AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U)

Module Version: bc0c0140FIPS001

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.3

Last update: 2023-07-21

Prepared for:
Advanced Micro Devices (AMD)
2485 Augustine Drive
Santa Clara, CA 95054
www.amd.com

Prepared by:
atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
www.atsec.com

Table of Contents

List of Tables

List of Figures

0. Introduction

0.1. Overview

This section is informative to the reader to reference cryptographic services and other services of AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U) (the “module”) from Advanced Micro Devices (AMD) (the “vendor”). Only the components listed in Section 2.1 are subject to the FIPS 140-3 validation. The CMVP (Cryptographic Module Validation Program) makes no statement as to the correct operation of the module or the security strengths of the generated keys (when supported) if the specific operational environment is not listed on the validation certificate.

0.2. This Security Policy Document

This Security Policy describes the features and design of the module named AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U)[1] using the terminology contained in the FIPS 140-3 specification. The FIPS 140-3 Security Requirements for Cryptographic Module specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic module to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The Security Policy document is one document in a FIPS 140-3 Submission Package. In addition to this document, the Submission Package contains:

- The validation report prepared by the lab.
- The Entropy Assessment Report (EAR) if applicable.
- Other supporting documentation and additional references.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

0.3. How this Security Policy was Prepared

The vendor has provided the non-proprietary Security Policy of the cryptographic module, which was further consolidated into this document by atsec information security together with other vendor-supplied documentation. In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

[1]PSP: Platform Security Processor

1. General

This document is the non-proprietary FIPS 140-3 Security Policy for version bc0c0140FIPS001 of the AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U) cryptographic module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

Table 1 describes the individual security areas of FIPS 140-3, as well as the security levels of those individual areas.

Table 1: Security levels

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	1
8	Non-invasive Security	n/a
9	Sensitive Security Parameter Management	1
10	Self-tests	1
11	Life-cycle Assurance	1
12	Mitigation of Other Attacks	n/a
Overall		**1**

2. Cryptographic Module Specification

The following subsections describe the cryptographic module and how it conforms to the FIPS 140-3 specification in each of the required areas.

2.1. Module Overview, Embodiment, Type

The AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U) (hereafter referred to as "the module") is defined as type sub-chip hybrid firmware module in a single chip embodiment, with hardware (the coprocessor) and firmware components implementing general purpose cryptographic algorithms. The module supports the Ryzen PRO 5000 Series SoC (System on a Chip) by providing digital signature verification of the key database during secure boot procedures. The module resides within the Ryzen SoC that contains the module, the processor, the firmware, and other components in a single chip embodiment (Figure 1).

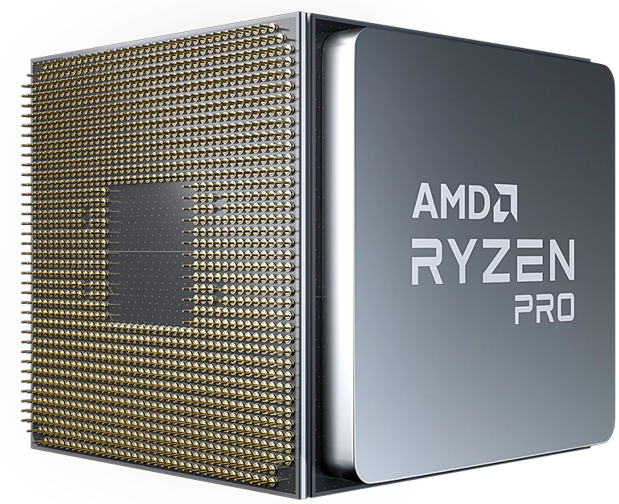

Figure 1: The AMD Ryzen PRO SoC, representing all versions of the single chip tested platforms.

The Operational Environments tested for the module are described in Section 2.4

2.2. Module Design, Components and Versions

Figure 2 shows a block diagram that represents the design of the module. In this diagram, the physical perimeter of the operational environment, defined by the perimeter of the AMD Ryzen PRO SoC (i.e., the enclosure of the SoC), is indicated by a purple dashed line. The cryptographic boundary is represented by the components painted in orange blocks. These components are further described in Table 2.

