Certification Report

TOMITA Tatsuo, Chairman
Information-technology Promotion Agency, Japan
2-28-8 Honkomagome, Bunkyo-ku, Tokyo

Protection Profile (PP)

Reception Date of Application (Reception Number)	2021-10-12 (ITC-1797)
Certification Identification	JISEC-C0764
PP Name	Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit
Version and Release Numbers	1.20
PP Manufacturer	National Institute of Advanced Industrial Science and Technology (AIST)
Conformance of Functionality	CC Part 2 Extended
Protection Profile Conformance	None
Assurance Package	EAL1 augmented with ASE_SPD.1, ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, ALC_FLR.1, AVA_VAN.2, and AVA_SCU_EXT.1
Name of IT Security Evaluation Facility	ECSEC Laboratory Inc., Evaluation Center

This is to report that the evaluation result for the above PP has been certified as follows.
2022-09-30

SATO Shinji, Technical Manager
IT Security Technology Evaluation Department
IT Security Center

Evaluation Criteria, etc.: This PP is evaluated in accordance with the following standards prescribed in the "IT Security Evaluation and Certification Scheme Document."

- Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
- Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

Evaluation Result: Pass

"Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit" has been evaluated based on the standards required, in accordance with the provisions of the "Requirements for IT Security Certification" by Information-technology Promotion Agency, Japan, and has met the specified assurance requirements.

Notice:
This document is the English translation version of the Certification Report published by the Certification Body of Japan Information Technology Security Evaluation and Certification Scheme.

Table of Contents

1 Executive Summary

This Certification Report describes the content of the certification result in relation to IT Security Evaluation of "Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit, Version 1.20" (hereinafter referred to as the "PP[12]") developed by National Institute of Advanced Industrial Science and Technology (AIST), and the evaluation of the TOE was completed on 2022-06-17 by ECSEC Laboratory Inc., Evaluation Center (hereinafter referred to as the "Evaluation Facility"). It is intended to report to the sponsor, National Institute of Advanced Industrial Science and Technology (AIST), and provide security information to procurement entities and consumers who are interested in this PP[12].

Readers of the Certification Report are advised to read the corresponding PP[12]. Especially, details of security functional requirements, assurance requirements and rationale for sufficiency of these requirements of the PP[12] are described in the PP[12].

This Certification Report assumes "developers who develop the product conformant to the PP[12] and procurers" to be readers. Note that the Certification Report presents the certification result based on assurance requirements to which the PP[12] conforms, and does not guarantee an individual IT product itself.

1.1 Evaluated PP

An overview of the security functions required in PP[12] is described below. Refer to Chapter 2 and subsequent chapters for details.

1.1.1 Assurance Package

Assurance Package required by the PP[12] is EAL1 augmented with ASE_SPD.1, ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, ALC_FLR.1, AVA_VAN.2, and AVA_SCU_EXT.1.

In addition, the PP and ST that claim conformance to the PP[12] shall claim strict conformance.

1.1.2 PP Overview

The PP[12] specifies the security requirements of a single chip microcontroller (called Microcontroller) for embedded equipment. The Microcontroller is equipped with a secure cryptographic unit (SCU) that provides security features.

A Single Chip Microcontroller equipped with an SCU is the TOE of the PP[12]. Figure 1-1 shows a conceptual diagram of the SCU. The SCU consists of a cryptographic engine, and

software and hardware gates that can access the cryptographic engine via “software gate APIs”. The assumed TOE is a built-in memory type in a single-chip microcontroller. An external memory type is outside the scope of this Certification Report.

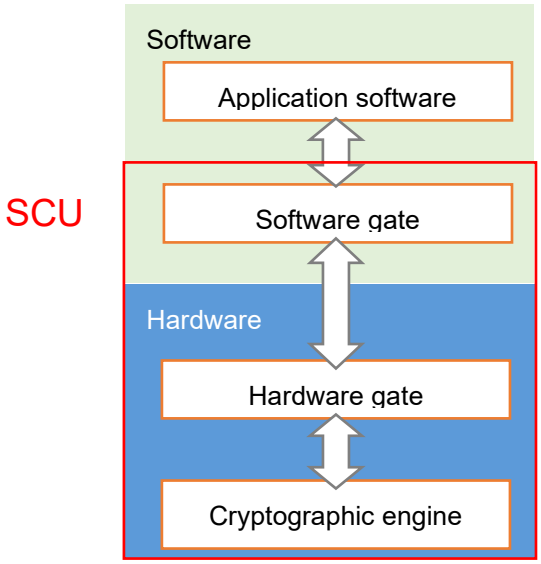

Figure 1-1 Conceptual diagram of the SCU

The TOE is generally distributed in the form of a SoC. In the case of the TOE with built-in memory, it is packaged by mounting it on a single die. This SoC is soldered on a board on which various circuits necessary for embedded device applications are mounted, and the board is placed in the housing of the embedded device.

