AIST
Create the Future, Collaborate Together

CPSEC

Supply Chain Security: Security Requirement Documents for Connected Components

Hirotaka Yoshida
AIST/CPSEC Group Leader
ICSS-RT Secretary-General

This presentation is based on results obtained from a project, JPNP23013, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Contents

AIST
Create the Future, Collaborate Together

Background -Security Assurance-

Security certification/assurance schemes

EU Cyber Resilience Act (CRA)[CRA]

BSZ （Beschleunigte Sicherheitszertifzierung）[BSZ]

U.S. Cyber Trust Mark. [Cyber]

CSPN （Certification de sécurité de premier niveau） [CSPN]

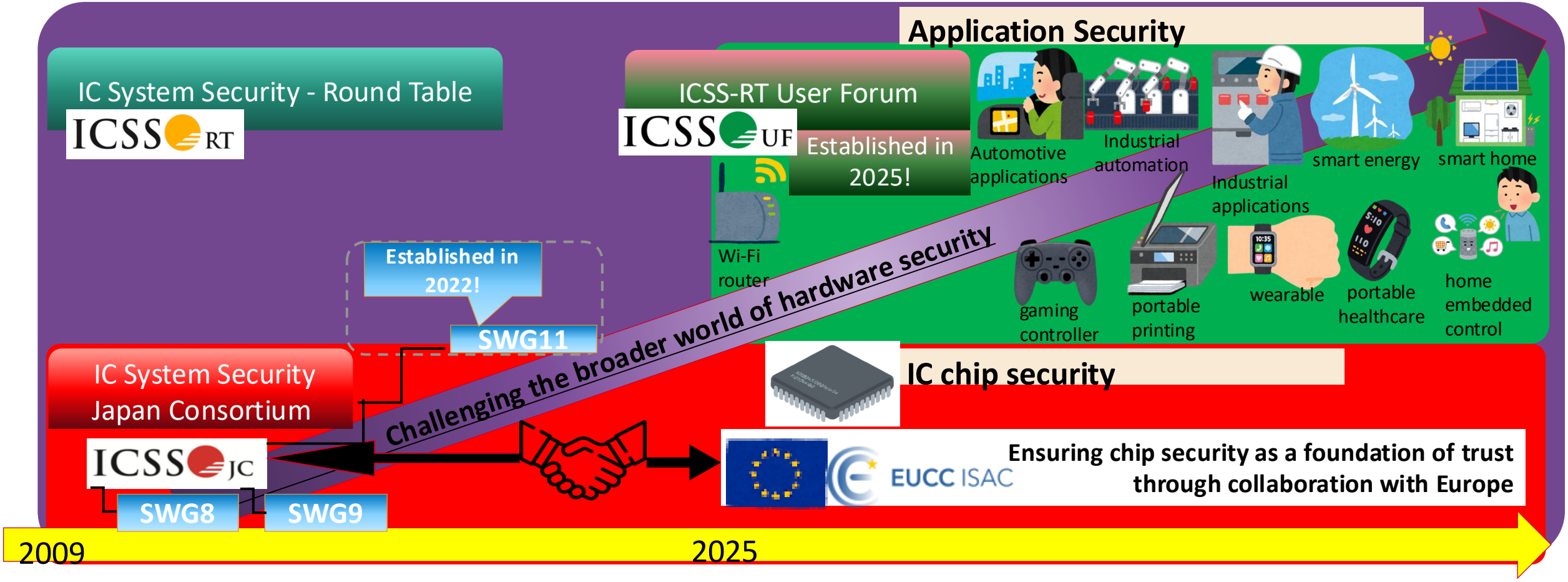
Cybersecurity Labelling Scheme [CLS]

Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements [JC-STAR]

[CRA] EU CRA: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF
[JC-STAR] https://www.ipa.go.jp/security/jc-star/index.html
[METI] https://www.meti.go.jp/press/2023/03/20240315005/20240315005-3r.pdf
[ETSI] ETSI EN 303 645https://www.ipa.go.jp/security/controlsystem/hjuojm000000418j-att/en_303645v020101p.pdf
[NIST] NISTIR 8425https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf
[Cyber] Executive Order 14028, Improving the Nation's Cybersecurity, May 12, 2021 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[RED] Radio Equipment Directive (RED): DIRECTIVE 2014/53/ https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053
[FiT CEM] EN 17640, “Fixedtime cybersecurity evaluation methodology for ICT products” (FiT CEM), October 2022, Cen/Cenelec
[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
[CSPN] www.ssi.gouv.fr/administration/produitscertifes/cspn/
[BSZ] www.bsi.bund.de/bsz
[CLS] About Cybersecurity Labelling Scheme for IoT - CLS(IoT) https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about