Table 2: Components in the cryptographic boundary.

Component	Type	Version	Description
Bootloader (boot_loader_stage1 .sbin)	Firmware	bc0c0140FIPS001	Performs self-tests, provides service indicator and show status service.
BootROM	Non-reconfigur	bc0c0140FIPS001	Provides interface to the hardware

Component	Type	Version	Description
	able memory		cryptographic implementations.
RSA implementation in the CCP	Hardware	bc0c0140FIPS001	Hardware implementation of the algorithm.
SHA2-384 implementation in the CCP	Hardware	bc0c0140FIPS001	Hardware implementation of the algorithm.

The flow of information between the components and the relation between that data and the module’s FIPS interfaces are depicted through arrows. The arrows are colored differently to facilitate visualization. The color does not identify the type of data: the type of data flow (namely, data input, data output, status output and control input) is indicated by labels pointing to the arrows.

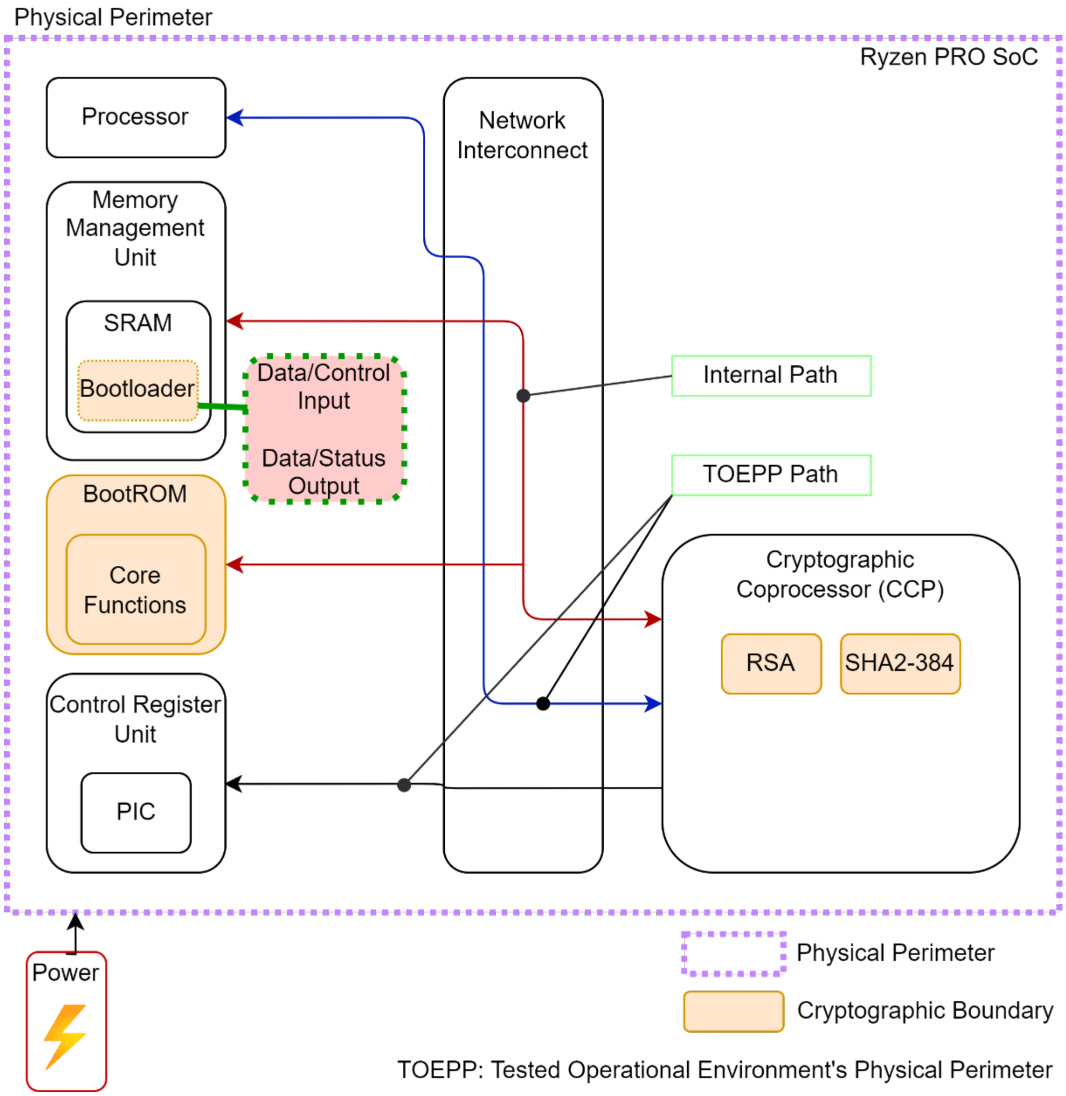

Figure 2: The block diagram depicting physical perimeter of the operational environment and cryptographic boundary, and data flow between the components in the single chip.

2.2.1. Components Excluded from Security Requirements

The components inside the single chip that are indicated in white blocks in Figure 2 are not included in the cryptographic boundary and hence are excluded from the requirements of FIPS 140-3. Table 3 lists these components and a rationale for their exclusion.

Table 3: Components excluded from the security requirements of FIPS 140-3.

Component	Rationale for Exclusion
Processor	Does not implement the cryptographic functions and does not interfere with the functions of the cryptographic coprocessor (CCP). Inside the single-chip, the processor executes non-cryptographic functions from the firmware components (i.e., functions not implemented in the cryptographic coprocessor).

Component	Rationale for Exclusion
Memory Management Unit	Manages memory functions only. The unit does not share the Bootloader space with other functions within the SoC. In this unit, only the Bootloader component is utilized by the module.
