prominent local cybersecurity laboratories in Taiwan.

By organizing these activities, III gradually enables domestic chip designers, manufacturers and cybersecurity laboratories to understand the government's plans and progress in developing chip security standards. This aims to raise awareness and importance among them regarding chip security, thereby gradually establishing a chip security ecosystem in Taiwan.

While engaging in vendor feedback collection and conducting seminar/workshop, and after 57 meetings over 8 months, the working group developed a comprehensive set of chip security requirements and testing methods. These requirements encompass various aspects of chip security, starting from the pre-silicon stage where suspicious circuits, commonly known as Hardware Trojans (HT), are identified in chip designs. In the post-silicon stage, measures are taken to prevent side-channel attacks. Additionally, security requirements are also established for chip packaging, firmware, and debug interfaces.

Figure 2 depicts the draft version of the Security Standard for ICT Product Supply Chain. This chip security standard is specifically designed for the security-related hardware components of ICT products, making it applicable to chip vendors. Additionally, there is a separate section in the standard dedicated to security requirements at the system and software layers, targeting system software vendors. For Original Equipment Manufacturers (OEMs), both the chip security standard and system software security standard are applicable.

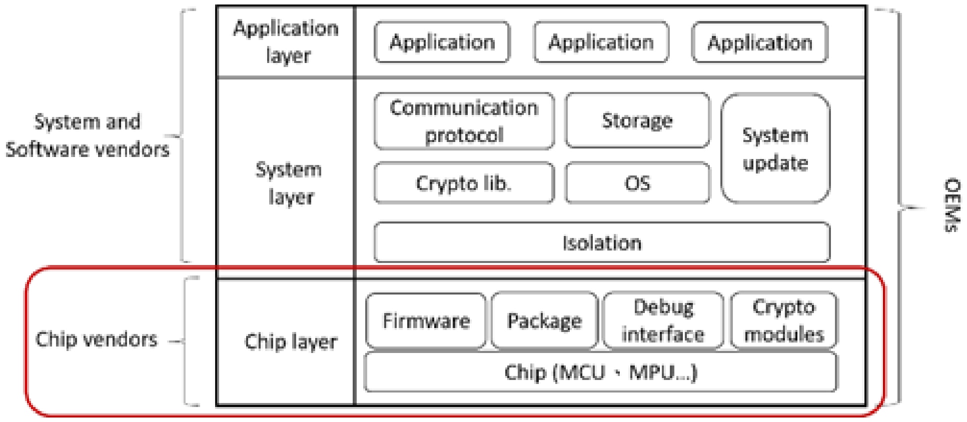
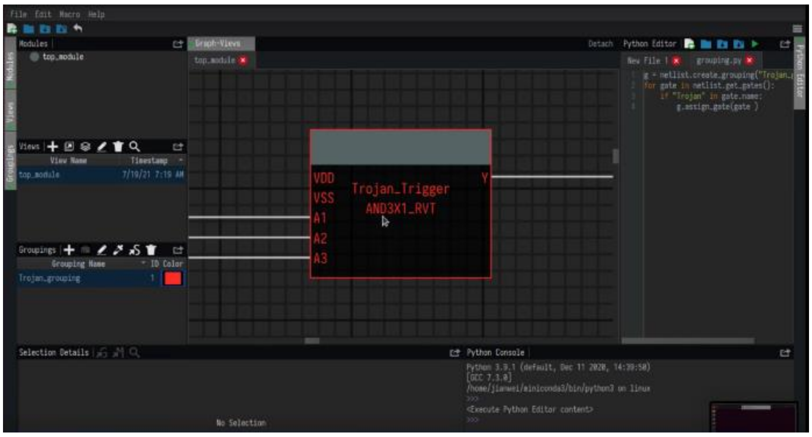


Fig. 2. Security Standard for ICT Product Supply Chain

It is worth noting that during interactions with chip vendors, III recognized the challenge of conducting suspicious circuits testing, as designers are reluctant to share their sensitive chip design files with testing laboratories. To address this issue, III developed a dedicated HT testing software tool (refer to Figure 3), capable of detecting different types of HTs based on the TrustHub [43] benchmark.



```
g = netlist.create_grouping("Trojan_
for gate in netlist.get_gates():
    if "Trojan" in gate.name:
        g.assign_gate(gate )
```

```
Python 3.9.1 (default, Dec 11 2020, 14:39:50)
[GCC 7.3.0]
/home/jianwei/miniconda3/bin/python3 on linux
>>>
<Execute Python Editor content>
>>>
```

Fig. 3. HT test tool developed by III

This tool will be shared with chip designers. Once they have access to the tool, they can utilize the user-friendly graphical interface to import their Verilog files. The tool will then generate a comprehensive test report in PDF format. Chip vendors can simply provide the testing report to the testing laboratory for verification purposes.