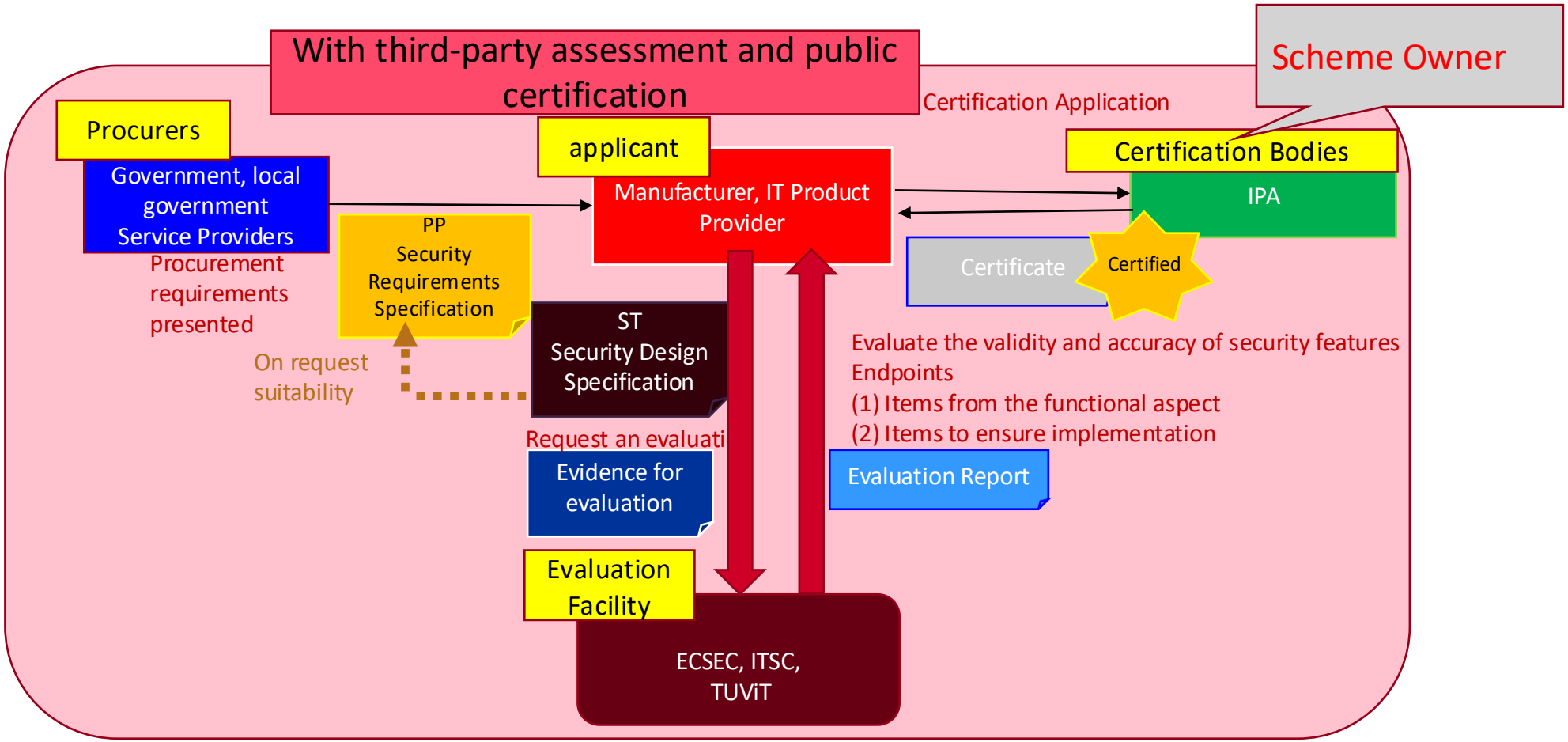
ICSS-RT Activities in Japan

- The concept and applications of “IC systems” have expanded from the IC card field to semiconductor chips for embedded devices and a wide range of applications.
- Modern requirements: Implementing minimal security and quantum-resistant cryptography even in lightweight edge devices.



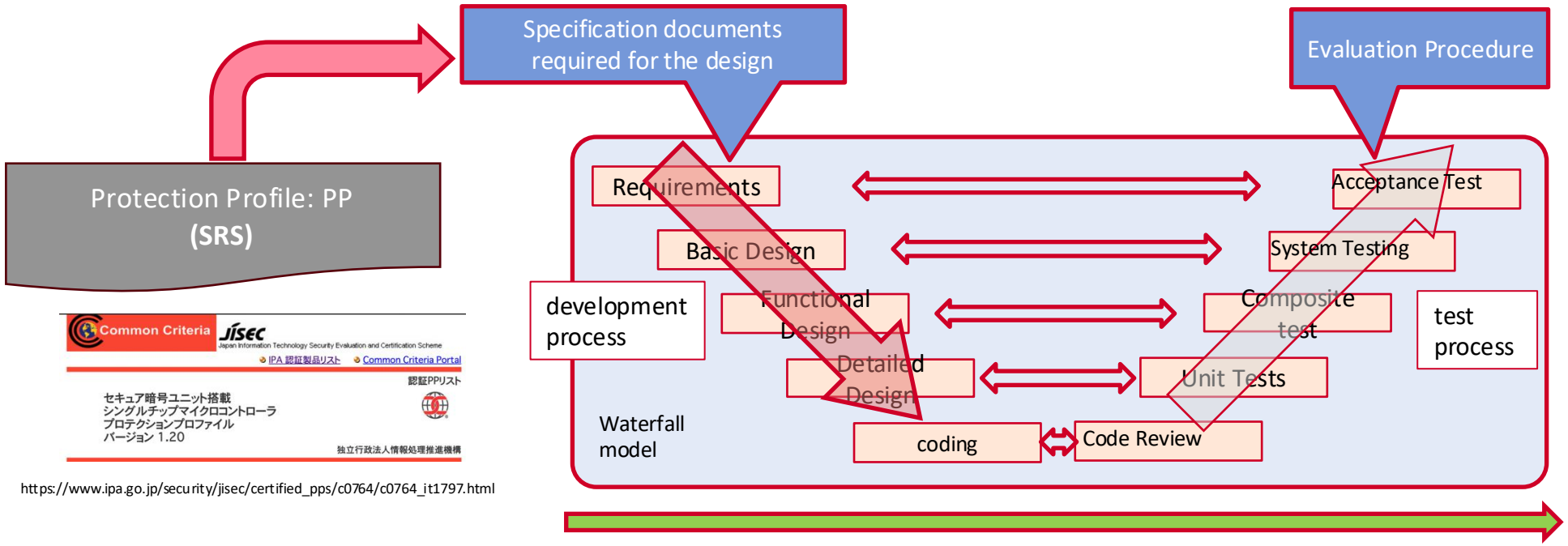
Evaluation and certification with PP/ST in CC