Network Interconnect	Provides paths for data without otherwise modifying or exporting the data without knowledge of the module.
Control Register Unit	Provide control of the internal registers of the SoC. No data is modified or exported from this unit.

2.3. Security Level

The module is validated according to FIPS 140-3 at overall security level 1. The security levels of individual areas are indicated in Table 1.

2.4. Tested Operational Environments

The module has been tested on the operational environments indicated in Table 4 with the corresponding module variants and configuration options.

Table 4: Tested operational environments.

#	Operating System	Hardware Platform	SoC/Processor	PAA/ Acceleration
1	N/A	AMD Ryzen PRO 5475U (100-000000587)	AMD Ryzen PRO 5475U (100-000000587)	None
2	N/A	AMD Ryzen PRO 5675U (100-000000584)	AMD Ryzen PRO 5675U (100-000000584)	None
3	N/A	AMD Ryzen PRO 5875U (100-000000581)	AMD Ryzen PRO 5875U (100-000000581)	None

2.5. Modes of Operation of the Module

The module implements only one mode of operation, the approved mode, in which the approved services are available. No configuration is necessary for the module to operate and remain in the approved mode.

2.6. Security Functions

2.6.1. Approved Security Functions

Table 5 lists all approved security functions (cryptographic algorithms) of the module, including specific key lengths employed for approved services, and implemented modes or methods of operation of the algorithms.

Table 5: Approved cryptographic algorithms.

CAVP Cert.	Algorithm and Standard	Mode/Method	Description, Key Size / Key Strength	Use / Function
A1719	RSA FIPS186-4	PKCSPSS with SHA2-384	4096	Digital signature verification
A1719	SHS FIPS180-4	SHA2-384	N/A	Message digest

2.6.2. Non-Approved Security Functions Allowed in Approved Services

The module does not offer any non-approved cryptographic algorithms that are allowed in approved services.

2.6.3. Non-Approved Security Functions Allowed in Approved Services with No Security Claimed

The module does not offer any non-approved cryptographic algorithms that are allowed in approved services but claim no security.