In Nov. 2021, TEEMA organized an Industry Consultation Seminar on Chip Security Testing Standards to facilitate discussions and gather feedback from vendors. The seminar successfully attracted the participation of 30 companies and research units, providing a platform for valuable exchanges and insights into chip security testing standards.

After integrating the feedback from stakeholders, III has proposed a working group draft with 31 requirements for chip security standards. For each security requirement, relevant testing specifications have been developed, covering the following eight aspects: compliance, security level, test purpose, precondition, required information from the vendor, test method, pass criteria, and value. The draft was sent to TEEMA for expert committee review.

### 3.2 Tasks of TEEMA

In order to validate the conformity of the standard with industry demands, TEEMA organized the "Expert Review Meeting on Chip Security Standards and Testing Specifications," inviting representatives from the industry, academia, and government department, totaling 12 individuals.

During the comprehensive review conducted by the committee, various comments were provided, including the observation that the threat of Fault Injection Attacks, specifically clock glitch and voltage glitch, is increasing in relation to microcontroller units (MCUs) security. The document currently focuses on chips having the ability to withstand physical attacks, but it is recommended that the capabilities to explicitly counter fault injection attacks, such as clock glitch and voltage glitch, be included in the document.

Another comment highlighted the need for a mechanism to detect physical attacks on chip cryptographic modules, specifically the inclusion of a tamper response logging mechanism. It was noted that relying solely on packaging protection may not be sufficient to meet this requirement.

Therefore, it is necessary to incorporate chip protection design to effectively fulfill this requirement.

The standard and testing specifications underwent a comprehensive review by the committee. III utilized these comments to revise the standard and testing specifications accordingly. After two rounds of professional review meetings and a vote to release, the committee finally approved the Security Standards and Testing Specifications for ICT Product Supply Chain as expert committee draft.

Following TEEMA's industry standard publication process, TEEMA subsequently convened a "Standard and Regulatory Committee" consisting of another group of 8 experts to conduct a further review of the expert committee draft. III made necessary adjustments based on the committee's feedback. After formal ballot by the committee, TEEMA conducted a one-month public review of the final draft standard. Finally, on November 8, 2022, following the completion of the public review, the standard and testing specifications were officially published as the industry standard in Taiwan.

## 4. Overview of Chip Security Standard in Taiwan

The Chip Security Standard delineates security requirements at the chip level. During the pre-silicon stage, chip designs must circumvent the inclusion of suspicious circuits, while in the post-silicon stage, they should thwart non-intrusive side-channel and fault injection attacks. Additionally, this standard outlines security requirements pertaining to chip packaging, firmware, and debug interfaces. As the chip layer serves as the foundational component of ICT products, it establishes a fundamental security environment for the proper functioning of upper-layer system software. Consequently, Part 1: Chip Security Standard is eligible for independent certification. The Chip Security Standard encompasses five key aspects, each elucidating distinct security requirements for components.

### 4.1 Chip Security

The component shall possess the capability to detect and resist intrusion. Chip security requirements encompass secure chip design and the use of robust packaging materials. The three primary sub-aspects defining chip security are detailed below:

1. Chip body

I. During the cryptographic operations, the component shall not cause differences in processing time due to different Critical Security Parameter (CSP, such as secret keys, passwords, etc.) values, so as to prevent the discovery of the dependency between execution time and CSP through timing analysis.

II. During the cryptographic operations, the component shall prevent attackers from finding out the operation sequence of cryptographic operations through simple power analysis or simple electromagnetic analysis.

III. The traces of the component during cryptographic operations shall prevent attackers from discovering the CSP used by the component through differential power analysis or differential electromagnetic analysis.

IV. During the cryptographic operations, the component shall prevent attackers from generating stable abnormal output through differential fault analysis or electromagnetic fault injection, or causing potential CSP leakage problems.

2. Chip design

   I. The component shall not be suspected of being a hardware Trojan in the circuit design.

3. Chip security module protection

   I. 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.

   II. The Cryptographic module components shall be covered with opaque, hard tamper-resistant coating or packaging material, and shall retain evidence of tampering or removal when tampered with.