- JISEC (Japan Information Security Evaluation and Certification Scheme)
  A scheme for certifying IT products based on the evaluation standard ISO/IEC 15408 (Common Criteria: CC)
- CC: Common Criteria for Information Technology Security Evaluation



Security Requirements Specification

- The security requirements specification clarifies what requirements must be met in secure development.



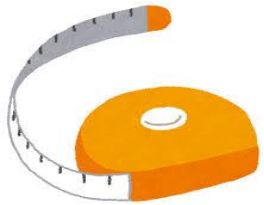
https://www.ipa.go.jp/security/jisec/certified_pps/c0764/c0764_it1797.html

The position of PP in secure development

Background – Hardware Security –

Hardware security evaluation/certification by the European SOG-IS

- Smart cards can move with users “anytime, anywhere”
- Attackers can easily obtain them
- Attacks may place a probe needle directly on the semiconductor chip mounted on the card and may steal signals flowing through the chip's circuitry
- To obtain cryptographic keys, attacks may exploit via the “physical interface” etc., by observing the power consumption or electromagnetic waves generated when the chip performs cryptographic processing
- In the field of hardware security, numerous attacks have been known since the year 2000, SOG-IS consolidates these into ten attacks, organizes them, and then **establishes evaluation criteria**



A critical role in high-assurance security evaluations

Working Group Structure

JIWG
(Joint Interpretation Working Group)
JIL (Joint Interpretation Library)

JHAS
(JIL Hardware Attack Subgroup)
Examine security evaluation and certification standards for smart cards (IC chips) and similar technologies

JEDS
(JIL Embedded Devices Subgroup)
Reviewing security evaluation certification standards for embedded devices

Crypto Working Group
Examine cryptographic mechanisms

JTEMS
(JIL Terminal Evaluation Methodology Subgroup)
Examining Security Evaluation Methods for Payment Terminals

https://www.sogis.eu/
https://www.sogis.org/uk/detail_operation_en.html

Transition of from SOGIS to ENISA

- The EU Cybersecurity Act was adopted by the Parliament in 2019 and entered into force in June of the same year.
- The European Union Agency for Cybersecurity (ENISA) was tasked with establishing EU Cybersecurity Certification Scheme on Common Criteria (EUCC)*
- CC-based Security Assurance Scheme for Introducing Unified European Standards for IT Security Products
- **Smartcard** remains focused technical domain at European level

Government agencies, public institutions
(National Agency, Public CB)

Private Certification

Scope of EUCC
↓
Third-party evaluation is required.