Figure 1-2 shows an example of the TOE configuration. The blue line shows the physical boundary of the TOE and the configuration of a typical microcontroller equipped with an SCU. The red line shows the logical boundary of the TOE. In Figure 1-2, the application software is logically located outside the TOE and uses cryptographic functions through the software and hardware gates. The application software is stored in non-volatile memory of the TOE.

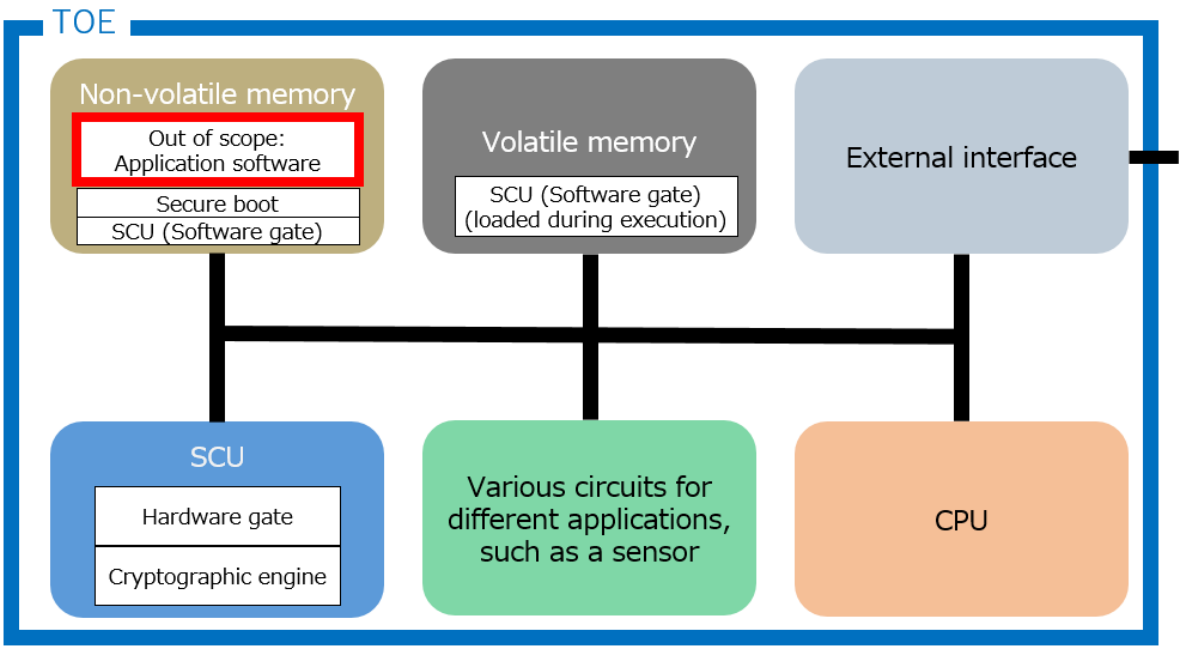

Figure 1-2 TOE configuration example

The software and hardware gates are mechanisms for controlling access to the cryptographic functions, and they correspond to software and hardware components of the access control function. Access to the cryptographic functions by the application software is legitimate and should be permitted, but access by others must be denied. The TOE access control mechanism is implemented to distinguish between these accesses.

The software and hardware gates operate as follows.

Each time the hardware gate receives cryptographic command data directed at it, it transitions its internal state. This is uniquely determined by the previous internal state and the current input (cryptographic command data). If the hardware gate knows the correct transition data of the internal state, it can compare the result of the transition by the current input with the correct transition data to determine whether the input command data is legitimate.