   III. Cryptographic module components shall have a tampered response mechanism.

### 4.2 Physical Interface Security

The debugging interface provided by the chip shall have robust security measures. The key sub-aspects encompassing physical interface security are delineated below:

1. Debug interface

   I. 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.

   II. 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.

2. Functional protection

   I. 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.).

### 4.3 Hardware Component Security

The proper identification (authentication) and secure updating/factory resetting of hardware components are imperative. Consequently, the five primary sub-aspects constituting hardware component security are outlined as follows:

1. Chip Identity

   I. The component shall have unique identification information and can be correctly identified.

   II. The hardware instance shall have unique identification information and can be correctly identified.

   III. The component shall provide a mechanism to verify its authenticity to ensure that it is not an illegal clone.

2. Hardware operating status

   I. The authenticity and integrity of the component shall be verified during start-up.

   II. 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.

3. Security update
    - I. The component shall provide a secure firmware update capability in the user environment.
4. Factory reset
    - I. The component shall provide a factory reset function to destroy user data stored in the product.
    - II. The component shall provide decommissioning capabilities to destroy applications, sensitive data, and personal data in the product, rendering the product unusable.
    - III. 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.
5. Isolation security
    - I. 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.
    - II. The component shall provide effective isolation between hardware components, preventing weak components from becoming an attack agents that cause damage to other components.

### 4.4 Cryptographic Security

The cryptographic algorithms, keys, and random number generators employed in the component shall exhibit adequate security strength. Hence, the three sub-aspects comprising cryptographic security are expounded below:

1. Cryptographic algorithm security
    - I. Various cryptographic operations used by the component, such as encryption, decryption, digital signature, etc., shall 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.
2. Key security
    - I. 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.
    - II. CSPs stored in KeyStore shall protect their authenticity, integrity, and confidentiality.
3. Random number generator security
    - I. 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.

### 4.5 Firmware Security

The firmware employed in the component shall guarantee confidentiality, authenticity, and integrity. Therefore, the five sub-aspects encompassing firmware security are elucidated as follows

1. Firmware protection

I. Firmware shall not be extracted to analyze CSPs in plaintext.

II. 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.

III. The firmware shall have an authenticity check mechanism, and the keys used for authenticity check shall be protected.

IV. Firmware shall have an integrity check mechanism to prevent users from updating with tampered firmware.

V. Firmware shall have an authenticity check mechanism to prevent users from updating with fake firmware.

## 5. Conclusions

Since the chip security standard was published as an industry standard, III has been continuously promoting the importance of chip security to the public. Many chip designers have started inquiring about chip security testing methods and the benefits they can bring. Some vendors have begun collaborating with III, and after signing an NDA, they have entrusted III's chip security testing laboratory to conduct pre-tests to evaluate the security of their products against side-channel attacks and fault injection attacks.

It must be acknowledged that Taiwan's chip security industry is still in its early stages, and many procedures and systems are still being explored. For example, there is significant concern about how to enable the reuse of evaluation results and where to obtain chip security consulting services. Additionally, Taiwan also needs to establish its own certification bodies, and efforts are currently underway in this regard.

In the long run, it is important for Taiwan's chip security standards to align with international standards. In line with this objective, III signed a Memorandum of Understanding (MOU) with GlobalPlatform in November 2022. The collaboration aims to facilitate the harmonization of Taiwan's chip security standards with SESIP. Both parties will engage in relevant work to achieve this goal.

This paper elaborates on III's efforts in formulating chip security standards to enhance the trustworthiness of the semiconductor supply chain. A total of 31 chip security requirements that have been endorsed by experts and published as industry standards in Taiwan. These security requirements cover chip design security, packaging security, debug interface security, side-channel and fault injection security, among others. With the support of the Taiwan Ministry of Digital Affairs, III continues visiting chip vendors and laboratories, organizing various workshops, and conducting promotional activities. Currently, chip design companies in Taiwan are increasingly aware of the importance of chip security. When chips are required for critical applications such as the automotive industry, more companies are seeking domestic resources to help address their challenges.

Securing the semiconductor supply chain at its source is essential to building trust in the digital world, the government is committed to continuously allocating resources for the development of Taiwan's chip security ecosystem. The goal is to establish a comprehensive chip security assessment process domestically and establish international certification bodies through cross-border collaboration and interoperability. Additionally, efforts are being made to enhance evaluation techniques through product assessments, cultivate talent in chip security evaluation, and build a robust chip security industry ecosystem, laying a solid foundation for "local testing, global recognition."

