

Advanced Micro Devices (AMD)

AMD ASP Cryptographic CoProcessor ("Phoenix2")

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 9
2.7 Algorithm Specific Information 10
2.8 RBG and Entropy 10
2.9 Key Generation 10
2.10 Key Establishment 10
2.11 Industry Protocols 10
3 Cryptographic Module Interfaces 11
3.1 Ports and Interfaces 11
4 Roles, Services, and Authentication 12
4.1 Authentication Methods 12
4.2 Roles 12
4.3 Approved Services 12
4.4 Non-Approved Services 13
4.5 External Software/Firmware Loaded 13
5 Software/Firmware Security 14
5.1 Integrity Techniques 14
5.2 Initiate on Demand 14
6 Operational Environment 15
6.1 Operational Environment Type and Requirements 15
6.2 Configuration Settings and Restrictions 15
7 Physical Security 16
7.1 Mechanisms and Actions Required 16
8 Non-Invasive Security 17
9 Sensitive Security Parameters Management 18
9.1 Storage Areas 18

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.2 SSP Input-Output Methods 18
9.3 SSP Zeroization Methods 18
9.4 SSPs 18
10 Self-Tests 20
10.1 Pre-Operational Self-Tests 20
10.2 Conditional Self-Tests 20
10.3 Periodic Self-Test Information 21
10.4 Error States 21
10.5 Operator Initiation of Self-Tests 22
11 Life-Cycle Assurance 23
11.1 Installation, Initialization, and Startup Procedures 23
11.2 Administrator Guidance 23
11.3 Non-Administrator Guidance 23
11.4 Design and Rules 24
11.5 Maintenance Requirements 24
11.6 End of Life 24
12 Mitigation of Other Attacks 25
A Glossary and Abbreviations 26
B References 27

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 9
Table 5: Non-Approved, Not Allowed Algorithms 9
Table 6: Security Function Implementations 10
Table 7: Ports and Interfaces 11
Table 8: Roles 12
Table 9: Approved Services 13
Table 10: Non-Approved Services 13
Table 11: Mechanisms and Actions Required 16
Table 12: Storage Areas 18
Table 13: SSP Input-Output Methods 18
Table 14: SSP Zeroization Methods 18
Table 15: SSP Table 1 19
Table 16: SSP Table 2 19
Table 17: Pre-Operational Self-Tests 20
Table 18: Conditional Self-Tests 21
Table 19: Pre-Operational Periodic Information 21
Table 20: Conditional Periodic Information 21
Table 21: Error States 22

List of Figures

Figure 1: AMD Ryzen 5 PRO 8500GE (left), AMD Ryzen 3 PRO 7440U (middle & right) 7
Figure 2: Block Diagram 7

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version bc0d0b41FIPS001 of the AMD ASP Cryptographic CoProcessor ("Phoenix2") 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.

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.

1.2 Security Levels

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 Level	1

Table 1: Security Levels

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The AMD ASP Cryptographic CoProcessor ("Phoenix2") (hereafter referred to as "the module") is defined as a sub-chip hardware module in a single chip embodiment, with hardware and firmware components providing digital signature verification of the key database during secure boot procedures.

Upon boot, the module verifies the SHA2-384 hash of the root public key, which serves as the trust anchor for the SoC. Then, it loads the key database and computes the firmware de-obfuscation keys. Additional firmware loaded from outside the SoC is verified using RSA-PSS and de-obfuscated using AES. Finally, the key database is verified again using RSA-PSS, after which the module automatically ends its operation.

Module Type: Hardware
Module Embodiment: Single Chip
Module Characteristics: SubChip

Cryptographic Boundary:

The module consists primarily of the ARM Cortex-A5, hardware implementations of RSA, SHA-2, and AES in the Cryptographic CoProcessor, and the non-reconfigurable Boot ROM. These hardware components are sub-components of the Ryzen PRO 7000 Series and Ryzen PRO 8000 Series SoCs.

In addition, the cryptographic boundary contains two associated firmware components: the Stage 1 Bootloader and the fips_module firmware. Both components are permanently stored inside SPI flash storage, outside the SoC, and loaded into the SRAM on startup.

The block diagram in Figure 2 shows the design of the module when the module is operational and the firmware components have been loaded into the SRAM. In this diagram, the physical boundary of the module, defined by the perimeter of the Ryzen SoC (i.e., the enclosure of the SoC), is indicated by a dashed purple line. The cryptographic boundary is represented by the components painted in orange blocks. Solid orange lines indicate the flow of data within the cryptographic module (i.e., internal paths). Dashed green lines are used to denote the logical interfaces defined in Section 3.