The software gates provide information to manage the state transitions of the hardware gates. All patterns of access to the cryptographic functions, which are unique and predicted in advance by the developer, are known only to the developer. The internal state transitions of the hardware gate associated with these access patterns are calculated in advance and stored in the software gate. When the software gate receives the access command data to the cryptographic function from the application software, it transfers both the access command data and the next internal state transition data of the hardware gate to the hardware gate. The hardware gate checks the internal state transition data passed to it against the internal state transition results from the command data received at the same time, and if

the two match, it determines that the received command data is legitimate. Software gates, which contain internal state transition data to be passed to hardware gates, are stored in non-volatile memory in the TOE at the time of TOE manufacturing and cannot be generated except by developers. In other words, the access pattern to the cryptographic function calculated in advance by the developer will be executed, but if an emulator or other device tries to use the cryptographic function with any other pattern, it will not be able to provide the encrypted internal state transition data and the hardware gate will deny access. If the internal state transition data embedded in the software gate in advance is to be cryptographically protected, the implementing algorithm is chosen from Chapter 7 of the PP[12].

The SCU has a self-protection function to protect its own security function. The TOE stores the HGK, which is the RoT, and information that uniquely identifies the TOE to external entities in the TOE. It is the responsibility of the TOE developer to generate a random number HGK with sufficient entropy.

The TOE protects confidentiality of TSF data by the self-protection function of the hardware. The TOE protects user data that exists in non-volatile memory by the cryptographic function of the TOE. TSF data are an HGK, a key for decrypting user keys in the key storage, data for verification of the integrity of the key storage, data for verification of the integrity of the software gate, an IV, internal state transition data, and a chip ID.

The TOE's secure boot program extracts the software gate and application software into RAM at startup, verifies the integrity of the software gate, and verifies the integrity (and optionally the authenticity) of the application software. The TOE also verifies the integrity and authenticity of the application software when updating it, and updates it after successful verification. Here, authenticity refers to the property that the application software was developed by a legitimate application software developer.

1.1.3 Overview of Security Functions

The PP[12] requires the TOE to provide the following functions:

The TOE provides SCU's cryptographic functions for the application software via the software gate. The application software implements security functions such as communication protocol, memory encryption, and identification/authentication using the cryptographic functions. The TOE also implements the cryptographic and self-protection functions that protect the security functions.

The main security functions provided by the TOE are as follows. These functions are baseline requirements, hence TOE’s mandatory requirements.

- Monitoring access to the cryptographic function: The ability to detect and respond to unauthorized use of the cryptographic function by an attacker through the cooperative operation of the software and hardware gates.
- Self-protection function: The ability to prevent unintentional leakage of information to radiated electromagnetic waves and power consumption during SCU operation, exposing useful information to an attacker, and the ability to detect and respond to physical attacks.
- Secure boot function: The ability to verify the integrity of the software gate and the application software during startup.
- Store keys: The ability to store keys in the non-volatile memory of the TOE whose confidentiality and integrity are protected by cryptography.
- Import user keys: The ability to import key storage containing user keys and secret information from external entities to the TOE while protecting confidentiality.
- Update function: The ability to update after verifying the authenticity and integrity of the application software while obtaining the correct application software version and preventing rollback.

The cryptographic functions for achieving the baseline functions of the TOE are as follows. The ST author selects the required SFR from the PP[12] Chapter 7.

- Encryption/Decryption: To protect confidentiality, a plaintext is encrypted into a cipher text and a cipher text is decrypted into a plaintext.
- Digital signature verification: Verifying the digital signature for authenticity and integrity verification.
- Calculation of hash value: Cryptographic hash functions calculate hash values.
- MAC generation and verification: Attaching a MAC and verifying the integrity of data with the MAC.
- Random bit generation: The TOE generates a random bit and provides it for the application software.
- Using salt, nonce and generating IV: Appropriate use of salts and nonces required for cryptographic functions and generating IVs.
- Deriving keys: It derives keys.
- Encrypt key: It encrypts the keys using KEKs.

The cryptographic functions provided by the TOE to the application software via the software gate are as follows. These functions are optional features, and the ST author selects the necessary SFRs from the PP[12] Chapter 8.

- Key generation: Keys suitable for the cryptographic algorithm are generated by the random bit generator (RBG) of the TOE.
- Destruction of keys and key materials: Making the key and key materials in volatile memory unrecoverable. Note that the keys stored in the key storage of non-volatile memory are encrypted and are not expected to be destroyed.
- Digital signature generation: Generating a digital signature for the protection of authenticity and integrity.

The life cycle of the TOE is divided into seven phases as described in Figure 1-3. The TOE developer shall secure the process from TOE development in Phase 1 to TOE manufacturing in Phase 4, and the delivery of the TOE to embedded device developers in Phase 6. The TOE developer or key installation providers must also secure the importing user key in Phase 5.