## Acknowledgements

This paper is conducted under the “Taiwan Information Security Research Excellently and Carefully – Information security key technology development plan for Semiconductor and Information Communication Supply Chain (3/4)” of the Institute for Information Industry which is subsidized by Ministry of Digital Affairs of the Republic of China (Taiwan).

### References

[1] Lin, Y.L. and Ong, C.S. Three Legs of the Vessel for Customer Loyalty: Security, Risk and Trust. Journal of Information Management, 2021, 28, 101-124.

[2] Wu, Y.H., Chu, S. Y. and Fang, W.C. An Empirical Study of Trust and TAM - An Example of Online Shopping. Journal of Information Management, 2008, 15, 123-152.

[3] Ting, H.L.J., Kang, X., Li, T., Wang, H. and Chu, C. -K. On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study, 2021, 9, 106743-106783, DOI: 10.1109/ACCESS.2021.3100767.

[4] Wang, Y.M. and Hsueh, L.W. Assessing the Internet Privacy Self-Efficacy Scale Using the Partial Least Squares Structural Equation Modeling (PLS-SEM) Approach. Basic & Clinical Pharmacology & Toxicology, 2019, 124, 366-366.

[5] Wang, Y.M. and Lin, W.C. Understanding consumer intention to pay by contactless credit cards in Taiwan. International Journal of Mobile Communications, 2018, 17, 1-23. DOI: 10.1504/IJMC.2018.10008698.

[6] Wang, Y.M., Wang, Y.S. and Yang, Y.F. Understanding The Determinants of RFID Adoption In The Manufacturing Industry. Technological Forecasting and Social Change, 2010, 803-815. DOI: 10.1016/j.techfore.2010.03.006.

[7] Wu, C.M., Chu, S.Y. and Fang, W.C. The Study of Trust and Commitment Influence Factors in Supply Chain Relationships-Transaction Cost and Social Exchange Theories Perspectives. Journal of Information Management, 2006, 13, 91-118. DOI: 10.6382/JIM.200610.0005

[8] Kim, Y., et al. Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors. 2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA), 2014, 361-372. DOI: 10.1109/ISCA.2014.6853210.

[9] Jattke, P., Van Der Veen, V., Frigo, P., Gunter, S. and Razavi, K. BLACKSMITH: Scalable Rowhammering in The Frequency Domain. 2022 IEEE Symposium on Security and Privacy, 2022, 716-734. DOI: 10.1109/SP46214.2022.9833772

[10] Paul, K., et al. Spectre Attacks: Exploiting Speculative Execution. 2019 IEEE Symposium on Security and Privacy, 2019, DOI: 10.1109/SP.2019.00002

[11] Lipp, M., et al. Meltdown: Reading Kernel Memory from User Space. Communications of the ACM, 2020, 63, 46–56. DOI: 10.1145/3357033

[12] Prout, A., et al. Measuring the Impact of Spectre and Meltdown. 2018 IEEE High Performance Extreme Computing Conference (HPEC), 2018, 1-5. DOI: 10.1109/HPEC.2018.8547554.

[13] Markettos, A.T., et al. Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection Via DMA from Untrustworthy Peripherals. 26th Annual Network and Distributed System Security Symposium (NDSS 2019), 2019, DOI: 10.14722/ndss.2019.23194.

[14] Classen, J., Gringoli, F., Hermann, M. and Hollick, M. Attacks on wireless coexistence: exploiting cross-technology performance features for inter-chip privilege escalation. 2022 IEEE Symposium on Security and Privacy (SP), 2022, 1229-1245. DOI: 10.48550/arXiv.2112.05719.

[15] Arm Limited. Platform Security Model, Version 1.1. Document number: JSADEN014, Dec. 2021.

[16] GlobalPlatform Technology. Security Evaluation Standard for IoT Platforms (SESIP), Version 1.1. Document Reference: GP_FST_070, Jun. 2021.

[17] Cooper, M.J. and Schaffer, K.B. FIPS 140-3, Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication. National Institute of Standards and Technology, March 2019.

[18] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 24759:2017 Information Technology — Security Techniques — Test Requirements for Cryptographic Modules, Mar. 2017.

[19] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 19790:2012 Information Technology — Security Techniques — Security Requirements for Cryptographic Modules, Nov. 2015.