2.6.4. Non-Approved Security Functions Not Allowed in Approved Services

The module does not offer any non-approved cryptographic algorithms not allowed in approved services.

2.7. Rules of operation

The module initializes upon power-on. After the pre-operational self-tests are successfully concluded, the module automatically transitions to the operational state.

In the operational state, the module automatically performs the signature verification of the key database using the RSA signature verification service, which is the sole service provided by the module. The key database and RSA public key are accessed by the module bootloader component (who then acts as the operator of the module) without operator input. After the successful signature verification of the key database, the module unloads itself from memory, ceasing its operation.

All the procedures described above are conducted without operator assistance. To perform the procedures again, the module must be reset, which will trigger a new boot.

3. Cryptographic Module Interfaces

Table 6 summarizes the cryptographic module interfaces[2]. The logical interfaces are logically separated from each other by the API design. The power interface is physically separated from any other interface.

Table 6: Ports and interfaces.

Physical Port	Logical Interface	Data that passes over port/interface
Input registers, DMA interface	Data Input	API input parameters for data.
Output registers, DMA interface	Data Output	API output parameters for data.
Command Queue Control registers	Control Input	API function calls, API input parameters for control.
Status registers	Status Output	API return codes, status values.
Power port	Power (input) interface	Power port or pin in the single-chip.

2

4. Roles, Services and Authentication

4.1. Roles

Table 7 lists the roles supported by the module with corresponding services with input and output.

The module supports the Crypto Officer role only. This sole role is implicitly and always assumed by the operator of the module.

Table 7: Roles, service commands, input, and output.

Role	Service	Input	Output
Crypto Officer	Digital Signature Verification	Key database (pointer to contents), signature, public key.	Success, fail.
Crypto Officer	Show Version	None.	Name and version information in data output interface.
Crypto Officer	Show Status	None.	Current status in status output interface (as return codes and/or log messages).
Crypto Officer	On-Demand Self-Test	None.	None.
Crypto Officer	On-Demand Integrity Test	None.	None.
Crypto Officer	Zeroize	None.	None.

4.2. Authentication

The module does not support authentication for roles.

4.3. Services

The module provides services to operators that assume the available role. All services are described in detail in the user documentation.

The next subsections define the services that utilize approved, allowed, and non-approved security functions in this module. For the respective tables, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **Generate (G)**: The service establishes the SSP by generation, agreement, or derivation.
- **Read (R)**: The SSP exists in the module and is read by the service, and may be output.
- **Write (W)**: The caller provides the SSP to the service to be imported into the module; written; or updated if the SSP already exists in the module.
- **Execute (E) (or use)**: The service uses the SSP in performing a cryptographic operation. Other access types identify the provenance of the SSP.
- **Zeroize (Z)**: The service zeroizes the SSP.

- **N/A**: The service does not access any SSP or key during its operation.

The module provides only one approved service with approved parameters, and no non-approved services. The approved service indicator is thus considered a global indicator and it is set after successful completion of the pre-operational and conditional self-tests.

4.3.1. Approved Services

Table 8 lists the approved services in this module, the roles that can request the service, the algorithms involved, the Sensitive Security Parameters (SSPs) involved and how they are accessed, and the respective service indicator.

In the service tables, CO specifies the Crypto Officer role.

Table 8: Services that use approved and allowed algorithms.

Service	Service Description	Approved Security Functions	Keys, SSPs	Role	Access Types	Indicator
Digital Signature Verification	Verify signature operations	RSA PSS using SHA2-384	RSA public key	CO	W, E	Global indicator readable through Microsoft HSTI and through UEFI interactive shell tool (upon successful self-tests and the module becomes operational, module only offers approved services).
Other Services						
Show Version	Show the version of the module's components	N/A	None	CO	N/A	None.
Show Status	Show status of the module state	N/A	None	CO	N/A	None.
On-Demand Self-Test	Initiate on-demand self-tests by reset	N/A	None	CO	N/A	None.
On-Demand Integrity Test	Initiate the integrity test (pre-operational self-test)	SHA2-384	None	CO	N/A	Global indicator readable through Microsoft HSTI and through UEFI interactive shell tool (upon successful self-tests and the module becomes operational, module only offers approved services).