Self Declaration

High

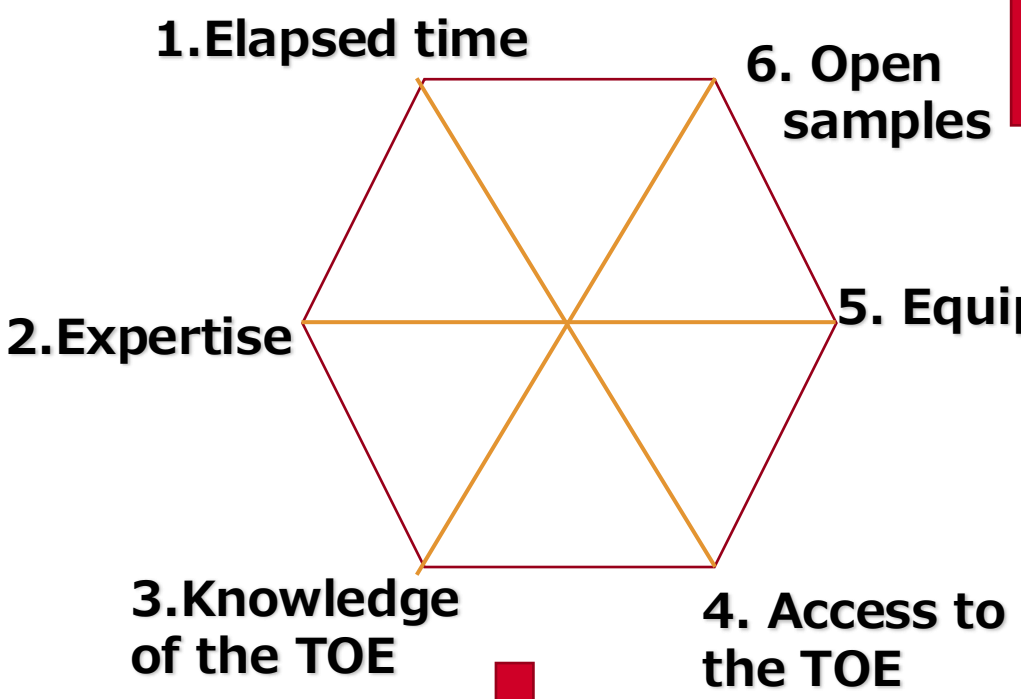
Substantial

Basic

CSA Assurance Level

- EU Cybersecurity Certification
- https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

Calculating the attack potential for smartcard evaluations in EUCC



As levels increase, countermeasures to withstand strong attackers become necessary.

Range of values	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

	CC Part3	EU CSA
	–	Basic
AVA_VAN.1	Vulnerability Survey o TOE resistance against **BASIC Attack Potential (AP)**	Substantial
AVA_VAN.2	(Unstructured) Vulnerability Analysis o TOE resistance against **BASIC AP**	
AVA_VAN.3	Focused (Unstructured) Vulnerability Analysis o TOE resistance against **ENHANCED-BASIC AP**	High
AVA_VAN.4	Methodical Vulnerability Analysis o TOE resistance against **MODERATE AP**	
AVA_VAN.5	Advanced Methodical Vulnerability Analysis o TOE resistance against **HIGH AP**	

- EU Cybersecurity Certification
- https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

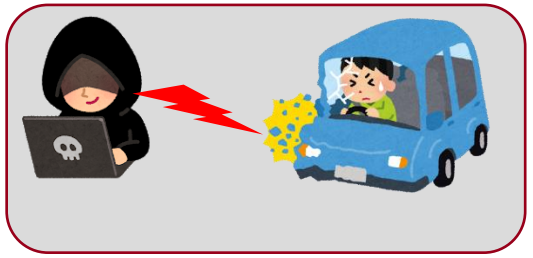
AIST
Create the Future, Collaborate Together

Background –Security of connected components–

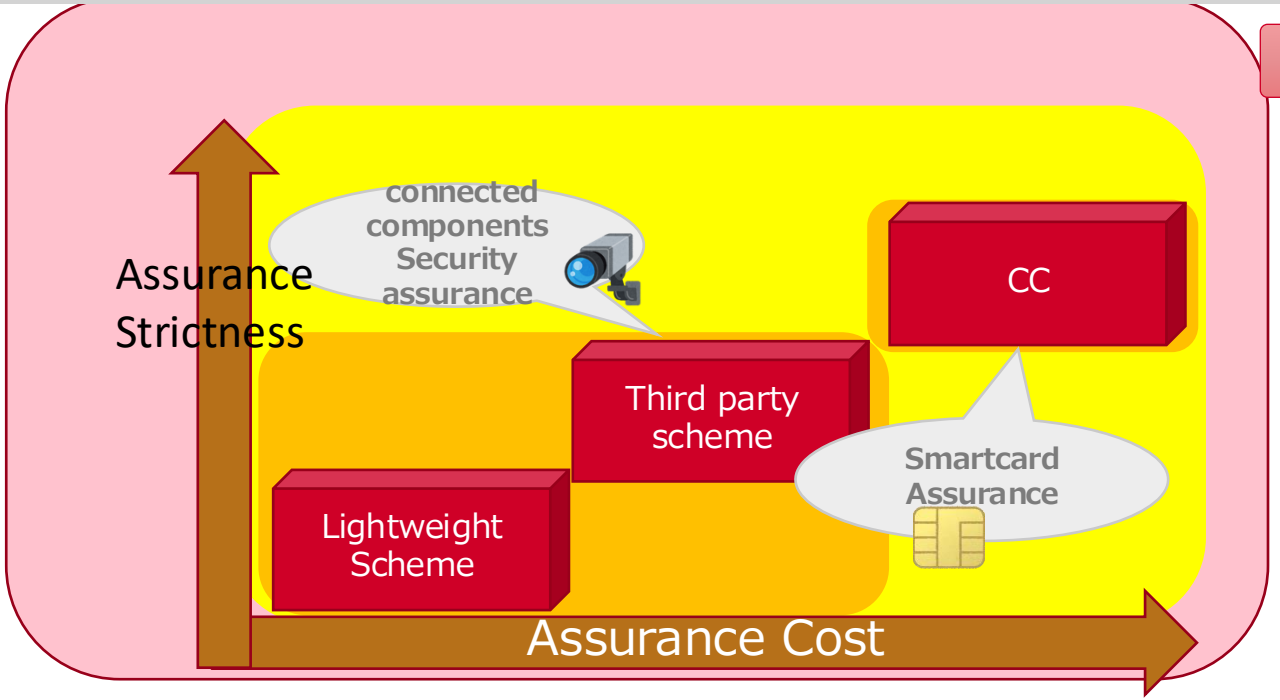
Security Assurance Schemes for Connected Components

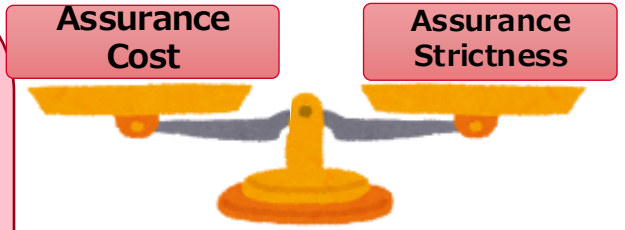
Wider range of ToE of ToE for security assurance

focus of security assurance has expanded from IC cards to connected components.



How to balance assurance cost and assurance strictness?





Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit 1.20*

- This PP specifies security requirements for a single-chip microcontroller equipped in an embedded device.
- This PP was issued in 2022.
- The core technology is **SCU** (Secure Cryptographic Unit).
- The target edge devices include sensors, actuators, and surveillance cameras.
- AVA_VAN.2 is needed
  - Balanced assurance components for cheap TOE

Common Criteria JISEC Japan Information Technology Security Evaluation and Certification Scheme

JISEC-Protection Profiles Certification | Common Criteria Portal

Protection Profile List

Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit 1.20

National Institute of Advanced Industrial Science and Technology

Last Updated 2026-02-10

Protection Profile Name : Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit

Version of PP : 1.20

Technology Type: Single Chip Microcontroller for embedded device

Certification Identification : JISEC-C0764

Date : 2022-09-30

Version of Common Criteria: 3.1 release5

Conformance Claim : EAL1 Augmented with ASE_SPD.1, ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, ALC_FLR.1, AVA_VAN.2, AVA_SCU_EXT.1

PP Identifier : None

Procurement Entity : -

Sponsor : National Institute of Advanced Industrial Science and Technology

POC : Hirotaka Yoshida

Division : Cyber Physical Security Research Center

Phone : +81-3-3599-8001

E-mail : hirotaka.yoshida@aist.go.jp

Evaluation Facility : ECSEC Laboratory Inc. Evaluation Center

Certification/Validation Report : (658 KB)(2024-09-02) CC Certificate Image : (228 KB)(2024-07-18)

Protection Profile : (1.8 MB)(2024-09-02)

PRODUCT DESCRIPTION

Description of PP

This PP specifies security requirements for a single-chip microcontroller with an SCU (Secure Cryptographic Unit) equipped in an embedded device.
The TOE conformant to this PP is a microcontroller for embedded devices that are so-called IoT edge devices such as sensors, actuators, and surveillance cameras.
The SCU consists of a cryptographic engine, a software gate allowing access to the cryptographic engine via “software gate APIs,” and a hardware gate.

https://www.ipa.go.jp/en/security/jisec/pps/certified-cert/c0764_it1797.html
https://www.commoncriteriaportal.org/pps/index.cfm

TOE with a secure cryptographic unit (SCU)

- Secure Cryptographic Unit as Root-of-Trust
  - Published in IEICE Transactions on Electronics in July 2021
  - Tsutomu MATSUMOTO, Makoto IKEDA, Makoto NAGATA, Yasuyoshi UEMURA
- Secure cryptographic unit (SCU)
  - A root of trust providing a secure public-key cryptographic capability that can be embedded in a microcontroller chip or systems on a chip (SoC)
  - The SCU is represented as a security intellectual property (IP) that realizes these hardware-level security functions
- There are several different security situations for small chips in embedded devices
  - While there are already properly managed vulnerability assessment methods in place for using smart cards
- SCU Security Platform

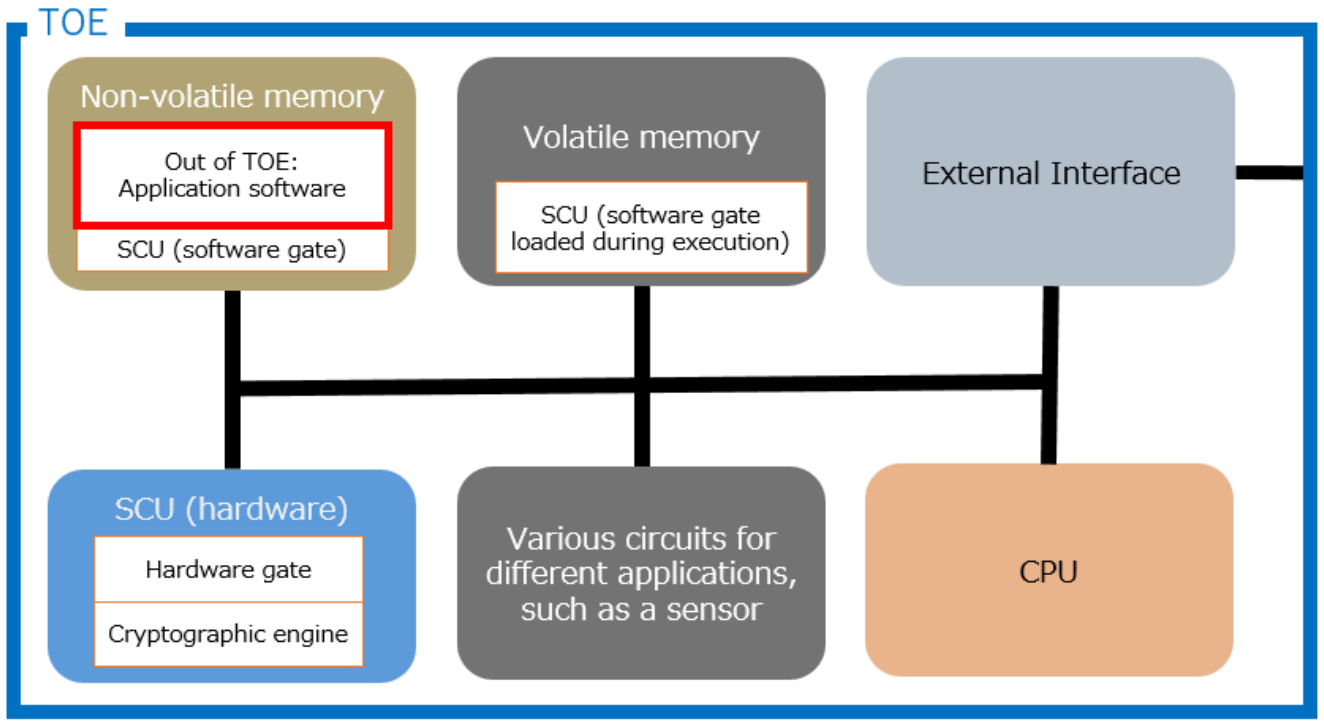


Figure 1-2 an example of TOE configuration

TOE protects following assets 'As'.

#	Notation	Asset
1	As.SCU	Integrity of security services provided for the application software.
2	As.ConfUD	Confidentiality of user data that requires confidentiality.
3	As.IntegUD	Integrity of user data that requires integrity

The very reason why our PP exists

- PPs [PP84] on secure MCUs and the SD [SDSM] (supporting document) that have been widely used exist:
  - high-value assets (financial or personal information) stored in **smart cards**.
  - TOE is resistant to attacks performed by an attacker of High attack potential, typically AVA_VAN.5
- Our PP in contrast to these existing PPs includes:
  - TOE is used for **connected components**:
    sensors, actuators, surveillance cameras.
  - Asset value handled is low.
    The use of the TOE does not assume high-value assets.
  - Attacker is a *pleasant criminal* showing off his technology
  - TOE resists attacks performed by an attacker of Basic attack potential

    TOE could be resistant to certain types of attacks performed by an attacker possessing Enhanced-Basic attack potential

Range of values	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

	CC Part3	
	AVA_VAN.1	Vulnerability Survey o TOE resistance against **BASIC Attack Potential (AP)**
Our PP (SCU PP)	AVA_VAN.2	(Unstructured) Vulnerability Analysis o TOE resistance against **BASIC AP**
Our PP (SCU PP)	AVA_VAN.3	Focused (Unstructured) Vulnerability Analysis o TOE resistance against **ENHANCED-BASIC AP**
	AVA_VAN.4	Methodical Vulnerability Analysis o TOE resistance against **MODERATE AP**
Known PP [PP84]	AVA_VAN.5	Advanced Methodical Vulnerability Analysis o TOE resistance against **HIGH AP**

[PP84] Eurosmart - Security IC Platform Protection Profile with Augmentation Packages: BSI-CC-PP-0084-2014 ver.1.0
[SDSM] JIL Application of Attack Potential to Smartcards and Similar Devices
[EUCC] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1

SESIP (Security Evaluation Standard for IoT Platforms)*

- GlobalPlatform
- Reduce cost in security certification
- Scope: HW、Library、Root of Trust、RTOS
- SESIP1 - SESIP 5
- EN 17927:2023 (MAIN) Security Evaluation Standard for IoT Platforms
- Over 28 SESIP-certified products

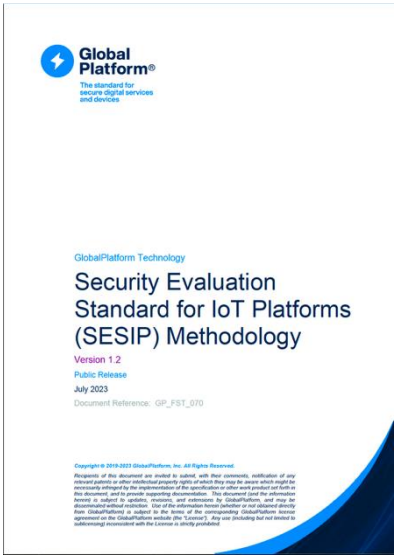
Certified chips

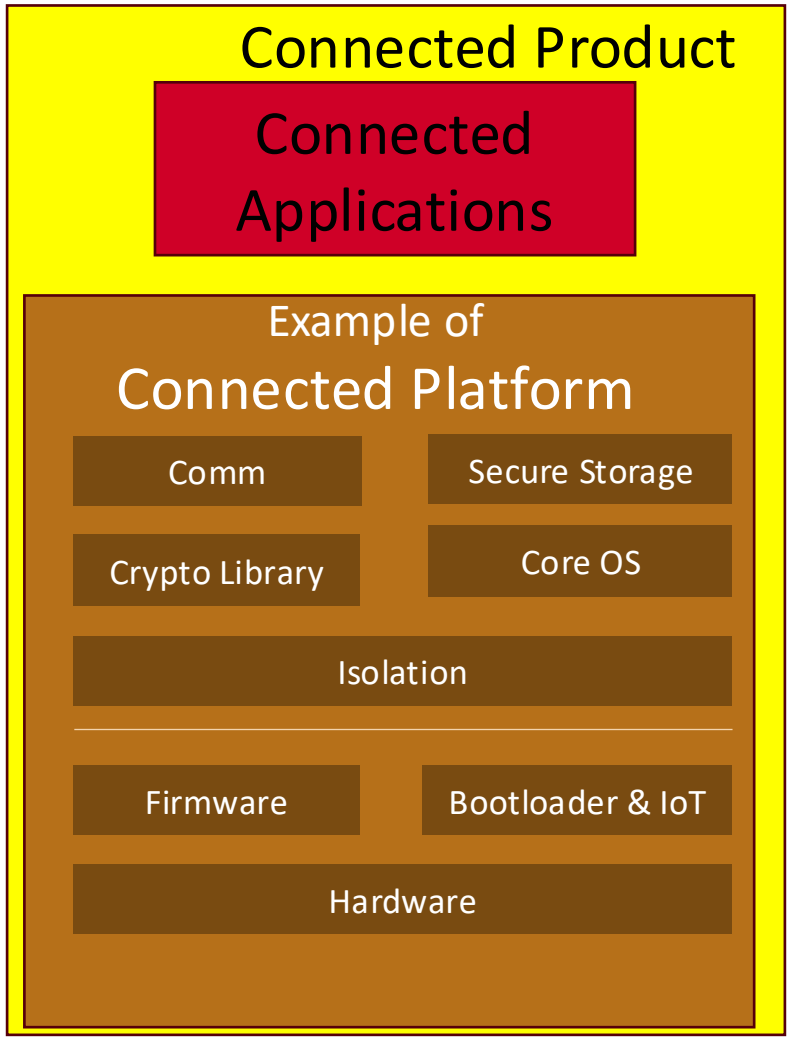
Assurance Claim	Issue Date	TOE type	Usecase	TOE Name	Package				
					Base SP	Secure Services	Software Isolation	Hardware Protection	Secure Enclave
SESIP2	2024/5/24	MCU with BLE and CAN-FD	Automotive and Industrial applications	KW45 / K32W148 / MCX W71 Product Family	✅	✅	✅		
SESIP3	2024/3/11	Wireless MCU	smart home, gaming controllers, enterprise and industrial automation, smart energy	NXP RW61x Version A1, A2	✅	✅	✅	✅	✅

* https://globalplatform.org/sesip/
** https://trustcb.com/iot/sesip/
*** EN 17927:2023 (MAIN) Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products. https://standards.iteh.ai/catalog/standards/cen/e545f156-f87b-4463-a711-9483b31a202d/en-17927

SESIP Methodology and Connected Platform

SESIP focuses on the security of Connected Products based on the Connected Platform.



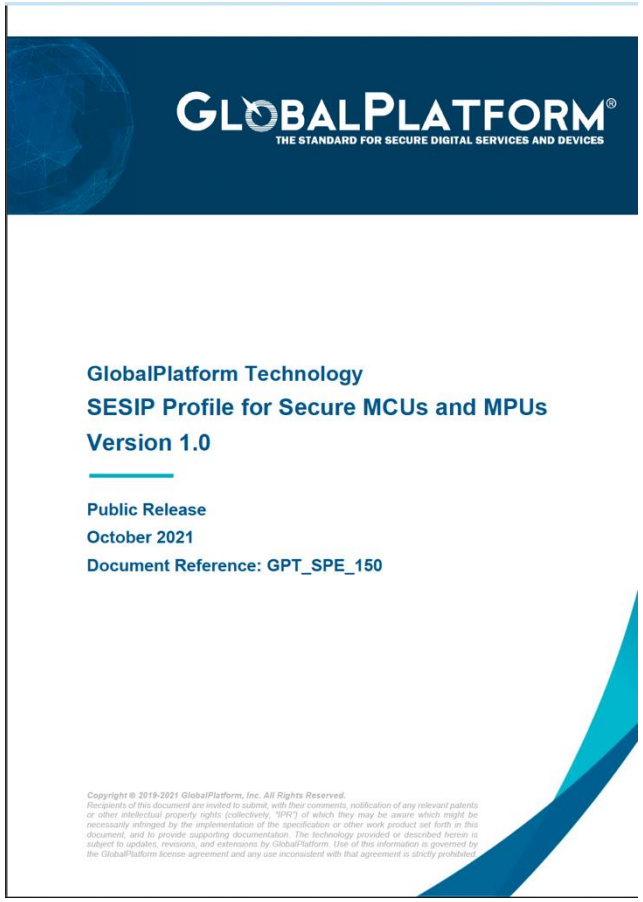


Threat Model in SESIP methodology

- **Base scenario**
  - Essential threat model, the attack phase only involves **remote access** to the platform
    This addresses a primary concern:
    scalable attacks exploiting remote connections to connected platforms.
- **Extended scenario– physical access**
  - When the platform is physically accessible to attackers
- **Extended scenario- untrusted software**
  - When untrusted software is loaded onto the platform by an attacker,
    → it may affect the platform, its components, or its applications.

