Microsoft Corporation
FIPS 140-3 Security Policy

(Non-Proprietary)

Pluton™ Security Processor ROM

Ryzen 7 Pro 6850H with Radeon Graphics
Rembrandt B1 = 0x8262_0B00

Prepared By	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399
Document Version Number	1.1
Updated On	November 1, 2024

COPYRIGHT AND DISCLAIMER

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Microsoft, Pluton security processor, Azure, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Version history

Document Version	Date	Description
1.0	May 13, 2022	Draft submitted to CMVP for a full validation.
1.1	November 1, 2024	Updated in response to CMVP feedback.

1. General

Microsoft's Pluton™ Security Processor Read-Only Memory (ROM) module (the "module", or "Pluton ROM") is a sub-chip cryptographic subsystem in the AMD Ryzen 6000 Series System on a Chip (SOC). The module is a single chip hardware module that implements FIPS 140-3 approved cryptographic algorithms.

This document is the FIPS 140-3 Security Policy for the module. It contains a specification of the rules under which the module must operate and describes how the module meets security requirements as specified in ISO/IEC 19790:2012 and the Federal Information Processing Standards Publication 140-3 (FIPS PUB 140-3) for a Security Level 2 module, when achieving its primary functional objective. This document is intended for the FIPS 140-3 testing lab, the Cryptographic Module Validation Program (CMVP), and administrators and users of the module.

1.1. Security Level

The overall security level that this module is validated at is Level 2. The following table lists the security levels of individual areas for this validation, as required by the CMVP Security Policy Requirements (NIST SP 800-140B), ISO/IEC 19790 Annex B, and ISO/IEC 24759 section 6.14.

ISO/IEC 24759 Section 6. [Number Below]	**FIPS 140-3 Section Title**	**Security Level**
1	General	Level 2
2	Cryptographic module specification	Level 2
3	Cryptographic module interfaces	Level 2
4	Roles, services, and authentication	Level 2
5	Software/Firmware security	Level 2
6	Operational environment	N/A
7	Physical security	Level 2
8	Non-invasive security	N/A
9	Sensitive security parameter management	Level 2
10	Self-tests	Level 2
11	Life-cycle assurance	Level 2
12	Mitigation of other attacks	N/A

Table 1: Security Levels

2. Cryptographic Module Specification

2.1. Module Description

The primary functional objective of the Pluton™ Security Processor ROM module is to validate digitally signed files before they are imported into the Pluton Security Processor. The module and the Pluton Security Processor are embedded security subsystems within AMD's SOC silicon die. While the module incorporates other hardware elements, the following on-die design blocks are relevant to the primary functional objective of the module.

- The ARM Cortex R4 processor, which is configured to boot from the Pluton image at a specific address in the ROM.
- The Pluton ROM image, which is compiled by its developer before the Graphic Data System (GDS) Integrated Circuits (IC) layout of the SOC is finalized and fabricated.
- The Pluton ROM, to which the compiled Pluton image is written as part of the process to complete the SOC GDS IC layout.
- Pluton RAM, which provides runtime temporary stack or data spaces exclusive to the R4 processor when the R4 processor is executing the Pluton image.
- The Pluton AES engine, which is a hardware implementation of the AES block cipher for encryption and decryption of data.
- The Pluton SHA engine, which is a hardware implementation for performing hashing operations in authenticating and checking the integrity of blocks of data.
- The Pluton Public Key Acceleration (PKA) engine, which provides hardware acceleration to perform prime finite field arithmetic functions autonomously to support ECC public key operations.

2.2. Modes of Operation

The mode in which the module operates is implicitly the approved mode. The module has only an approved mode and, therefore, all services are approved services.

2.3. Operational Environments and Configurations

The module resides in all AMD Ryzen 6000 Series SOCs, regardless of SKU or model. This is a non-modifiable operational environment. The Ryzen 6000 Series includes multiple SKUs, e.g. Ryzen 3, Ryzen 5, Ryzen 7, and Ryzen 9, among others. The specific SKU and model used for testing in this validation is identified in the table below. Apart from the Pluton ROM image, the rest of the module is comprised of integrated circuits fabricated on silicon dies as hardware components.