The environment for application software development in Phase 3, embedded device manufacturing in Phase 6, and distribution to end consumers in Phase 7 are outside the scope of this PP[12], but it is assumed that the embedded device developer who purchased the TOE will take responsibility for maintaining the development environment security.

Phase 1: Developing hardware

Development of the TOE. The TOE developer purchases an IP of the SCU or develops the SCU and constructs the hardware TOE together with components such as a CPU.

Phase 2: Purchasing software or developing program

The TOE developer purchases the software gate for secure use of the cryptographic engine from the SCU IP vendor or develops their own software gate. The TOE developer purchases a secure boot program from the SCU IP vendor or develops their own secure boot program.

Phase 3: Developing the application software

The embedded device developer develops the application software for embedded devices. When requesting the TOE manufacturer to install the application software, the embedded device developer sends the application software to the TOE developer. If the embedded device developer installs the application software, it will be installed in Phase 6.

Phase 4: Manufacturing the TOE

The TOE developer manufactures the TOE, writes the HGK, and installs the secure boot and software gate into the non-volatile memory of the TOE. If requested by the embedded device developer, the TOE developer receives the application software developed by the embedded device developer in Phase 3 and loads it into the non-volatile memory of the TOE. Note that the application software may be mounted on the TOE in Phase 6 instead of this phase. The manufactured TOE becomes a product after a developer test.

Phase 5: Importing the user keys

The TOE developer generates key storage. The TOE developer receives the user key and secret information used by the application software from the embedded device developer and stores them in key storage, and the entire key storage is encrypted and assigned a MAC. The TOE writes the key storage to the TOE's non-volatile memory via a software gate. This key import may be performed by the TOE developer or may be outsourced to a key installation provider. In any case, it is necessary that key delivery and importing are performed in a secure environment. After writing the key, the TOE will be distributed from Phase 5 to Phase 6.

Phase 6: Manufacturing the embedded device

The embedded device developer manufactures the embedded device and mounts the TOE on the embedded device. In a number of cases, the embedded device developer installs the application software into the TOE. This development process may be divided into the development of a board on which the TOE is mounted and that of the embedded device on which it is mounted. The TOE in this process is assumed to be handled under a secure environment. The completed embedded device is distributed to the end consumer.

Phase 7: Operating by end consumers

The final phase of the TOE life cycle. It is used under the assumed operating environment with the TOE installed in the embedded device. The threats assumed by PP[12] occur during this operation phase.

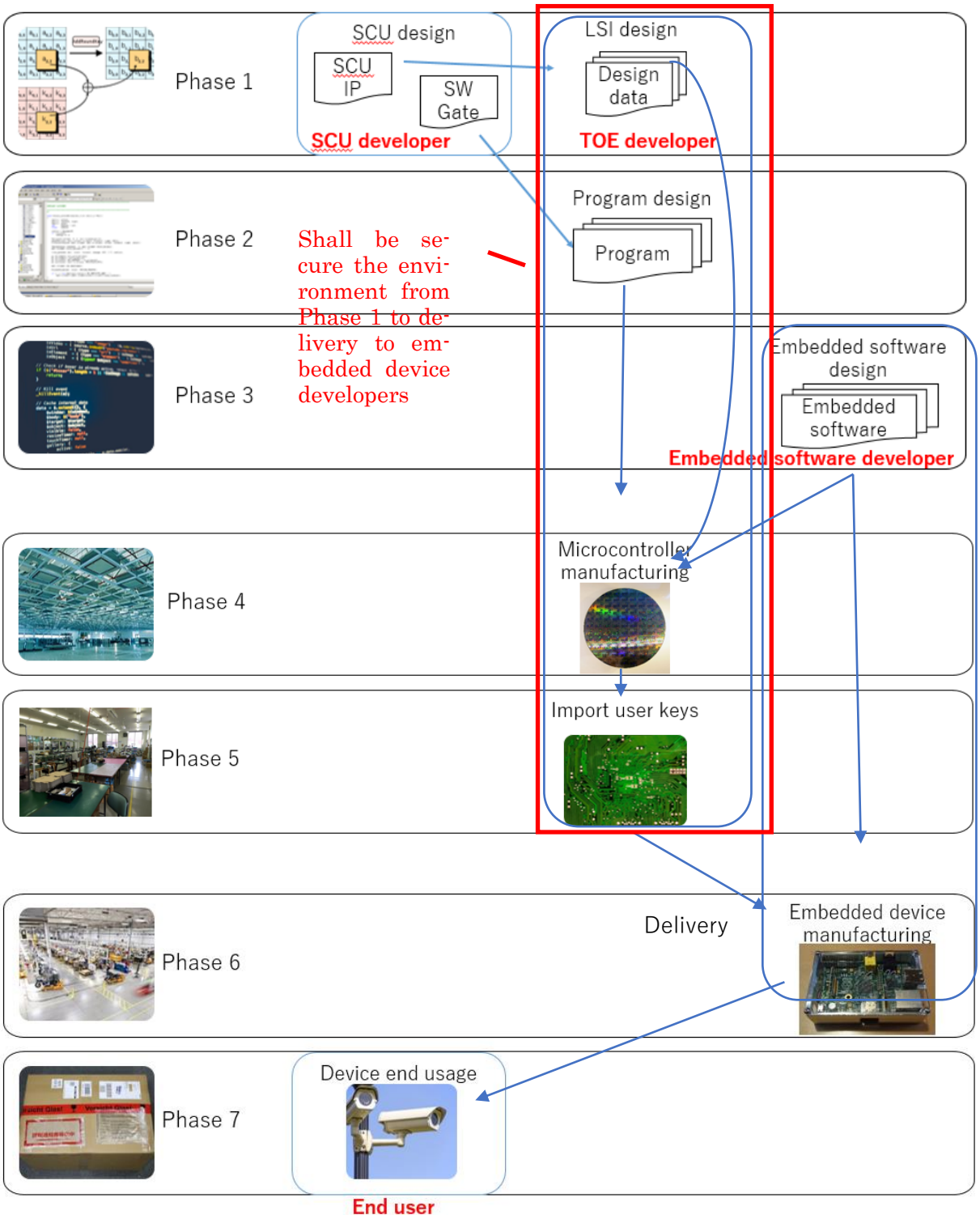

Figure 1-3 Life cycle of the TOE

The TOE provides key storage services and keeps cryptographic keys used by the cryptographic engine confidential and secure by encrypting them. The integrity of a key is protected by a MAC. As an example, when the user key used in the hardware gate is held in key storage, the following processing is performed. First, at the TOE developer's factory or

outsourced key installation provider in Phase 5, the KEK and MAC keys are derived from the HGK written inside the SCU. Next, the key storage (which contains user keys and other data) used in the TOE is encrypted using KEK, and a MAC is assigned to the encrypted key storage using the MAC key. In this way, the key storage is written in the non-volatile memory in the TOE but out of the SCU in a state of being encrypted and also attached with a MAC.

The TOE has a data object (protected storage) created by the manufacturer at the time of manufacturing, and the TOE developer stores the HGK in that data object. For example, the TOE developer generates an HGK with an RBG outside the TOE and embeds it in the TOE during the manufacturing process. The HGK guarantees the integrity of the TSF and is the starting point for permissions to other data objects. Since the HGK must be protected, the TOE needs a self-protection function.

1.1.4 Disclaimers

None.

1.2 Conduct of Evaluation

Under the IT Security Evaluation and Certification Scheme that the Certification Body operates, the Evaluation Facility conducted IT security evaluation and completed in 2022-06, based on functional requirements and assurance requirements of the PP[12] according to the publicised documents "IT Security Evaluation and Certification Scheme Document"[1], "Requirements for IT Security Certification"[2], and "Requirements for Approval of IT Security Evaluation Facility"[3] provided by the Certification Body.

1.3 Certification

The Certification Body verified the Evaluation Technical Report[13] and the Observation Report[14] prepared by the Evaluation Facility as well as evaluation documentation, and confirmed that the PP[12] evaluation was conducted in accordance with the prescribed procedure.

The certification oversight reviews were also prepared for those concerns found in the certification process.

The Certification Body confirmed that all the concerns pointed out by the Certification Body were fully resolved, and that the PP[12] evaluation had been appropriately conducted in accordance with the CC ([4][5][6] or [7][8][9]) and the CEM (either of [10][11]).

The Certification Body prepared this Certification Report based on the Evaluation Technical Report and fully concluded certification activities.

2 Identification

The PP is identified as follows:

PP Name:	Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit
PP Version:	1.20
Developer:	National Institute of Advanced Industrial Science and Technology (AIST)

3 Security Policy

This chapter describes security function policies adopted by the TOE conforming to the PP[12] to counter threats.

3.1 Security Function Policies

The PP[12] specifies security functions to counter the threats shown in Section 3.1.1.1 and to satisfy the organisational security policies shown in Section 3.1.2.1.

3.1.1 Threats and Security Function Policies

3.1.1.1 Threats

The PP[12] presumes the threats shown in Table 3-1 and requires the TOE to provide security functions to counter them.

Table 3-1 Threats

Identifier	Threat
T.Internal_Access	An attacker may attempt to tamper with the application software or the software gate and then use the TOE's cryptographic functions without permission to disclose or modify the user data.
T.Weak_Import	An attacker may abuse the key storage import function to disclose or tamper with user data.
T.Unauthorized_Update	An attacker may install unauthorized application software on the TOE to expose user data of the embedded device or disrupt the device's services. Alternatively, an attacker may illegally roll back to a version with a security failure to disclose the user data of the embedded device or disrupt embedded device services.
T.Weak_Crypto	An attacker may disclose or alter the user data by exploiting improperly selected encryption algorithms, key generation method, key lengths, key destruction method, or an RBG.
T.Leak_Inherent	An attacker may expose the user or TSF data like cryptographic keys, by observing and analyzing changes in the TOE's power consumption during cryptographic operations.
T.Phys_Probing	By physically probing the inside of the TOE, an attacker

	may expose or modify the user data of the TOE like cryptographic keys, or other TSF data that is useful for other attacks.
T.Phys_Manipulation	An attacker may modify the user data and encryption keys stored in the cryptographic function by physically manipulating the inside of the cryptographic function or modify the security mechanism of the TOE for other attacks.

3.1.1.2 Security Function Policies against Threats

The TOE conforming to the PP[12] counters the threats described in Table 3-1 by the following security functions.

(1) Countering the threat T. Internal_Access

Following SFRs prevent modified application software or modified software gate from accessing the hardware inside the TOE to use the TOE's cryptographic functions.

- FDP_IFC.1/API, FDP_IFF.1/API specifies requirements for operating cryptographic functions by the application software that is an external entity. Only when the state transition of data of the software gate is verified, data is output from the cryptographic function to the external entity. That is, only the correct use of the cryptographic function is accepted.
- FDP_MFW_EXT.1 is called by FPT_TST.1 to verify the integrity and, if needed, authenticity of the application software at startup.
- FPT_TST.1 defines the integrity verification of the software gate at startup and supports the validation of the state transition data of the software gate by FDP_IFC.1/API and FDP_IFF.1/API.
- FPT_FLS.1/SG maintains a secure state even if the integrity of the state transition of data of the software gate is compromised.
- FPT_FLS.1/SB maintains a secure state even if the integrity of the software gate and application software and, if needed, authenticity of the application software is compromised at startup.

(2) Countering the threat T. Weak_Import

According to the following SFRs, importing of the key storage with encrypted integrity verification data attached and integrity verification are performed to prevent the import of unauthorized user data.

- FDP_IFC.1/Import, FDP_IFF.1/Import specifies the requirements for operating the import functions by the application software that is an external entity. Only when the state transition of data of the software gate is verified can the user data be stored in the key storage via the import function. That is, only the correct use of the import function is accepted.
- FDP_UIT.1 verifies the integrity of user data to be imported into key storage.

(3) Countering the threat T.Unauthorized_Update

According to the following SFRs, the TSF obtains the correct version of the application software, updates the application software, and verifies the updated application software.

- FPT_TUD_EXT.1 queries the application software for its “current version”, triggers the update, and verifies the updated application software before installation.
- FPT_RPL.1 prevents rollback attempts.
- FPT_FLS.1/UD preserves a secure state when an integrity or authenticity error of the application software occurs.

(4) Countering the threat T.Weak_Crypto

The TOE counters this threat by implementing an RBG with a sufficient entropy source and cryptographic algorithms with sufficient key length on the basis of an approved standard, and providing it to the application software, as defined in the following SFRs.

- (Option) FCS_CKM.1/AK generates asymmetric keys.
- (Option) FCS_CKM.1/SK generates symmetric keys.
- (Option) FCS_CKM.4 ensures that keys and key materials in the volatile memory are destroyed in such a way as to prevent future recovery.
- (Selection) FCS_COP.1/SKC encrypts and decrypts using symmetric key algorithms.
- (Selection) FCS_COP.1/KeyEnc performs key encryption and decryption.
- (Selection) FCS_COP.1/Hash uses hashing mechanisms.
- (Selection) FCS_COP.1/MAC calculates MAC.
- (Option) FCS_COP.1/SigGen generates digital signatures.
- (Selection) FCS_COP.1/SigVer verifies digital signatures.

- (Selection) FCS_KDF_EXT.1 performs key derivation.
- (Selection) FCS_RBG_EXT.1 performs random bit generation.
- (Selection) FCS_SNI_EXT.1 ensures that the salt, nonce, and initialization vector used by the TOE do not adversely affect key strength.

(5) Countering the threat T.Leak_Inherent

It mitigates leakage of unnecessary information to radiated electromagnetic waves and power consumption when SCU processes user and TSF data, making it difficult for attackers to expose useful data by performing statistical processing.

- FPT_EMS_EXT.1 mitigates the leakage of user data and TSF data from the TOE.

(6) Countering the threat T.Phys_Probing

The following SFRs are to counter this threat of modifying or acquiring the user data by using equipment used for semiconductor analysis to photograph a memory cell or physically contact the inside of the TOE.

- FPT_PHP.3 counters physical probing.
- FCS_STG_EXT.1 implements key storage outside the SCU.
- FCS_STG_EXT.2 uses cryptography to ensure confidentiality of the key storage outside the SCU.
- FCS_STG_EXT.3 uses cryptography to ensure integrity of the key storage outside the SCU.

(7) Countering the threat T.Phys_Manipulation

The following SFRs are aimed at countering this threat that directly alters information assets or uses them as a stepping-stone for other attacks by conducting physical operations inside the TOE.

- FPT_PHP.3 counters physical tampering.
- FCS_STG_EXT.1 maintains key storage outside the SCU.
- FCS_STG_EXT.2 uses cryptography to ensure confidentiality of the key storage outside the SCU.
- FCS_STG_EXT.3 uses cryptography to ensure integrity of the key storage outside the SCU.

3.1.2 Organisational Security Policies and Security Function Policies

3.1.2.1 Organisational Security Policies

There is no organisational security policy.

3.1.2.2 Security Function Policies to Organisational Security Policies

As there is no organisational security policy, there is no security function for organisational security policies.

4 Assumptions and Clarification of Scope

This chapter describes the assumptions and the operational environment for the operation of the TOE conforming to the PP[12].

4.1 Usage Assumptions

Table 4-1 shows assumptions to operate the TOE conforming to the PP[12]. The effective performances of the security functions of the TOE conforming to the PP[12] are not assured unless these assumptions are satisfied.

Table 4-1 Assumptions

Identifier	Assumptions
A.Trusted_User	The embedded device developer appropriately protects data stored outside the TOE.

5 Evaluation conducted by Evaluation Facility and Results

5.1 Evaluation Facility

ECSEC Laboratory Inc. Evaluation Center that conducted the evaluation as the Evaluation Facility is approved under JISEC and is accredited by NITE (National Institute of Technology and Evaluation), the Accreditation Body, which joins Mutual Recognition Arrangement of ILAC (International Laboratory Accreditation Cooperation). It is periodically confirmed that the above Evaluation Facility meets the requirements on the appropriateness of the management and evaluators for maintaining the quality of evaluation.

5.2 Evaluation Approach

Evaluation was conducted by using the evaluation methods prescribed in the CEM in accordance with the assurance requirements in the CC Part 3. Details for evaluation activities were reported in the Evaluation Technical Report[13].

The Evaluation Technical Report[13] explains the summary of the PP[12] as well as the content of the evaluation and the verdict of each work unit in the CEM.

5.3 Overview of Evaluation Activity

The history of the evaluation conducted is described in the Evaluation Technical Report[13] as follows.

The evaluation started in 2021-10 and concluded upon completion of the Evaluation Technical Report dated 2022-06. The Evaluation Facility received a full set of evaluation deliverables necessary for evaluation provided by the developer, and examined the evidence in relation to a series of evaluations conducted.

Concerns found in evaluation activities were issued as the Observation Report[14], and reported to the developer.

The concerns were reviewed by the developer, and all of them were solved eventually.

Concerns in the evaluation process that the Certification Body found were described as the certification oversight reviews, and sent to the Evaluation Facility. The Evaluation Facility and the developer examined them, which was reflected in the Evaluation Technical Report[13].

5.4 Evaluation Results

The evaluators had concluded that the PP[12] satisfies all work units prescribed in the CEM as per the Evaluation Technical Report[13].

In the evaluation, the following were confirmed.

- Security functional requirements: Common Criteria Part 2 Extended
- Security assurance requirements: Common Criteria Part 3 Extended

As a result of the evaluation, the verdict "PASS" was confirmed for the following assurance components:

APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1

5.5 Evaluator Comments/Recommendations

There is no evaluator recommendation to be addressed to procurers.

6 Certification

Based on the documentation submitted by the Evaluation Facility during the evaluation process, the Certification Body has performed certification from the following perspectives:

1. Contents pointed out in the Observation Report[14] shall be adequate.

2. Contents pointed out in the Observation Report[14] shall properly be solved.

3. The submitted documentation was examined, and the related work units shall be evaluated as presented in the Evaluation Technical Report[13].

4.Rationale of the evaluation verdict by the evaluator presented in the Evaluation Technical Report[13] shall be adequate.

5. The evaluator's evaluation methodology presented in the Evaluation Technical Report[13] shall conform to the CEM.

Concerns found in the certification process were prepared as the certification oversight reviews, and they were sent to the Evaluation Facility. The Certification Body confirmed such concerns pointed out in the certification oversight reviews were solved in the PP[12] and the Evaluation Technical Report[13] and issued this Certification Report.

6.1 Certification Result

As a result of verification of the Evaluation Technical Report[13], Observation Report[14] and related evaluation documentation submitted by the Evaluation Facility, the Certification Body determined that the PP[12] satisfies all assurance requirements APE_INT.1, APE_CCL.1, APE_SPD.1, APE_OBJ.1, APE_ECD.1 and APE_REQ.1 in the CC Part 3.

6.2 Recommendations

The validity of the cryptographic algorithms is not assured at the time of the TOE evaluation conforming to the PP[12]. Therefore, it is necessary to confirm that each cryptographic algorithm specified in the PP[12] is still valid and not compromised yet.

7 Annexes

There is no annex.

8 Glossary

The abbreviations relating to the CC used in this report are listed below.

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

The abbreviations relating to the PP used in this report are listed below.

API	Application Program Interface, an interface between different parts of a computer program intended to simplify the implementation and maintenance of software.
Application software	From the viewpoint of the TOE, application software is user data and uses the encryption service of the SCU via the software gate API.
CPU	Central Processing Unit
External entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.
Hardware gate	A hardware part of an access control mechanism for a cryptographic function that accesses a cryptographic engine.
HGK	Hardware Gate Key
IP	Intellectual Property, a semiconductor intellectual property
IT	Information Technology
IV	Initialization Vector
KDF	Key Derivation Functions
KEK	Key Encryption Key
Key storage	Data object that stores user keys and secret information
MAC	Message Authentication Code
OTP	One Time Programmable
Protected storage	A special storage for storing the hardware gate key. It may be an OTP area where the HGK is written by a semiconductor test process, or it may be hard coded to be a part of a circuit.
RBG	Random Bit Generator
RoT	Root of Trust
SCU	Secure Cryptographic Unit
SoC	System on a Chip. The design method or the chip itself fabricated by

	the method that integrates many or all function components into a semiconductor chip necessary for the operation of a certain system.
User Keys	Keys used by the application software, encrypted by the key encryption key, and data for integrity check is attached.

9 Bibliography

[1] IT Security Evaluation and Certification Scheme Document, October 2020, Information-technology Promotion Agency, Japan, CCS-01

[2] Requirements for IT Security Certification, October 2020, Information-technology Promotion Agency, Japan, CCM-02

[3] Requirements for Approval of IT Security Evaluation Facility, October 2021, Information-technology Promotion Agency, Japan, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001, (Japanese Version 1.0, July 2017)

[8] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002, (Japanese Version 1.0, July 2017)

[9] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003, (Japanese Version 1.0, July 2017)

[10] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] Common Methodology for Information Technology Security Evaluation: Evaluation methodology, Version 3.1 Revision 5, April 2017, CCMB-2017-04-004, (Japanese Version 1.0, July 2017)

[12] Protection Profile for Single Chip Microcontroller equipped with a secure cryptographic unit, Version 1.20, (June 15, 2022), National Institute of Advanced Industrial Science and Technology (AIST)

[13] Protection Profile Evaluation Technical Report SCV21-ETRPP-0001-03, Version 1.3, June 17, 2022, ECSEC Laboratory Inc., Evaluation Center

[14] Observation report SCV21-EOR-7001-00, (November 26, 2021), ECSEC Laboratory Inc. Evaluation Center