[20] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 17825:2016 Information Technology — Security Techniques — Testing Methods for The Mitigation of Non-Invasive Attack Classes Against Cryptographic Modules, Jan. 2016.

[21] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 15408-1:2009 Information Technology — Security Techniques — Evaluation Criteria for It Security — Part 1: Introduction and General Model, Jan. 2014.

[22] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 15408-2:2008 Information Technology — Security Techniques — Evaluation Criteria for It Security — Part 2: Security Functional Components, May. 2011.

[23] ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection. ISO/IEC 15408-3:2008 Information Technology — Security Techniques — Evaluation Criteria for It Security — Part 3: Security Assurance Components, May. 2011.

[24] CWE Content Team. CWE VIEW: Hardware Design, View ID: 1194, MITRE, Dec. 2019.

[25] Taiwan Association of Information and Communication Standards. Video Surveillance System Cybersecurity Standard-Part 1: General Requirements, Release date: 2019-03-26, File number: TAICS TS-0014-1(E) v1.0.

[26] Taiwan Association of Information and Communication Standards. Video Surveillance System Cybersecurity Standard-Part 2: IP Camera, Release date: 2019-03-26, File number: TAICS TS-0014-2(E) v2.0.

[27] Taiwan Association of Information and Communication Standards. Video Surveillance System Cybersecurity Standard-Part 3: Video Recorder, Release date: 2019-03-26, File number: TAICS TS-0014-3(E) v1.0.

[28] Taiwan Association of Information and Communication Standards. Video Surveillance System Cybersecurity Standard-Part 4: Network Attached Storage, Release date: 2019-03-26, File number: TAICS TS-0014-4(E) v1.0.

[29] Taiwan Association of Information and Communication Standards. Cybersecurity Test Specification for Video Surveillance System-Part 1: General Requirements, Release date: 2019-05-30, File number: TAICS TS-0015-1(E) v1.0.

[30] Taiwan Association of Information and Communication Standards. Cybersecurity Test Specification for Video

Surveillance System-Part 2: IP Camera, Release date: 2019-05-30, File number: TAICS TS-0015-2(E) v2.0.

[31] Taiwan Association of Information and Communication Standards. Cybersecurity Test Specification for Video Surveillance System-Part 3: Video Recorder, Release date: 2019-05-30, File number: TAICS TS-0015-3(E) v1.0.

[32] Taiwan Association of Information and Communication Standards. Cybersecurity Test Specification for Video Surveillance System-Part 4: Network Attached Storage, Release date: 2019-05-30, File number: TAICS TS-0015-4(E) v1.0.

[33] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Standard-Part 1: General Requirements v2, Release date: 2019-08-13, File number: TAICS TS-0020-1 v2.0.

[34] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Standard-Part 2: On Board Unit v2, Release date: 2019-08-13, File number: TAICS TS-0020-2 v2.0.

[35] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Standard-Part 3: Intelligent Bus Stop v2, Release date: 2019-08-13, File number: TAICS TS-0020-3 v2.0.

[36] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Test Specification-Part 1: General Requirements v2, Release date: 2019-08-13, File number: TAICS TS-0021-1 v2.0.

[37] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Test Specification-Part 2: On Board Unit v2, Release date: 2019-08-13, File number: TAICS TS-0021-2 v2.0.

[38] Taiwan Association of Information and Communication Standards. Intelligent Bus Telematics System Security Test Specification -Part 3: Intelligent Bus Stop v2, Release date: 2019-08-13, File number: TAICS TS-0021-3 v2.0.

[39] Taiwan Association of Information and Communication Standards. Intelligent Streetlight System Security Standard-Part 1: General Requirements, Release date: 2020-07-27, File number: TAICS TS-0027-1(E) v1.0.

[40] Taiwan Association of Information and Communication Standards. Intelligent Streetlight System Security Standard-Part 2: Intelligent Lighting, Release date：2020-07-27 / File number：TAICS TS-0027-2(E) v1.0.

[41] Arter, D.R. The Standards Development Process. Quality Progress, 1999, 32, 65-69.

[42] Sulzberger, V. and Gallagher, T. Reliability and Security: The NERC New Standards Development Process. IEEE Power and Energy Magazine, 2004, 2, 56-61. DOI: 10.1109/MPAE.2004.1269623.

[43] Tehranipoor, M., Karri, R., Koushanfar, F. and Potkonjak, M. Trusthub, http://trust-hub.org