Service	Service Description	Approved Security Functions	Keys, SSPs	Role	Access Types	Indicator
Zeroize	Zeroize PSP in volatile memory	N/A	All SSPs	CO	Z	PSP is no longer accessible

4.3.2. Non-Approved Services

There are no non-approved services.

5. Software/Firmware Security

5.1. Integrity Techniques

The integrity of the bootloader component of the module (in firmware) is verified by comparing a SHA2-384 digest value calculated at run time with the SHA2-384 digest value stored in the module that was computed at build time.

The bootROM component of the module is a non-reconfigurable memory (specifically masked ROM), thus exempt from the requirements of integrity test. The vendor declares that this bootROM component composed of non-reconfigurable memory does not degrade before 10 (ten) years of manufacture date, thus complying with the requirements of IG 5.A. Please refer to Section 11.1.3.

5.2. On-Demand Integrity Test

Integrity tests are performed as part of the Pre-Operational Self-Tests. The integrity test may be invoked on-demand in two ways: through the On-Demand Self-Test service, and through the On-Demand Integrity Test service.

The module provides the On-Demand Self-Test service to perform self-tests on demand. This service performs the same cryptographic algorithm tests executed during power-up, i.e., the cryptographic algorithm self-tests and the pre-operational self-test. This service is invoked by powering-off and reloading the module.

The On-Demand Integrity Test service can be used to perform only the on-demand pre-operational self-tests. This service is invoked by calling the integrity test API using the module’s logical interfaces. More details on the API are provided by the vendor in its developer’s manual.

6. Operational Environment

6.1. Applicability

The module operates in a non-modifiable operational environment per FIPS 140-3 level 1 specifications.

6.2. Tested Operational Environments

Please see Section 2.4.

6.3. Policy and Requirements

The operational environment provides context separation for the memory and registers utilized by the module. When these components are used by the module, no other process or sub-component can access the information concurrently.

The bootloader component also acts as the sole operator of the module, thus there are no concurrent operators.

7. Physical Security

7.1. General

The embodiment of the sub-chip module is a single chip consisting of production-grade components. The coating is a standard sealing coat applied over the single chip.

The module provides no additional physical security techniques.

8. Non-Invasive Security

The module claims no non-invasive security techniques.

9. Sensitive Security Parameter Management

Table 9 summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module in the approved services (Table 8).

Table 9: Sensitive Security Parameters (SSPs).

SSP	Strength	Security Function and Cert. #	Generation	Import /Export	Establishment	Storage	Zeroization	Use
RSA public key	150 bits	RSA signature verification (A1719)	N/A	Input in plaintext through data input interface. No output.	N/A	Volatile memory	When the module ends its operation	RSA signature verification

9.1. SSP Generation

The module does not generate SSPs.

9.2. SSP Establishment

The module does not implement SSP establishment.

9.3. SSP Entry/Output

The module does not support manual key entry or intermediate key generation key output. In addition, the module does not produce key output..

The public key supplied to the module's services is provided by the operator via the data input interface.

9.4. SSP Storage

SSPs are provided to the module by the calling process and are destroyed when released by the respective functions.

The module does not perform persistent storage of SSPs; keys in use by the module exist in volatile memory only.

9.5. SSP Zeroization

The module's functions deallocates and zeroizes temporary SSP values in volatile memory used during the function's execution. The zeroization consists of writing zeroes to the memory location used by the SSP before deallocating the area. The module does not overwrite the SSP with another SSP.

The zeroization service for the SSP in volatile memory consists of powering off the module, which will remove power from the volatile memory. This action will cause the value of the SSP in volatile memory to be overwritten by random values the next time the module is powered on.

The RSA public key used for the RSA signature verification function is not stored within the components of the module, but in permanent storage outside of the single chip. This storage can be zeroized by blowing the memory fuse (outside of the single chip).

