I want to use the same mobile for business and personal calls.
But keep the bills separate.

Taiwan Chip Security Test Specification

Institute for Information Industry

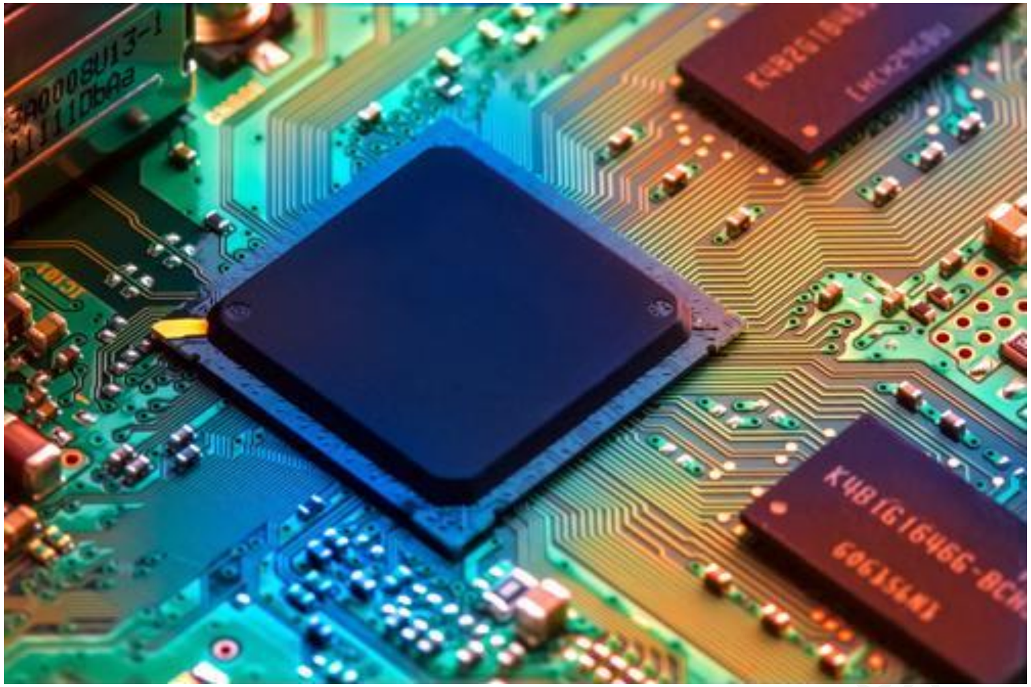
Cyber Security Technology Institute

Increasing threat to chip security

Various IoT devices continue to add chip functions, unknowingly introducing other vulnerabilities with different threat levels into the device

If the hardware that runs the software is compromised, efforts to protect the software will be futile

- National defense and military systems, or critical infrastructure related to people's livelihood, are increasingly dependent on information and communication technology (ICT).
- Under the trend of globalization of ICT procurement, chip security is not only related to national security, but also the foundation of all ICT supply chain security.