Model	Hardware Part # and Version	Firmware Version	Distinguishing Features
AMD Ryzen 6000 Series SOC	Model Ryzen 7 Pro 6850H with Radeon Graphics	Rembrandt B1 = 0x8262_0B00	CPUID F.4.1 Extended CPUID 19.44

Table 2: Cryptographic Module Tested Configuration

The following photograph shows the specific AMD Ryzen 6000 Series, Model 7 Pro 6850H with Radeon Graphics.

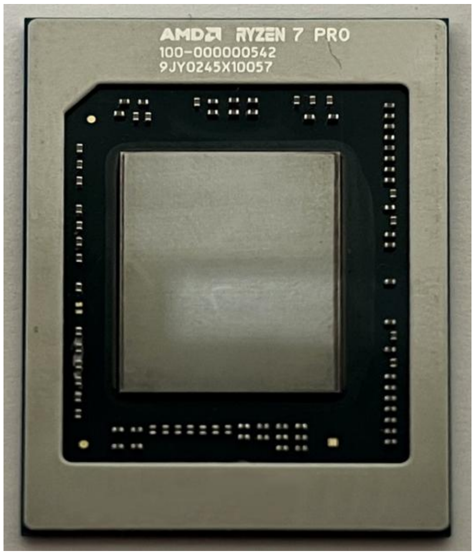

Figure 1: Processor Photograph

2.4. Algorithms and Security Functions

The following tables present the cryptographic algorithms and security functions used in the module in its single mode of operation. Table 3 lists the FIPS 140-3 approved algorithms used in the module, and tables 4-5 list the non-approved algorithms that may be used in certain modes of operation in the module.

CAVP Certificate #	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2348	ECDSA SigVer (FIPS 186-4)	Signature Verification	P-384 curve with SHA2-256.	Signature Verification
A2348	SHA2-256 (FIPS 180-4)	SHA2-256	Message length: 0-51200, increment 8.	Secure Hashing

Table 3: Approved Algorithms

Algorithm	Caveat	Use / Function
N/A (The module implements only approved algorithms.)		

Table 4: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use / Function
N/A (The module implements only approved algorithms.)		

Table 5: Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm / Function	Use / Function
N/A (The module implements only approved algorithms.)	

Table 6: Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.5. Cryptographic Boundaries

The module's physical boundary per IG 2.3.B is the physical perimeter of the AMD SOC. Consequently, the module qualifies as a single-chip cryptographic module. As a Sub-Chip Cryptographic Subsystem, the cryptographic boundary consists of the circuitry cores of sub-chip cryptographic subsystem and the Hardware Module Interface (HMI) interfaces documented in Section 3 of this document. Figure 2 visualizes the cryptographic boundary of the module, and Figure 3 provides a photograph of the physical boundary of the SOC.

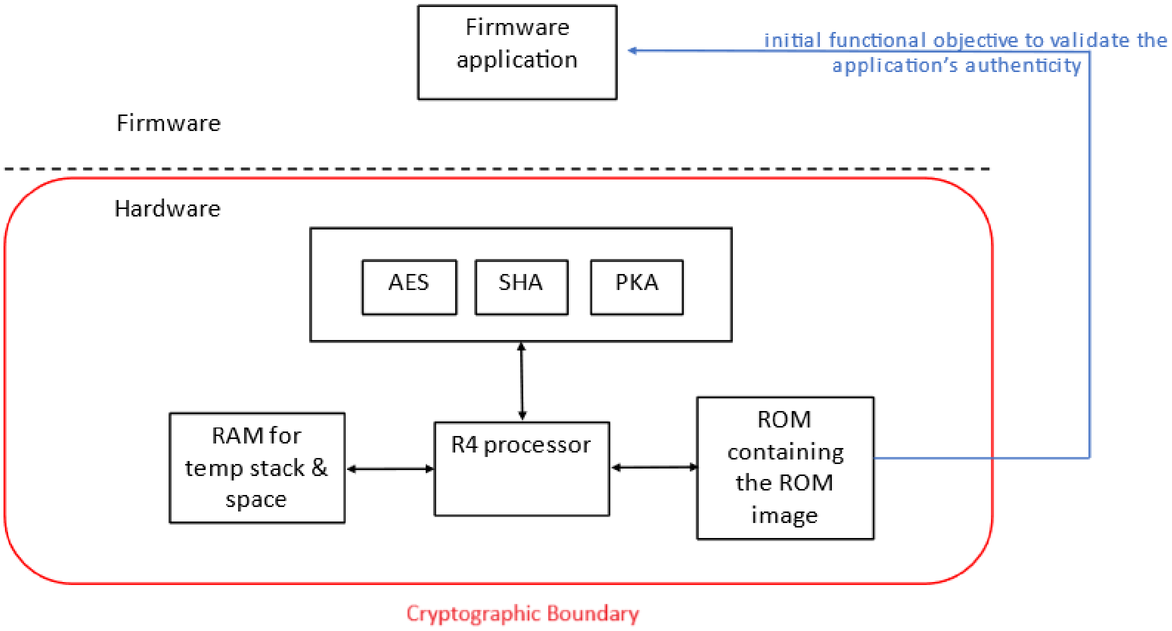
Firmware application
initial functional objective to validate the application's authenticity
Firmware
Hardware
AES
SHA
PKA
RAM for temp stack & space
R4 processor
ROM containing the ROM image
Cryptographic Boundary

Figure 2: Cryptographic Boundary (HMI)

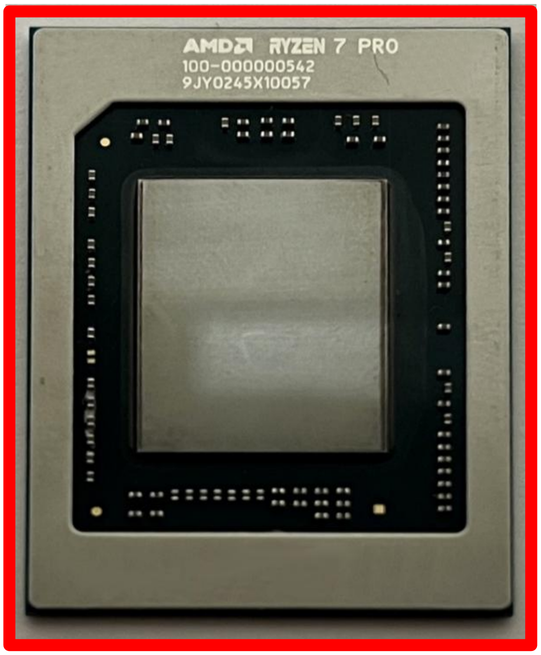

Figure 3: Photograph of the SOC with Red Overlay Identifying the Physical Boundary

The module's primary functional objective is to validate the SHA2-256 ECDSA P-384 signature of a firmware application. If the signature is valid, the firmware application may be imported and loaded into the Pluton RAM for the R4 processor to execute. (Note that the module itself contains no firmware per CMVP definitions.) As a result, firmware applications remain outside of the FIPS cryptographic boundary. No components within the boundary are excluded from the security requirements. All information processed by the component is strictly for internal use of the module towards its security function and does not impact the secure operation of the module or the correctness of control, status, or data outputs. The inclusion of specific firmware applications would be the subject of another validation under CMVP which extends the module's current functionality and CMVP validation assessment verdicts.

2.6. Design and Rules of Operation

The module is a sub-chip embedded in the AMD Ryzen 6000 Series SOC, which is a single-chip standalone device. The primary functional objective of the hardware module is to validate digitally signed files before they are imported into the module. The module is an embedded security subsystem within AMD's SOC. No user installation or maintenance is required. The FIPS 140-3 functional requirements are always invoked when the validated hardware version listed is used. The other sections of this document provide additional details on the design of the module and rules for its operation.

3. Cryptographic Module Interfaces

As indicated in the table below, all status and control ports are accessed through the Pluton registers and the API command handlers implemented in the Pluton ROM image. For data input, direct access to memory through the address spaces maintained by the Pluton registers and the API command handlers implemented in the Pluton ROM image are used. This direct access to memory, the Pluton registers, and API commands defines the FIPS interfaces across the module's cryptographic boundary. Error statuses available through these interfaces do not reveal any sensitive materials to the interface initiators.

Physical Port	Logical Interface	Data that Passes over the Port / Interface
Direct access of memory, registers	Data Input	Hard-coded ECDSA Signature (PSP) used for verification of firmware image, measurements.
Registers	Control Input	Platform Configuration Register (PCR) numbers.
Registers	Status Output	Return and error codes.

Table 7: Ports and Interfaces

4. Roles, Services, and Authentication

The module supports a single role, Crypto Officer, which may use any of the module's services. The Crypto Officer role is implicitly assumed by the party accessing services implemented by the Module. There is no non-Crypto Officer role in approved mode. The module does not support cryptographic bypass.

The following table identifies all services offered in each role, with corresponding input and output.

Role	Service	Input	Output
Crypto Officer	Show Status	Automatically executed by the module.	Status output across the module's Status Output logical interface.

Role	Service	Input	Output
Crypto Officer	Perform Self-Tests	Automatically executed by the module after every power on or reset.	Implicit in Module availability: if the Module is available, the self-tests have passed; if the self-tests fail, the Module resets.
Crypto Officer	Load Firmware	Executed when the “load firmware” command is received; firmware address and size is passed in.	Firmware application ECDSA signature is validated.
Crypto Officer	Decommission	Executed when the “disable Pluton” command is received.	Permanently changes the module state to end of life.
Crypto Officer	PCR3 Extend	Executed when the “PCR3 extend” command is received, with value and software PCR number is passed in.	Extends PCR number 3 with passed-in data.
Crypto Officer	All PCR Extend	Executed when the “all PCR extend” command is received.	Extends all PCRs with a hard-coded, fixed value.
Crypto Officer	Show Module’s Versioning Information	Implicit by the AMD SOC the module resides within.	CPUID indicated in Table 2.

Table 8: Roles, Service Commands, Input, and Output

Details on authentication methods are N/A as the module does not provide authentication of users and is not required to as the module services that access approved security functions fall into the categories of FIPS 180-4 hash algorithms and FIPS 186-4 digital signature verification, per IG 4.1.A.

The following table identifies the approved services of the module. The module does not include a zeroization service because the single SSP accessed by the module (ECDSA public key used for firmware signature verification) is a Public Security Parameter (PSP) that is hardcoded in the ROM code. This PSP is immutable and thus is considered protected.

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Role(s)	Access Rights to Keys or SSPs	Indicator
Show Status	Shows module status.	N/A	None	Crypto Officer	N/A	Implicit in SOC availability. An error in module will result in the SOC failing to boot.
Perform Self-Tests	Performs module self-tests.	SHA2-256 (FIPS 180-4) and ECDSA SigVer (FIPS 186-4)	None	Crypto Officer	N/A	Implicit in module availability. If the SHA2 self-test fails, the module halts and no cryptographic function may be performed. For ECDSA, a failure status returned to the platform processor of the AMD SOC.

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Role(s)	Access Rights to Keys or SSPs	Indicator
Load Firmware	Validates a firmware application ECDSA signature.	ECDSA SigVer (FIPS 186-4)	ECDSA public key	Crypto Officer	R, E	LoadRuntime succeeds and the module generates a postcode that digital signature validation succeeded.
Decommission	Permanently changes the module state for decommissioning.	N/A	None	Crypto Officer	N/A	HSP state is changed and will reject any commands like LoadRuntime or PcrExtend.
PCR3 Extend	Extends the Platform Configuration Register (PCR) number 3 with passed-in data.	SHA2-256 (FIPS 180-4)	None	Crypto Officer	N/A	PCR3 extended with passed-in data.
All PCR Extend	Extends all PCRs with a hard-coded, fixed value.	SHA2-256 (FIPS 180-4)	None	Crypto Officer	N/A	PCR3 extended with hard-coded fixed value.

Service	Description	Approved Security Function(s)	Keys and/or SSPs	Role(s)	Access Rights to Keys or SSPs	Indicator
Show Module's Versioning Information	Show module's versioning information.	N/A	None	Crypto Officer	N/A	CPUID matching those indicated in Table 2.

Table 9: Approved Services

G = Generate: The module generates or derives the SSP.
R = Read: The SSP is read from the module (e.g. the SSP is output).
W = Write: The SSP is updated, imported, or written to the module.
E = Execute: The module uses the SSP in performing a cryptographic operation.
Z = Zeroise: The module zeroises the SSP.

The module implements only approved services.

5. Software/Firmware Security

The module's executable code is stored in non-reconfigurable memory on the SOC, as defined by FIPS 140-3 IG 5.A. The SOC non-reconfigurable memory will not change or degrade for a minimum of 10 years, guaranteeing firmware security. This design requires no integrity testing.

As a sub-chip embedded in the AMD SOC, the module is expected to last the lifetime of the SOC. The non-reconfigurable memory of the SOC should not degrade for at least 10 years. The module and SOC are determined to be end-of-life at the discretion of the user within this period. At end-of-life, the user should discontinue use of the SOC. As the module does not generate, establish, or import any CSPs, no sanitization process is required.

6. Operational Environment

The Operational Environment requirements do not apply, as the module's operational environment is non-modifiable and the physical security level claimed is Level 2. Apart from the Pluton ROM image, the rest of the module is comprised of integrated circuits fabricated on silicon dies as hardware components. The Pluton ROM image is non-modifiable as it is written to the SOC as part of the process to complete the SOC GDS IC layout before wafer fabrication. The module cannot be modified and no code can be added or removed.

7. Physical Security

The module is a sub-chip embedded in the AMD Ryzen 6000 Series SOC, which is a single-chip standalone device. The module is embedded in all AMD Ryzen 6000 SOC models and SKUs. The SOC conforms to the FIPS 140-3 Level 2 requirements for physical security. The SOC resides in a package which provides opaqueness in the visible spectrum and protection against environmental or other physical damage. It is contained in a tamper-evident enclosure which deters direct observation, probing, or manipulation and provides evidence of attempts to tamper with or remove the module. No operator-applied tamper evident seals or security appliances are required, as the seals are applied as part of manufacturing the SOC. The following table identifies the physical security mechanisms of the module and the protocol for maintaining them.

Physical Security Mechanism	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Tamper-evident enclosure	Inspect whenever the user is concerned they have lost physical control of the computer with the Pluton processor.	Examine the SOC for scratched or damaged epoxy coating. If tampering is evident, the user may contact Microsoft at FIPS@microsoft.com.

Table 10: Physical Security Inspection Guidelines

The following photographs show the tamper-evident enclosure. The image at left shows the module before tampering, with the epoxy tamper-evident enclosure intact. In the image at right, the epoxy tamper-evident enclosure shows tampering.

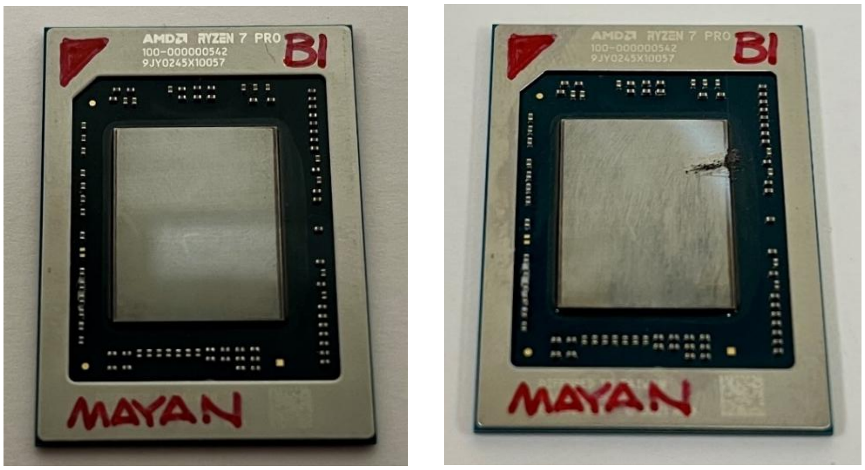

Figure 4: Module before Tampering (Left) and after Tampering (Right)

As a Level 2 module that does not implement EFP/EFT, the module is not subject to hardness testing.

8. Non-Invasive Security

The module does not implement non-invasive attack mitigation techniques to protect the unprotected SSPs from non-invasive attacks.

9. Sensitive Security Parameters Management

The module does not generate, establish, or import any critical security parameters (CSPs). The ECC public key used for firmware application signature verification is a Public Security Parameter (PSP) that is hardcoded in the ROM code. This PSP is immutable and thus is considered protected.

Key / SSP Name / Type	Strength	Security Function and Cert. Number	Generation	Import / Export	Establishment	Storage	Zeroization	Use and Related Keys
ECDSA Public Key (SHA2-256)	P-384 (192 bits)	ECDSA SigVer (FIPS 186-4), certificate #A2348.	Pre-loaded by the manufacturer.	N/A	N/A	Hard-coded in immutable memory.	N/A	Firmware application signature verification.

Table 11: SSPs

The module does not implement non-deterministic random number generation.

10. Self-Tests

10.1. Pre-Operational Self-Tests

The module does not perform pre-operational self-tests and is not required to per IG 5.A, as explained in section 5 Software/Firmware Security.

10.2. Conditional Self-Tests

The module runs conditional cryptographic algorithm self-tests during its crypto subsystem initialization after every power on or reset. No operator intervention is required. The following conditional cryptographic algorithm tests are included.

- SHA2-256 Known Answer Test.
- AES-128 encrypt ECB Known Answer Test (only used for self-test).
- AES-128 decrypt ECB Known Answer Test (only used for self-test).

If these self-tests succeed, the module becomes operational and waits for commands from the platform processor of the AMD SOC. If any self-test fails, the module halts and no cryptographic function may be performed. To recover from the halt and to re-initialize the module, either a power off / power on cycle or a reset event must be triggered from outside the module.

Upon receiving the “load firmware” command from the platform processor of the AMD SOC, the module automatically performs the following conditional cryptographic algorithm self-test.

- ECDSA Signature Verification Known Answer Test on P-384 curve with SHA2-256

The test must pass before the module will perform firmware application signature verification. The test data, key-pair, and signature used in this known answer test are hard-coded in the ROM. If the self-test succeeds, the firmware application image inferred by the “load firmware” command is loaded to the Pluton RAM. The handler of the “load firmware” command inside the module validates the SHA2-256 ECDSA P-384 signature of the firmware application. If the signature is valid, the handler jumps out of the ROM image and passes the R4 processor execution control to the firmware application. If the self-test fails or the firmware application signature is not valid, the handler returns a failure status to the platform processor of the AMD SOC, and the module returns to its ready state. At that point, the platform processor stops sending commands to the module and may trigger a power off / power on cycle, a reset event, or a retry using a firmware image from the recovery portion.

10.3. Error States

The following diagram presents the finite state model for the module, including all module states.

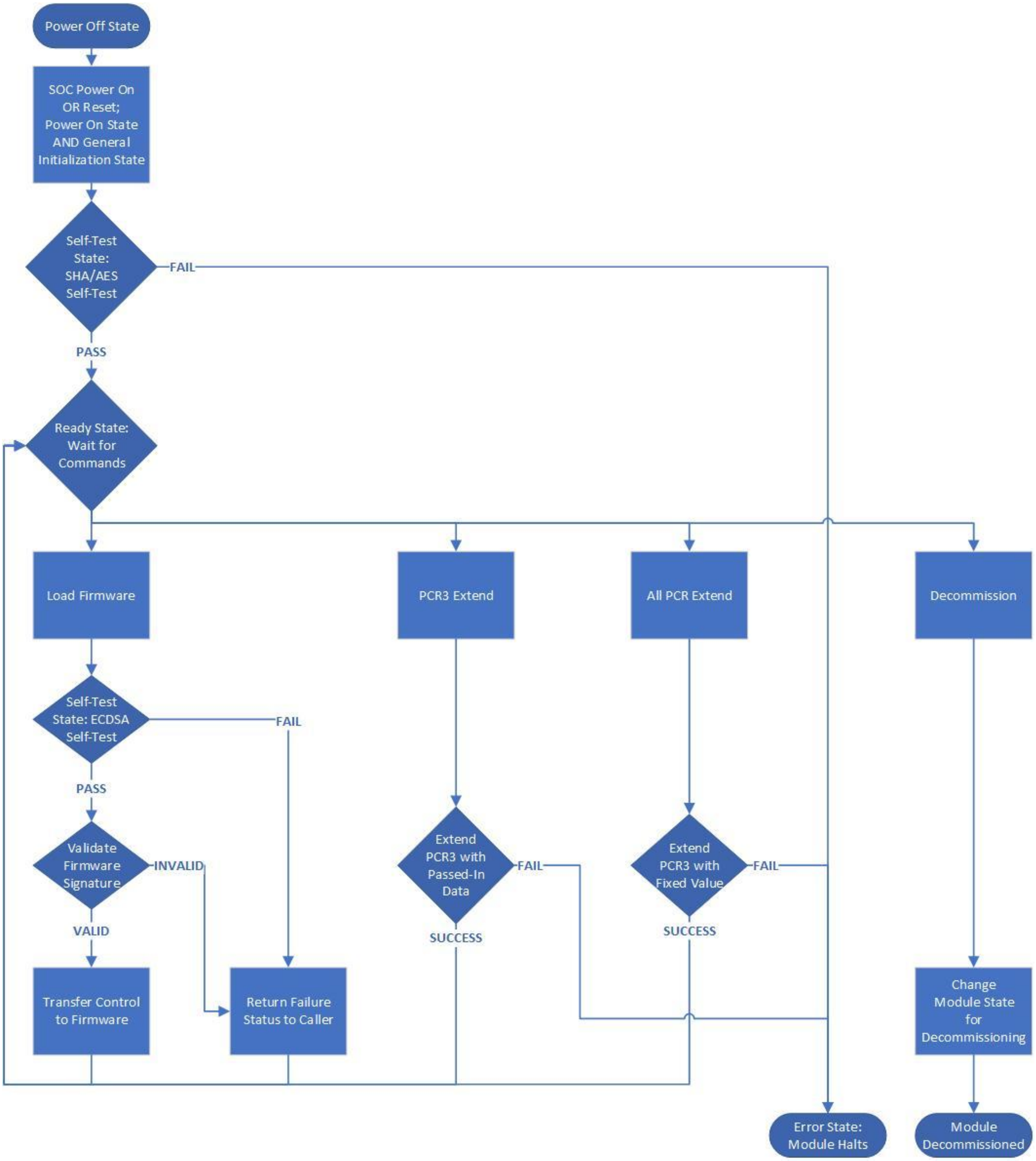
Power Off State
SOC Power On OR Reset; Power On State AND General Initialization State
Self-Test State: SHA/AES Self-Test
FAIL
PASS
Ready State: Wait for Commands
Load Firmware
PCR3 Extend
All PCR Extend
Decommission
Self-Test State: ECDSA Self-Test
FAIL
PASS
Validate Firmware Signature
INVALID
VALID
Extend PCR3 with Passed-In Data
FAIL
SUCCESS
Extend PCR3 with Fixed Value
FAIL
SUCCESS
Transfer Control to Firmware
Return Failure Status to Caller
Change Module State for Decommissioning
Error State: Module Halts
Module Decommissioned

Figure 5: Finite State Model Diagram

The states depicted in the finite state diagram map to the required operational and error states as follows.

- **Power On/Off state**: The module is in a Power Off state until power is applied to the underlying SOC platform, at which point the module enters the Power On state shown in the diagram. There is a single power source and no standby or hibernation state.

- **General Initialization state**: This is the same state as the Power On state, as shown in the finite state diagram. There is no additional action taken by the module between power on and self-test.

- **Approved state**: All approved services are available in the approved state, as shown in the diagram: Load Firmware, PCR3 Extend, All PCR Extend, and Decommission. As the Crypto Officer role is the only role implemented, the approved state is equivalent to a Crypto Officer state.

- **CSP entry state**: This state is N/A for this module as it does not support CSP entry.

- **User state**: This state is N/A for this module as no User role is implemented.

- **Self-test state**: The module is in a self-test state at two points pictured in the finite state diagram: immediately after power on, shown as the SHA/AES self test state, and after the load firmware command is handled, shown as the ECDSA self test state.

- **Error state**: The module is in an error state at two points pictured in the diagram: when a hard error is encountered, shown as Error State: Module Halts, and when a soft error is encountered, shown as Return Failure Status to Caller. When the module halts due to a hard error, a power cycle / reset must be triggered to re-initialize the module.

11. Life-Cycle Assurance

11.1. Crypto Officer Guidance

The operation of the module does not need FIPS 140-3 specific guidance. The FIPS 140-3 functional requirements are always invoked. The module is determined to be a FIPS 140-3 validated module by using the validated product described in this Security Policy. No Crypto Officer installation or maintenance is required.

11.2. User Guidance

The operation of the module does not need FIPS 140-3 specific guidance. The FIPS 140-3 functional requirements are always invoked. The module is determined to be a FIPS 140-3 validated module by using the validated product described in this Security Policy. No User installation or maintenance is required.

12. Mitigation of Other Attacks

The module does not claim any mitigation of other attacks.