Components in white are only included in the diagram for informational purposes. They are not included in the cryptographic boundary (and therefore not part of the module's validation).

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP is the Ryzen SoC (hardware) single chip, a rectangular enclosure measuring approximately 40 mm x 40 mm x 5.77 mm (AM5) or 25 mm x 35 mm x 1.38 mm (FP7/FP7r2).

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.



Figure 1: AMD Ryzen 5 PRO 8500GE (left), AMD Ryzen 3 PRO 7440U (middle & right)

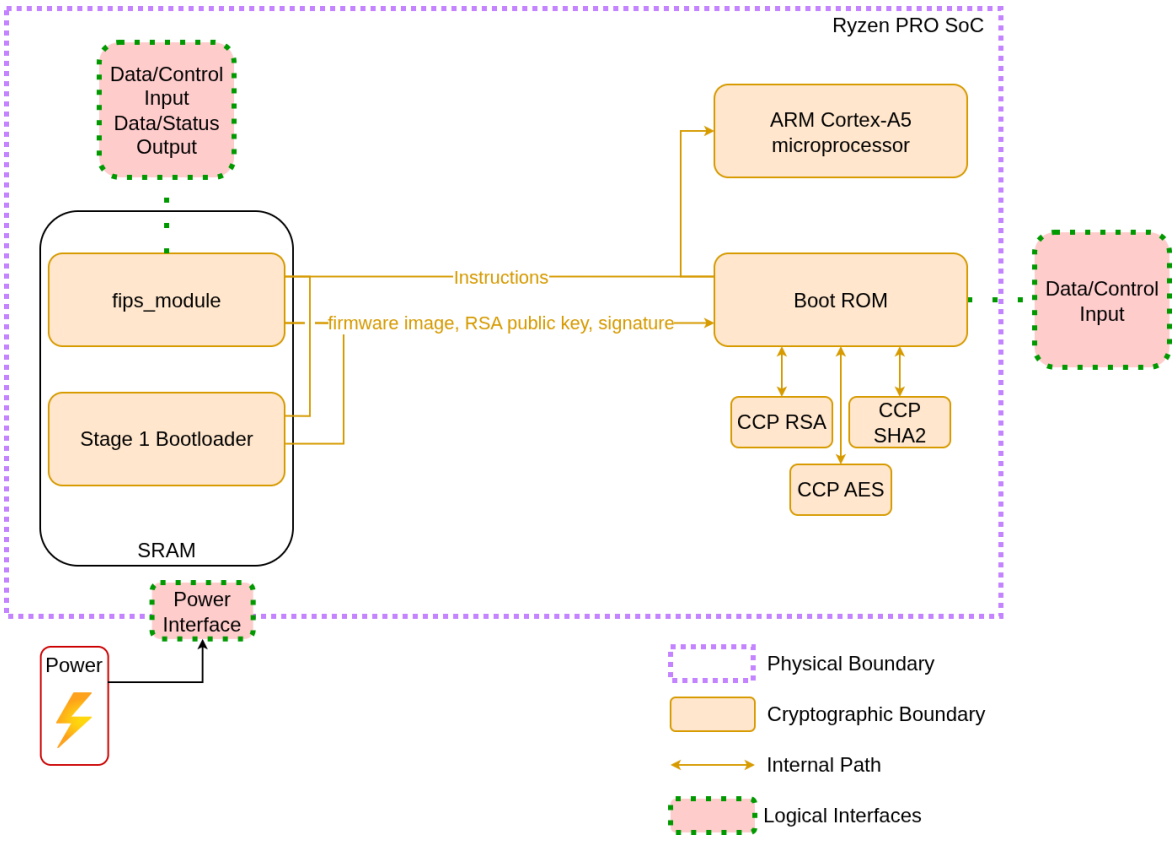


Figure 2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
AMD Ryzen 5 PRO 8500GE	bc0d0b41FIPS001	bc0d0b41FIPS001	ARM Cortex-A5	AM5 socket
AMD Ryzen 3 PRO 7440U (FP7)	bc0d0b41FIPS701	bc0d0b41FIPS701	ARM Cortex-A5	FP7 socket
AMD Ryzen 3 PRO 7440U (FP7r2)	bc0d0b41FIPS701	bc0d0b41FIPS701	ARM Cortex-A5	FP7r2 socket

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no components excluded from the requirements of the FIPS 140-3 standard.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	The operational state assumed by the module when executing any of its approved services	Approved	POST code 0x1023 or bit 0 in FIPS_selftest_status is set
Non-approved mode	On startup, while loading the firmware components	Non-Approved	POST code not 0x1023 and bit 0 in FIPS_selftest_status is not set

Table 3: Modes List and Description

On startup, the module operates in a non-approved mode while loading the firmware components. After passing all pre-operational self-tests and after all firmware components have been loaded, the module automatically transitions to the approved mode. No operator intervention is required to reach this point.