Chip security test specification

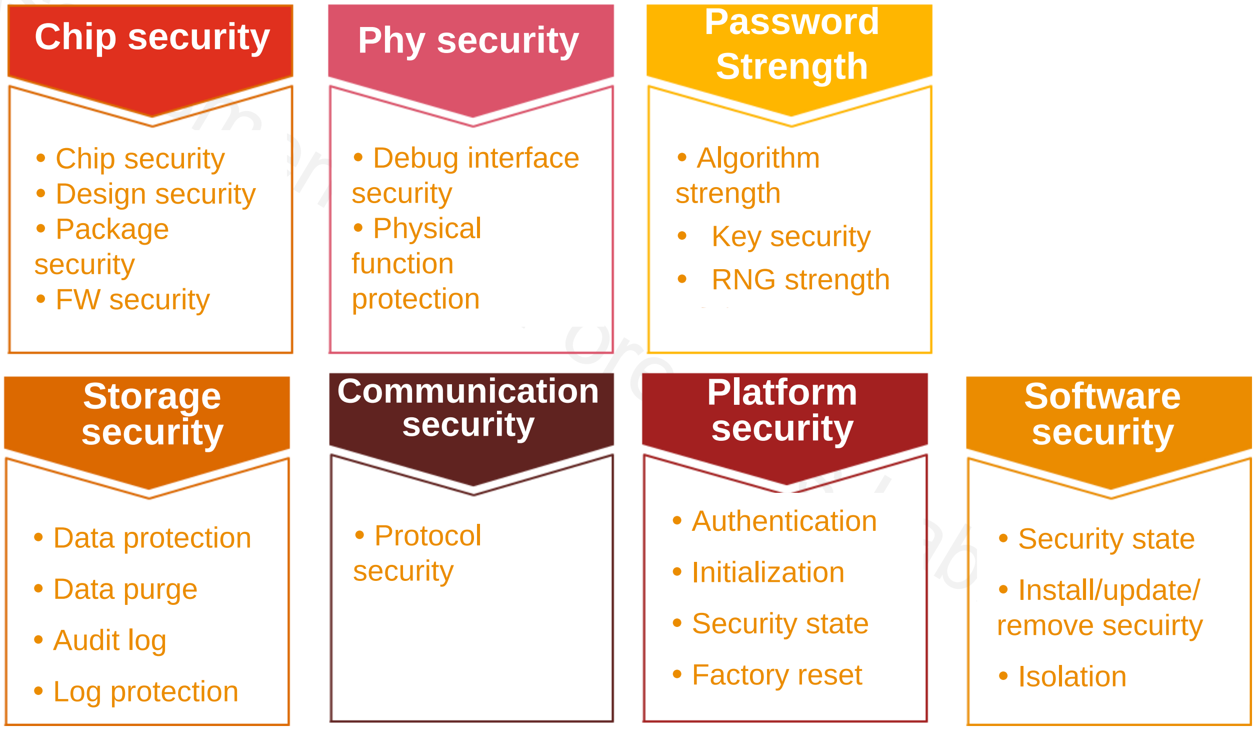
We have drafted 43 test items based on the requirements of international standards, which will become the security regulations for the import of chip products into Taiwan:

- SESIP (Security Evaluation Standard for IoT Platforms)
- ISO/IEC 24759 firmware security
- FIPS 140 physical security
- ISO/IEC 17825

There are 7 categories：

- Name
- Purpose
- Pre-condition
- Manufacturer declaration
- Test method
- Pass criteria
- Outcome

From hard to soft, from component to platform



Chip security
- Chip security
- Design security
- Package security
- FW security

Phy security
- Debug interface security
- Physical function protection

Password Strength
- Algorithm strength
- Key security
- RNG strength

Storage security
- Data protection
- Data purge
- Audit log
- Log protection

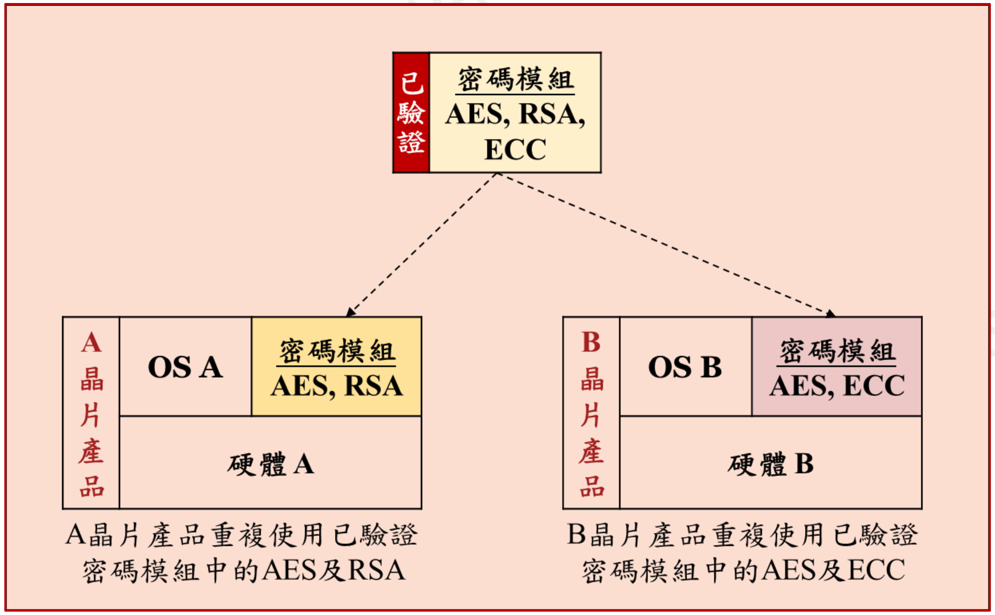
Communication security
- Protocol security

Platform security
- Authentication
- Initialization
- Security state
- Factory reset

Software security
- Security state
- Install/update/remove security
- Isolation

Certification Reuse

We proposed an evaluation method that is conducive to combination, allowing the testing of individual or combined product components, so that the component verification results completed in this way are still applicable in different product combinations



已驗證

密碼模組 AES, RSA, ECC

A晶片產品

OS A

密碼模組 AES, RSA

硬體 A

A晶片產品重複使用已驗證密碼模組中的AES及RSA

B晶片產品

OS B

密碼模組 AES, ECC

硬體 B

B晶片產品重複使用已驗證密碼模組中的AES及ECC

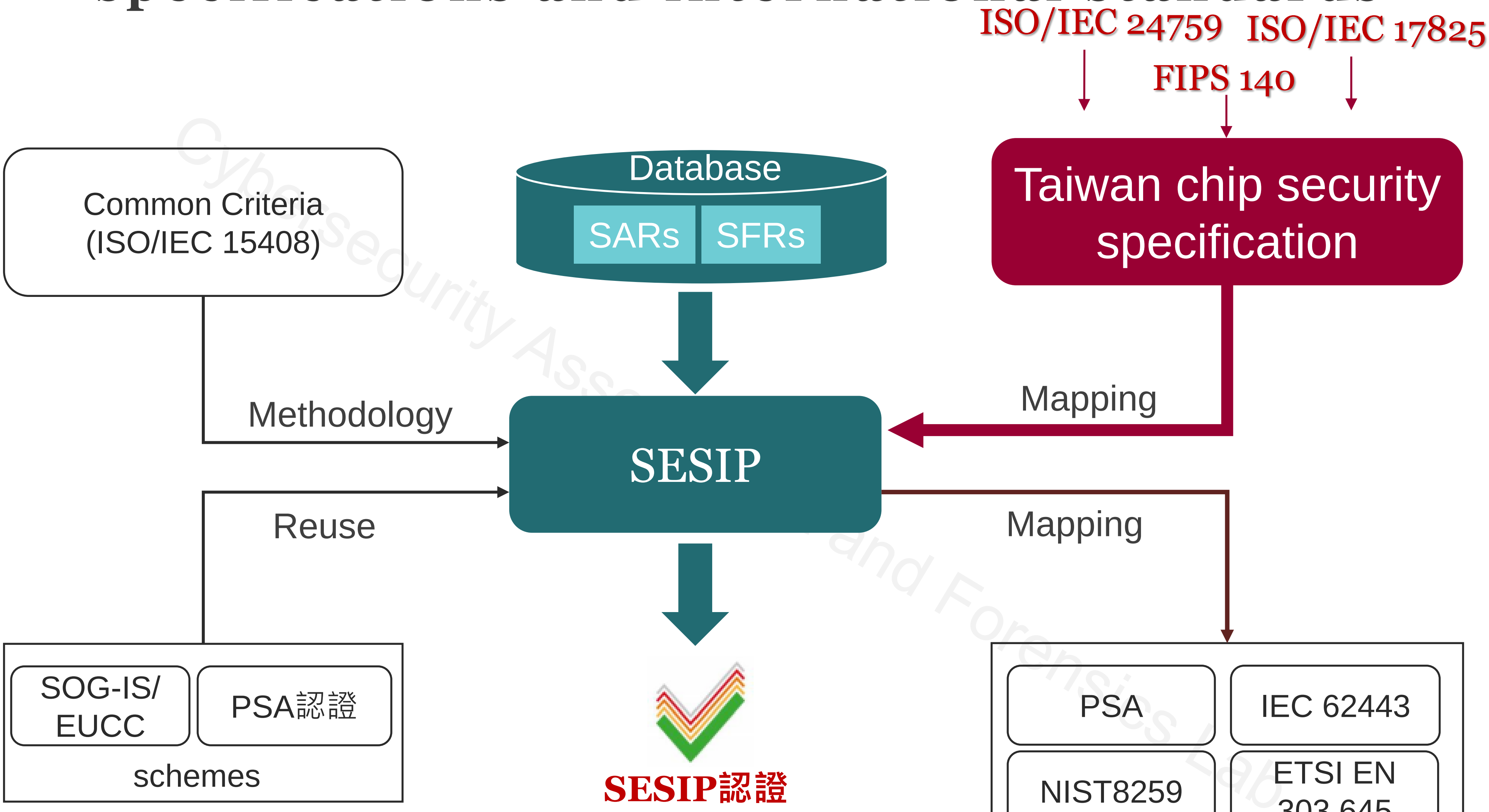
Reuse (reuse) the components that have been verified to reduce the cost and waste of repeated testing

For product manufacturers who purchase verified components, they will benefit from reducing test costs and shortening time to market

enisa

"As part of the new verification, it should be possible to reuse the evaluation results of other ICT product verification. Therefore, the applicant can provide the previous evaluation results to the conformity assessment body (CAB), including the product life cycle or the applicant The evaluation results related to the patch management method of the CAB are used as evidence of reuse. When the evidence provided meets the evidence requirements required by the CAB and the authenticity of the evidence can be confirmed, the CAB shall use these results in its evaluation tasks."

The relationship between test specifications and international standards



1. SAR: Security Assurance Requirement
2. SFR: Security Function Requirement

Chip security related test items

Safety/non-safety function protection

Detect or prevent the attacker with physical access before the attacker damages any safety function and non-safety function

Packaging protection

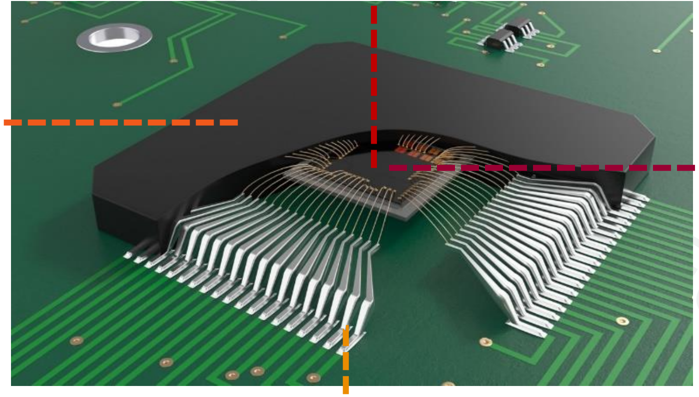
Verify whether chip module is tampered or removed cryptographic, whether the evidence of tampering or removal is retained, and whether there is a tampering record

debugging interface security

Ensure that the services provided by the interface will not be abused, and the security of the authentication function used by the debugging interface

Chip design

complex semiconductor supply chain, which may cause the chip to be implanted with suspicious circuits during the chip design process in order to launch an information security attack



Firmware security

Verify that there is no smart data in the firmware file, or the smart has been properly protected, and to avoid suspicious links and code in the firmware, and unauthorized disclosure and modification of the source code, etc.

Chip body

1. test whether the chip using attack mitigation technology can resist side channel attacks when performing cryptographic operations.
2. Use latent bias in physical quantity measurements (such as electromagnetic fields, power consumption, and time difference) measured on or around the chip to try to find smart information such as keys

cryptographic algorithm and other test items

Cryptographic strength

Detect whether the DUT uses a cryptographic algorithm that meets the specifications to reduce the probability of data being cracked.

Key security

Verify whether the key generation method of the DUT meets the specification, and ensure that the CSP stored in the KeyStore will not be destroyed, which will endanger the authenticity, integrity, and confidentiality of the data

RNG strength

The random number generation method conforms to the specification, which can ensure that the DUT generates a safer random number for use by the cryptographic algorithm

Data protection

Verify whether all data stored in the application is protected by authenticity, integrity, and confidentiality.

Information purge

Verify whether the deleted data may have valuable information remaining in the memory, and whether it has been erased at the same time and cannot be recovered.

Log protection

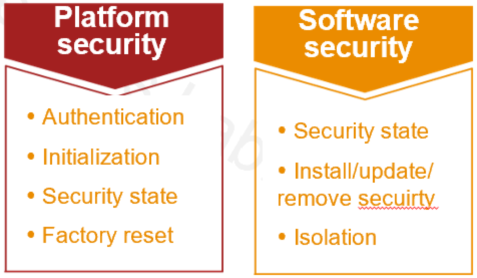
The generation and storage methods of the audit log meet the security requirements, which can be used to detect the attacker's attempts to the product.

Increasing log security

Verify whether the indicator increment counter is vulnerable to damage

Protocol security

Verify whether the security communication protocols and measures used are subject to the security specification



Platform security

- Authentication
- Initialization
- Security state
- Factory reset

Software security

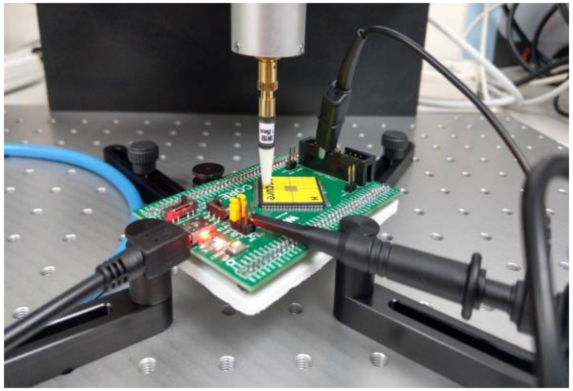
- Security state
- Install/update/ remove security
- Isolation

Example

TA test (1/3)

a) Purpose :

Detect whether the different CSP value of the device under test will cause the difference in processing time during the process of performing the cryptographic calculation, which is vulnerable to TA attacks.



b) Pre-condition :

The DUT can perform a cryptographic calculation.

c)) The products sent by manufacturers for testing should attach the following information :

1) The cryptographic algorithm used by the product.
2) Declare a mechanism to protect CSP and cryptographic algorithms against side-channel attacks.
3) Declare the conditions/modes under which the DUT is vulnerable to side channel analysis.
4) Explain the steps for triggering and judging the start and stop of cryptographic operations to obtain the best synchronization signal.
5) Explain the steps to modify CSP and ciphertext for side-channel attack testing.

TA test (2/3)

Example

d) Test methods :

1) Perform signal calibration for the start and stop of cryptographic calculations.

2) **Use random CSP and fixed plain text string, perform 1,000 times or less than 6 hours of timing measurement.**

3) Perform statistical analysis on timing measurement results, review execution time and CSP used.

4) Take a certain time unit (for example: microseconds, milliseconds, etc.) as a benchmark, count the execution time of all samples, and calculate whether the dependency between the execution time and CSP in the number of samples is ≥5%. If the threshold is exceeded, the test fails, otherwise continue to perform the following steps .

5) **Use random plain text strings and fixed CSP to perform 1,000 times or less than 6 hours of timing measurement.**

6) Take a certain time unit (such as microseconds, milliseconds, etc.) as a benchmark, count the execution time of all samples, and calculate the dependency between the execution time and the plain text string in the number of samples, whether ≥5%.

7) If the execution time of the above steps (4) and (6) is difficult to measure (for example, there is noise or delay time), use the clock cycle of the chip under test as the tolerance value ε.

TA test (3/3)

Example

e) Passing Criteria：

1) Unable to perform signal correction for the start and stop of cryptographic calculations.

2) Dependency between execution time and CSP < 5%, And the dependency between the execution time and the plain text string is < 5%.

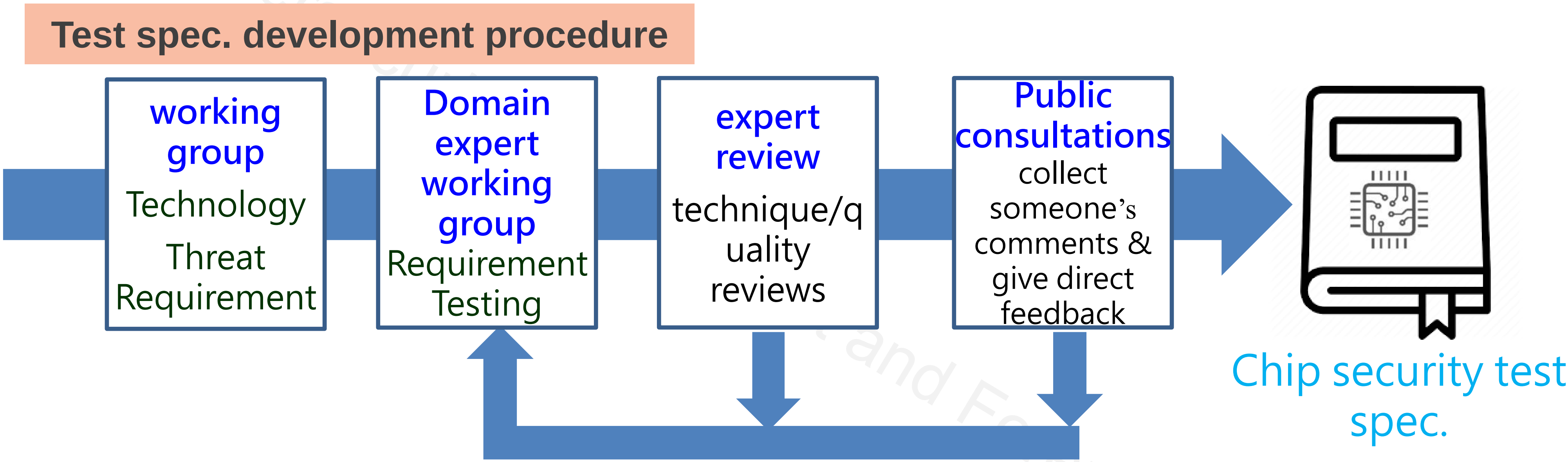
3) |T1 - T2|< ε， 且|T1’ - T2’|< ε。

1) ~ 3) results should meet one of them.

f) Pass Benefits：

TA attacks are often overlooked in the design stage, because timing weaknesses are only revealed in the implementation stage, and may be unintentionally introduced during compiler optimization. The chip that passes this test item indicates that mitigation measures used in the design or implementation phase can improve the chip's ability to resist side-channel attacks in timing analysis.

Chip security standard development



Test spec. development procedure

working group
Technology
Threat
Requirement

Domain expert working group
Requirement
Testing

expert review
technique/quality reviews

Public consultations
collect someone's comments & give direct feedback

Chip security test spec.

- Based on expert opinion to revise content
- Collect opinions
- Provide revision reference

Thank you