9.6. Random Number Generation

The module does not implement random number generation.

10. Self Tests

The module performs pre-operational self-tests and conditional self-tests. While the module is executing the self-tests, services are not available, and data output (via the data output interface) is inhibited until the tests are successfully completed.

All the self-tests are listed in Table 10, with the respective condition under which those tests are performed. The firmware integrity test is performed after all conditional algorithm self-tests (CASTs) are performed.

Table 10: Self-tests.

Algorithm	Parameters	Condition for Test	Type	Test
RSA	SHA2-384 and 4096-bit key	Power up	Conditional Algorithm Self-Test	KAT signature verification
SHA2-384	N/A	Firmware integrity test on bootloader component at power up (after all CASTs)	Pre-Operational Self-Test	Digest verification on bootloader firmware component
SHA2-384	N/A	Power up	Conditional Algorithm Self-Test	KAT SHA2-384

10.1. Pre-Operational Self-Tests

The module performs pre-operational tests automatically when the module is powered on. The pre-operational self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected. The module transitions to the operational state only after the pre-operational self-tests are passed successfully.

The types of pre-operational self-tests are described in the next sub-sections.

10.1.1. Firmware Integrity Test

The integrity of the bootloader component of the module (in firmware) is verified by comparing a SHA2-384 digest value calculated at run time with the SHA2-384 digest value stored in the module that was computed at build time. If the comparison verification fails, the module transitions to the error state (Section 10.3). The SHA2-384 algorithm goes through its conditional algorithm self-test before the integrity test is performed (Table 10).

The bootROM component of the module is considered non-reconfigurable memory, thus exempt from the requirements of integrity test. The vendor declares that this bootROM component composed of non-reconfigurable memory does not degrade before 10 (ten) years of manufacture date, thus complying with the requirements of IG 5.A.

10.2. Conditional Tests

10.2.1. Cryptographic Algorithm Self-Tests

The module performs self-tests on all approved cryptographic algorithms as part of the approved services supported in the approved mode of operation, using the tests shown in Table 10. Data output through the data output interface is inhibited during the self-tests.

10.2.2. Periodic/On-Demand Self-Test

The module performs on-demand self-tests initiated by the operator, by powering off and powering the module back on. The full suite of self-tests in Table 10 is then executed.

The same procedure may be employed by the operator to perform periodic self-tests.

10.3. Error States

If the module fails any of the self-tests, the module enters the error state. In the error state, the module outputs the error type through the status indicator and status output interface. In the error state, the data output interface is inhibited, and the module accepts no more inputs or requests. The module does not implement a control output interface.

Table 11 lists the error state and the status indicator (through FW_STATUS register) values that explains the error that has occurred.

Table 11: Error states.

Error State	Error Condition	Status Indicator (FW_STATUS)
Error	SHA2-384 self-test error	Error code AA0000FB
	RSA self-test error	Error code AA0000FC
	Integrity test error	Error code AA0000FD

To recover from the error state (clearing the error condition), the module shall be restarted or reset.

11. Life-Cycle Assurance

11.1. Delivery and Operation

11.1.1. Procedures for Secure installation, Initialization, Start-up, and Operation of the Module

The procedures herein described are directed at OEMs for producing and configuring their BIOS so that the FIPS module is properly enabled to operate as the validated module in conformance with the rules in this Security Policy document.

Once properly installed and enabled, no configuration is necessary for the module to operate and remain in the approved mode, as it is the only mode of operation of the module.

11.1.1.1. To enable the FIPS capability

1. Reserve 16KiB at least for Platform Security Processor level 1 directory, as the FIPS module requires additional 8KiB of ROM space for the Platform Security Processor L1 Bootloader.
2. The Platform BIOS must include the file with "_FIPS" postfix in the file name as Platform Security Processor entry 0x1. For example, the file PspBootLoader_stage1_prod_AB_RN_FIPS.sbin has "_FIPS" postfix in the file name. This file is thus a FIPS capable Platform Security Processor boot loader. Conversely, the file PspBootLoader_stage1_prod_AB_RN.sbin does not have "_FIPS" postfix in the file name, making this file a non-FIPS capable Platform Security Processor boot loader.
3. Set BIT 32 of Platform Security Processor soft fuse chain (Platform Security Processor entry 0xB) to enable FIPS capability.
    a. The BIT32 in Platform Security Processor entry 0xB is defined as FIPS capability enablement. If 0, the FIPS capability is OFF; if 1, the FIPS capability is ON (i.e., the module is properly installed as the validated module described in this document).