SESIP Profile Secure MCU/MPU

User-friendly writing style. Easy to read.
Specific purpose, highly concrete, but with lower versatility and flexibility.

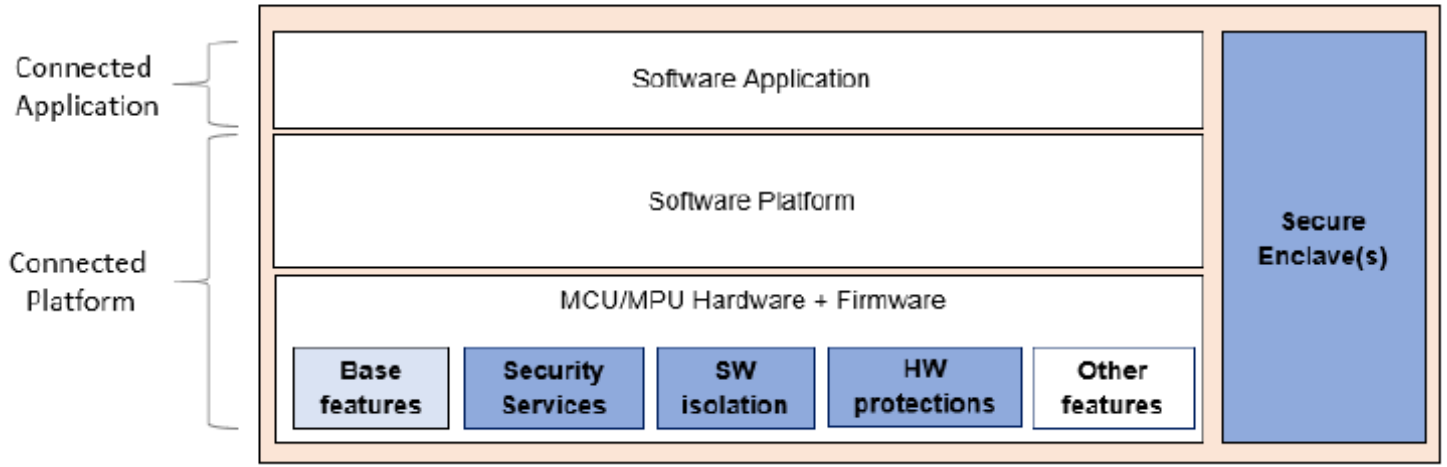


1. Introduction
2. SESIP Profile Introduction
3. Security Objectives for the Operational Environment
4. Security Requirements and Implementation
5. Mapping and Sufficiency Rationales

Annex. A. Relation of Assurance Levels and Relevant to this SESIP Profile (Informative)

Annex. B. Clarification on the Use Cases Relevant to Attack Rating (Informative)

Figure 2-1: TOE Scope Representation Example



https://globalplatform.org/wp-content/uploads/2024/09/GPT_SESIP_Profile_Secure_MCU_MPU_v1.0.0.4_PublicRvw.pdf

Base SP Security Functional Requirements

AIST
Create the Future, Collaborate Together

As a base, the platform fulfills the following Security Functional Requirements:

#	Names	Requirement
1	**Verification of Platform Identity**	The platform **provides a unique identification of itself**, including all its parts and their versions.
2	**Secure Initialization of Platform**	The platform **ensures its authenticity and integrity during platform initialization**. If platform authenticity or integrity cannot be ensured, the platform will go to <list of controlled states>.
3	**Secure Update of Platform**	The platform **can be updated to a newer version** in the field such that the integrity, authenticity, and confidentiality of the platform is maintained.
4	**Residual Information Purging**	The platform **ensures that <list of data>,** with the exception of <list of exceptions of data that is not erased automatically**>, is erased** using the method specified in <specification> **before the memory is (re)used** by the platform or application again and before an attacker can access it.
5	**Secure Debugging**	The platform **only provides <list of endpoints> authenticated** as specified in <specification> **with debug functionality**. The platform ensures that all data stored by the application, with the exception of <exceptions>, is made unavailable.

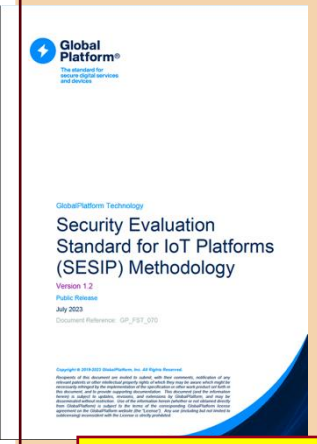
Harmonization to EUCC

To reuse SESIP certificate

GlobalPlatform

TRUSTCB

Consistent



規格文書SESIP

SESIP3

SESIP2

SESIP1

Europe

EUCC

CSA

AVA_VAN.5

AVA_VAN.4

AVA_VAN.3

AVA_VAN.2

AVA_VAN.1

High

Substantial

Basic

National Agencies

Private Certification

Self Declaration

TRUSTCB

SESIP

SESIP2

Reuse

A社 EUCC

AVA_VAN2

EUCC Cert.(Substantial)

Conclusion

- Introduction to Security assurance, HW security, security of connected components
- CC certified protection profile
- SESIP profile
  - SESIP Methodology
  - SESIP Profile Secure MCU/MPU