Mode Change Instructions and Status:

Once all firmware components have been loaded, the module automatically switches to 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.

2.5 Algorithms

Approved Algorithms:

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-5)	A8050	Hash Pair - Hash Algorithm - SHA2-384 Mask Function - mgf1 Modulo - 4096 Signature Type - pss Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
RSA SigVer (FIPS186-5)	A8226	Hash Pair - Hash Algorithm - SHA2-384 Mask Function - mgf1 Modulo - 4096 Signature Type - pss Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-384	A8050	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A8226	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES ECB de-obfuscation	De-obfuscation of firmware obfuscation keys
AES CBC de-obfuscation	De-obfuscation of firmware images

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Message Digest	SHA	Compute a message digest		SHA2-384: (A8050, A8226)

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Digital Signature Verification	DigSig-SigVer	Verify a digital signature		RSA SigVer (FIPS186-5): (A8050, A8226)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

RSA:
For RSA signature verification, the module supports a modulus size of 4096 bits. All supported modulus sizes have been CAVP tested.

2.8 RBG and Entropy

The module does not implement any random bit generation methods.

2.9 Key Generation

The module does not implement any key generation methods.

2.10 Key Establishment

The module does not implement any key establishment methods.

2.11 Industry Protocols

The module does not implement any industry protocols.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
RESET	Control Input	Power-on signal to Boot ROM
SMN	Data Input	Root public key, firmware image, key database image
USB	Data Input	Firmware image
FW_STATUS register	Status Output	Error codes (AA0000FB, AA0000FC, AA0000FD, or AA0000FE)
SRAM	Data Output Control Input Data Input Status Output	API output parameters for data; API function calls, API input parameters for control; API input parameters for data; API return codes, status values; POST codes
Power port	Power	Power port or pin on the SoC

Table 7: Ports and Interfaces

The logical interfaces are logically separated from each other by the API design. The module does not implement the control output interface. The power interface is physically separated from any other interface.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not implement any authentication methods.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 8: Roles

No support is provided for multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Load Root Public Key	Boot ROM validates and loads the root public key used for secure boot	POST code 0x1023	Root public key	POST code	Message Digest	Crypto Officer - Root public key hash: W - Root public key: W
Validate Firmware Image	Stage 1 Bootloader or fips_module validates a firmware image	Bit 0 in FIPS_selftest_status is set	Firmware image, RSA public key, signature	Pass/fail	Digital Signature Verification	Crypto Officer - RSA public key: W,E
Show Version	Return the module version information	None	None	Module version	None	Crypto Officer
Show Status	Return the module status	None	None	Module status	None	Crypto Officer
Self-test	Initiate on-demand self-tests by reset	None	None	Pass/fail	Digital Signature Verification Message Digest	Crypto Officer
Zeroization	Zeroize all SSPs	None	None	None	None	Crypto Officer - RSA

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						public key: Z

Table 9: Approved Services

For the above table, the convention below applies when specifying the access permissions (types) that the service has for each SSP.

- **Generate (G)**: The module generates or derives the SSP.
- **Read (R)**: The SSP is read from the module (e.g. the SSP is output).
- **Write (W)**: The SSP is updated, imported, or written to the module.
- **Execute (E)**: The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z)**: The module zeroizes the SSP.
- **N/A**: The module does not access any SSP or key during its operation.

The approved service indicator can be retrieved using Microsoft HSTI and through the UEFI interactive shell tool.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Load Firmware De-obfuscation Key	Boot ROM computes the key used to de-obfuscate firmware images	AES ECB de-obfuscation	Crypto Officer
Load Firmware Image	Boot ROM or Stage 1 Bootloader loads and de-obfuscates a firmware image	AES CBC de-obfuscation	Crypto Officer

Table 10: Non-Approved Services

4.5 External Software/Firmware Loaded

Upon startup, the Boot ROM loads the Stage 1 Bootloader firmware from external SMN storage (SPI flash) into the sub-chip cryptographic subsystem. The integrity of the Stage 1 Bootloader firmware is determined by verifying an RSA-PSS 4096 with SHA2-384 signature stored in the firmware that was computed at build time. Subsequently, the Stage 1 Bootloader loads the fips_module firmware component from external SMN storage (SPI flash) into the sub-chip cryptographic subsystem. The integrity of the fips_module firmware is verified identically to the Stage 1 Bootloader (i.e., RSA-PSS 4096 with SHA2-384).

If any signature verification fails, the firmware load test fails. The root public key used to verify the signatures is loaded on start-up by the Boot ROM and verified using a SHA2-384 hash stored inside the module. The private key associated with this public key is controlled by the vendor.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the loaded firmware components of the module is discussed in Section 4.5.

In addition to the firmware load test, the fips_module firmware also performs a pre-operational firmware integrity test on its own binary and the stage 1 bootloader binary. These integrity tests also perform RSA-PSS 4096 with SHA2-384 signature verification.

The functionality in the Boot ROM component of the module is non-reconfigurable memory (specifically masked ROM), thus exempt from the requirements of integrity test. The vendor declares that this Boot ROM does not degrade before 10 years of manufacture date, thus complying with the requirements of IG 5.A. Please refer to Section 11.6.

5.2 Initiate on Demand

The pre-operational firmware integrity tests and firmware load tests can be performed on demand by resetting the module.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The module operates in a limited operational environment, as the operational environment permits loading of external firmware, but only the firmware controlled / signed by the vendor.

How Requirements are Satisfied:

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.

6.2 Configuration Settings and Restrictions

No configuration of the operational environment is required for the module to operate in an approved mode. Therefore, there are no rules, settings, or restrictions to the configuration of the operational environment.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Opaque sealing coat	No actions are required to maintain the physical security of the module	No actions are required to maintain the physical security of the module

Table 11: Mechanisms and Actions Required

The embodiment of the 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. No actions are required to maintain the physical security of the module.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

This module does not implement any non-invasive security mechanisms.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Boot ROM	Persistent storage used to store the hash of the root public key	Static
SRAM	Temporary storage for SSPs used by the module as part of service execution	Dynamic

Table 12: Storage Areas

The module stores only one SSP persistently: the root public key hash. This PSP is always physically protected, as the sealing coating applied to the single chip provides some level of security against unauthorized modification. All other SSPs used by the module exist in volatile memory only.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
API input parameters	Operator residing on TOEPP	SRAM	Plaintext	Manual	Electronic	
SMN memory read	Flash external to the SoC	SRAM	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Destruction of the ROM	Procedural zeroization of the ROM by physically destroying it	The root public key hash is irretrievable if the memory is destroyed	By any appropriate disposal method (e.g., shredding)
Remove power from the SoC	De-allocates the volatile memory used to store SSPs	Volatile memory used by the module is overwritten within nanoseconds when power is removed	By removing power

Table 14: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Root public key hash	SHA2-384 hash of the root public key used to anchor secure boot	384 bits - 384 bits	Public key hash - PSP			
Root public key	RSA root public key used to anchor secure boot	4096 bits - 150 bits	Public key - PSP			
RSA public key	Public key used for RSA signature verification	4096 bits - 150 bits	Public key - PSP			

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Root public key hash		Boot ROM:Plaintext	For the lifetime of the module		
Root public key	SMN memory read	SRAM:Plaintext	While the module is operational	Remove power from the SoC	
RSA public key	API input parameters	SRAM:Plaintext	For the duration of the service	Remove power from the SoC	

Table 16: SSP Table 2

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 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. The module does not return control to the calling application until the tests are completed.

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Stage 1 bootloader firmware integrity test	PSS using 4096-bit root public key with SHA2-384	Signature verification	SW/FW Integrity	Module is operational	Signature verification is performed on the entire stage 1 bootloader firmware image
fips_module firmware integrity test	PSS using 4096-bit root public key with SHA2-384	Signature verification	SW/FW Integrity	Module is operational	Signature verification is performed on the entire fips_module firmware image

Table 17: Pre-Operational Self-Tests

The pre-operational firmware integrity test on the fips_module firmware component is performed automatically when the fips_module firmware is initialized. If this test fails, the module transitions to the error state.

10.2 Conditional Self-Tests

As part of the initialization, the firmware verification functionality in the Boot ROM loads the Stage 1 Bootloader firmware and performs the firmware load test on it. Then, execution is handed to the Stage 1 Bootloader, which loads the fips_module firmware component and performs the firmware load test on it. Finally, the fips_module firmware component performs the self-tests on all approved cryptographic algorithms, prior to the firmware integrity test. The module transitions to the operational state only after all self-tests pass successfully.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Stage 1 bootloader firmware load test	PSS using 4096-bit root public key with SHA2-384	Signature verification	SW/FW Load	POST code 0x102D	Signature verification is performed on the entire stage 1 bootloader firmware image	Power on
fips_module firmware load test	PSS using 4096-bit root public key with SHA2-384	Signature verification	SW/FW Load	Bit 4 in FIPS_selftest_status is set	Signature verification is performed on the entire fips_module	Power on

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					firmware image	
SHA2-384	32-bit message	KAT	CAST	Module is operational	Message digest	Module initialization (before firmware integrity test)
RSA SigVer (FIPS186-5)	PSS using 4096-bit key with SHA2-384	KAT	CAST	Module is operational	Signature verification	Module initialization (before firmware integrity test)

Table 18: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Stage 1 bootloader firmware integrity test	Signature verification	SW/FW Integrity	On demand	By resetting the module
fips_module firmware integrity test	Signature verification	SW/FW Integrity	On demand	By resetting the module

Table 19: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Stage 1 bootloader firmware load test	Signature verification	SW/FW Load	On demand	By resetting the module
fips_module firmware load test	Signature verification	SW/FW Load	On demand	By resetting the module
SHA2-384	KAT	CAST	On demand	By resetting the module
RSA SigVer (FIPS186-5)	KAT	CAST	On demand	By resetting the module

Table 20: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Secure Boot Error	An error occurred while loading the stage 1 bootloader or fips_module firmware	Firmware load test error	Resetting the module	The SoC does not boot

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Conditions	Recovery Method	Indicator
Self-Test Error	A self-test in the fips_module firmware failed	SHA2-384 CAST error RSA CAST error fips_module firmware integrity test error Stage 1 bootloader firmware integrity test error	Resetting the module	Error code AA0000FB, AA0000FC, AA0000FD, or AA0000FE

Table 21: Error States

In the error state, the module halts its execution, no input or output is possible at all. The error code is output through the FW status register, which explains the error that has occurred.

10.5 Operator Initiation of Self-Tests

All self-tests can be invoked on demand by resetting the module.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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.

These procedures install the module's associated firmware. The module's hardware and Boot ROM components are part of the SoC and need no installation. Its two firmware components are stored in SPI flash outside the SoC as part of the platform BIOS image. Steps 1 and 2 place the firmware in the BIOS image, and step 3 enables the FIPS capability. On startup the module's Boot ROM automatically loads the firmware components into SRAM as shown in Figure 2.

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

To enable the FIPS capability

1. Reserve 16KiB at least for AMD Secure Processor level 1 directory, as the FIPS module requires an additional 8KiB of ROM space for the AMD Secure Processor L1 Bootloader.
2. The Platform BIOS must include the file with "_FIPS" postfix in the file name as AMD Secure 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 AMD Secure 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 AMD Secure Processor boot loader.
3. Set BIT 32 of AMD Secure Processor soft fuse chain (AMD Secure Processor entry 0xB) to enable FIPS capability.
    a. The BIT32 in AMD Secure 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).

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 not installed.

11.2 Administrator Guidance

All the functions, ports and logical interfaces described in this document are available to the Crypto Officer. 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.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

11.4 Design and Rules

Not applicable.

11.5 Maintenance Requirements

There are no maintenance requirements.

11.6 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 previously, the module does not possess persistent storage of SSPs. The SSP values only exist in volatile memory and those values vanish 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. As a result of this sanitization via power-off, the SSPs are removed from the module, so that the module may either be distributed to other operators or disposed.

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

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

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

A Glossary and Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
ASP	AMD Secure Processor
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCP	Cryptographic Co-Processor
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
ECB	Electronic Code Book
HSTI	(Microsoft) Hardware Security Test Interface
FIPS	Federal Information Processing Standards
KAT	Known Answer Test
NIST	National Institute of Science and Technology
PSP	Public Security Parameter
PSS	Probabilistic Signature Scheme
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SoC	System on Chip
SRAM	Static Random-Access Memory
SSP	Sensitive Security Parameter

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

B References

FIPS 140-3	FIPS PUB 140-3 - Security Requirements For Cryptographic Modules March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS 140-3 IG	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf
FIPS 180-4	Secure Hash Standard (SHS) August 2015 https://doi.org/10.6028/NIST.FIPS.180-4
FIPS 186-5	Digital Signature Standard (DSS) February 2023 https://doi.org/10.6028/NIST.FIPS.186-5
SP 800-140Br1	Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B November 2023 https://doi.org/10.6028/NIST.SP.800-140Br1

© 2026 Advanced Micro Devices (AMD), atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.