11.1.1.2. To verify whether FIPS capability is on

1. Boot the system into UEFI shell with secure boot disabled.
2. Use the UEFI shell version of the AFF Tool version 0.3 and beyond. This tool is provided by the vendor. Run the AFF Tool with the command: afftool –fips from the interactive UEFI shell provided by the BIOS.
    a. If it shows "FIPS mode: on", this is the FIPS capable module installed.
    b. If it shows "FIPS mode: off", the module (described in this document) is disabled.

The screenshot in Figure 3 shows the usage of the AFF Tool. The output indicates that the FIPS module is disabled. In this condition, the module does not operate in conformance with this Security Policy document.

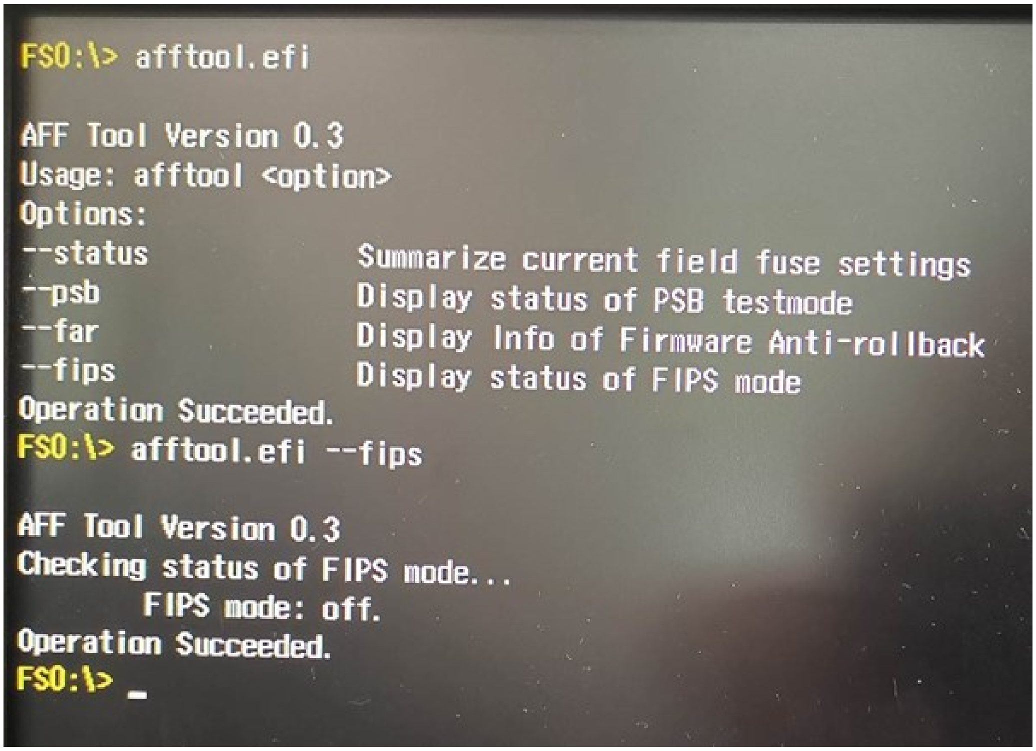

Figure 3: AFF Tool indicates that the module was not enabled.

The screenshot in Figure 4 again shows the usage of the AFF Tool. The output demonstrates that the FIPS module is enabled and thus will operate as the FIPS validated module according to the rules in this Security Policy document.

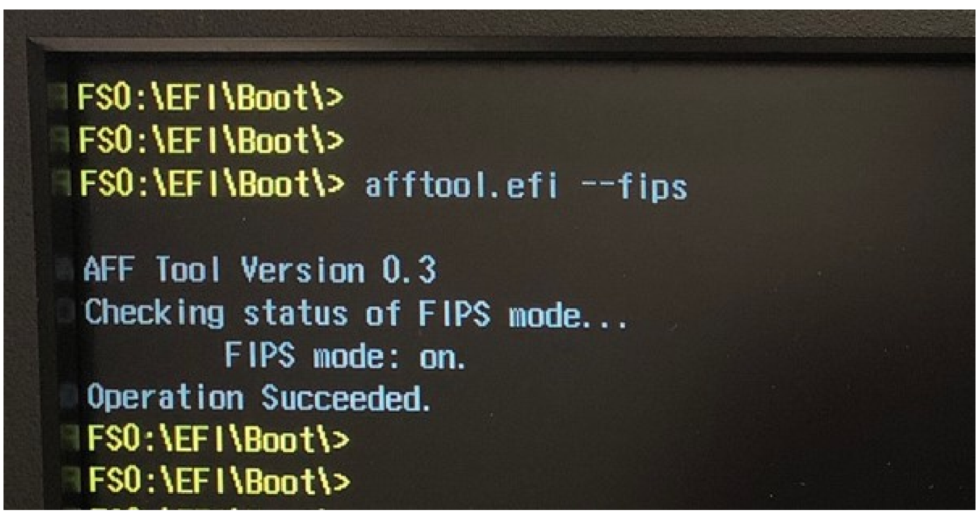

Figure 4: AFF Tool indicating that the module is enabled.

11.1.2. Maintenance Requirements

There are no maintenance requirements.

11.1.3. End of Life

The process for performing “End of Life” occurs at the chronological point of 10 years starting from manufacturing date of the module.

As stated in Section 9.4, the module does not possess persistent storage of SSPs. The SSP value only exists in volatile memory and that value vanishes when the module is powered off. The procedure for secure sanitization of the module at the end of life is simply to power it off, which is the action of zeroization of the SSPs (Section 9.5) . As a result of this sanitization via power-off, the SSP is removed from the module, so that the module may either be distributed to other operators or disposed.

11.2. Administrator Guidance

All the functions, ports and logical interfaces described in this document are available to the Crypto Officer. The module only provides approved functions, and as such there are no special procedures to administer the approved mode of operation.

11.3. Non-Administrator Guidance

The module implements only the Crypto Officer. There are no requirements for non-administrator operators.

12. Mitigation of Other Attacks

The module does not implement security mechanisms to mitigate other attacks.

13. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standards
HMAC	Hash Message Authentication Code
HSTI	(Microsoft) Hardware Security Test Interface
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
OS	Operating System
PAA	Processor Algorithm Acceleration
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

14. References

FIPS PUB 180-4. Secure Hash Standard (SHS). (2012, March). *FIPS PUB 180-4. Secure Hash Standard (SHS)*. Gaithersburg, MD 20899-8900: National Institute of Standards & Technology. Retrieved from http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

FIPS PUB 186-4. Digital Signature Standard (DSS). (2013, July). *FIPS PUB 186-4. Digital Signature Standard (DSS)*. https://doi.org/10.6028/NIST.FIPS.186-4. doi:https://doi.org/10.6028/NIST.FIPS.186-4

Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program. (2022, March 14). *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program*. Retrieved 03 8, 2021, from https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips 140-3/FIPS 140-3 IG.pdf

ISO/IEC. (2012, August). ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules. *ISO/IEC 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules*. Retrieved from https://www.iso.org/standard/52906.html

ISO/IEC. (2017, March). ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules. *ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules*. Retrieved from https://www.iso.org/standard/72515.html

National Institute of Standards Technology. (2019, March). FIPS PUB 140-3. Security Requirements for Cryptographic Modules. *FIPS PUB 140-3. Security Requirements for Cryptographic Modules*. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf