

NVIDIA Corporation

NVIDIA Vera PSC Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:

NVIDIA Corporation
2788 San Tomas Expressway
Santa Clara, CA 95051

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759

Document Version 1.0
Date: November 19, 2026

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 8
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 9
2.7 Algorithm Specific Information 10
2.7.1 SP 800-208 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 14
5 Software/Firmware Security 15
5.1 Integrity Techniques 15
5.2 Initiate on Demand 15
6 Operational Environment 16
6.1 Operational Environment Type and Requirements 16
7 Physical Security 17
7.1 Mechanisms and Actions Required 17
8 Non-Invasive Security 18
9 Sensitive Security Parameters Management 19

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.1 Storage Areas 19
9.2 SSP Input-Output Methods 19
9.3 SSP Zeroization Methods 19
9.4 SSPs 19
10 Self-Tests 21
10.1 Pre-Operational Self-Tests 21
10.2 Conditional Self-Tests 21
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 End of Life 23
12 Mitigation of Other Attacks 24

© 2026 NVIDIA Corporation, 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 9
Table 4: Approved Algorithms 9
Table 5: Security Function Implementations 10
Table 6: Ports and Interfaces 11
Table 7: Roles 12
Table 8: Approved Services 13
Table 9: Mechanisms and Actions Required 17
Table 10: Storage Areas 19
Table 11: SSP Input-Output Methods 19
Table 12: SSP Zeroization Methods 19
Table 13: SSP Table 1 20
Table 14: SSP Table 2 20
Table 15: Conditional Self-Tests 21
Table 16: Conditional Periodic Information 21
Table 17: Error States 21

List of Figures

Figure 1: Block Diagram 7
Figure 2: TB500-P 8
Figure 3: TB500-M 8

© 2026 NVIDIA Corporation, 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 the NVIDIA Vera Platform Security Controller (PSC) 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 a Security Level 1 cryptographic 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

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

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	N/A
6	Operational environment	N/A
7	Physical security	2
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 NVIDIA Corporation, 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 NVIDIA Vera PSC Cryptographic Module (hereafter referred to as "the module") is defined as a sub-chip hardware module in a single-chip embodiment.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The module consists of a ROM component ("PSC-ROM"), a hardware accelerator ("PSC-SE"), and supporting components. These components are all located within the single-chip.

The block diagram in Figure 1 shows the design of the module when the ROM is loaded and the module is operational. In this diagram, the cryptographic boundary is represented by the components shown in orange. Dashed green lines show the logical interfaces listed in Section 3.

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter is the single-chip containing the module. The physical perimeter is represented by a dashed purple line in Figure 1. The chip is present in two packages, shown in Figure 2 and Figure 3.

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

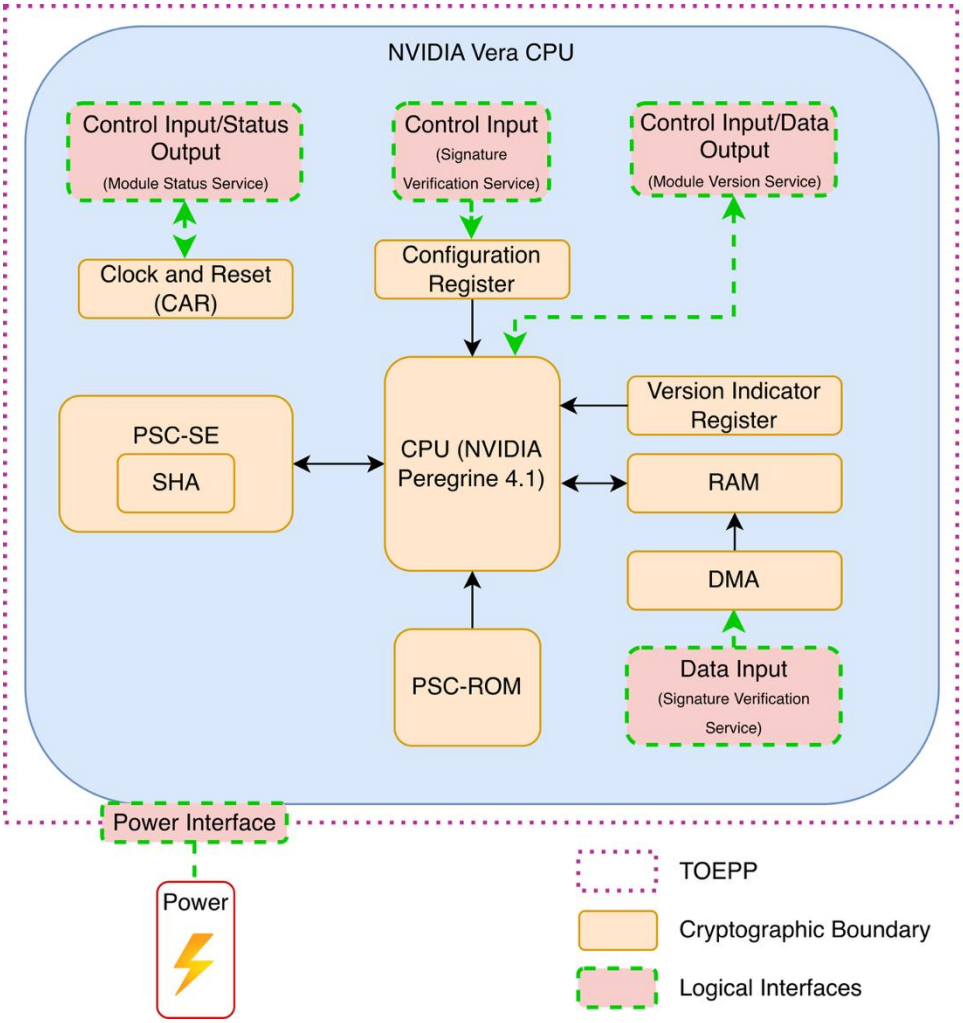
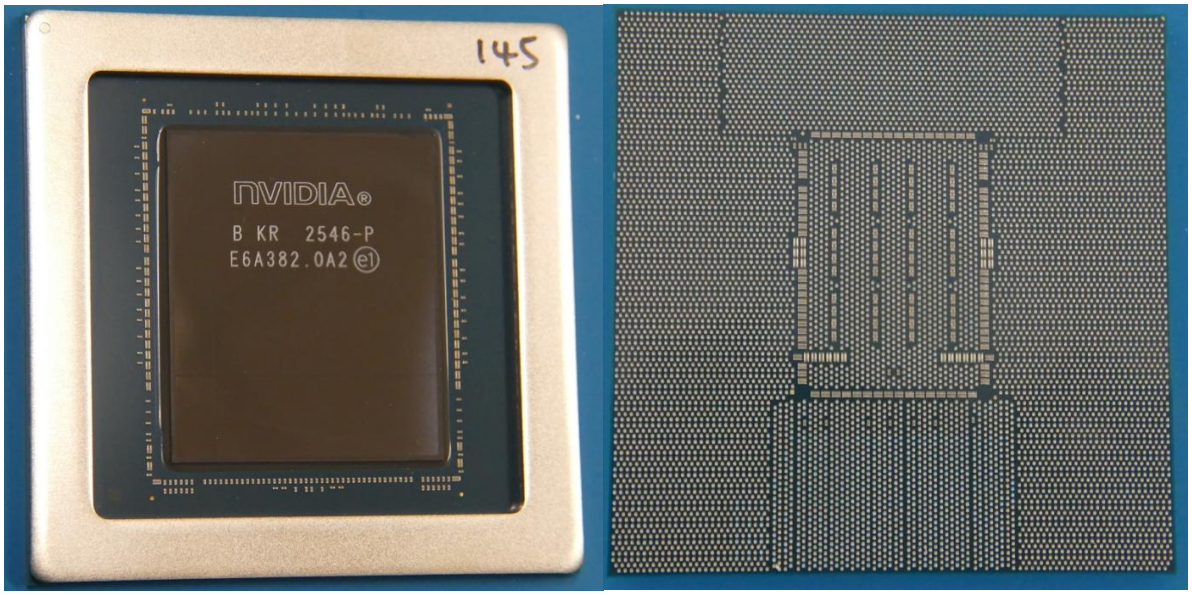


Figure 1: Block Diagram



© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Figure 2: TB500-P

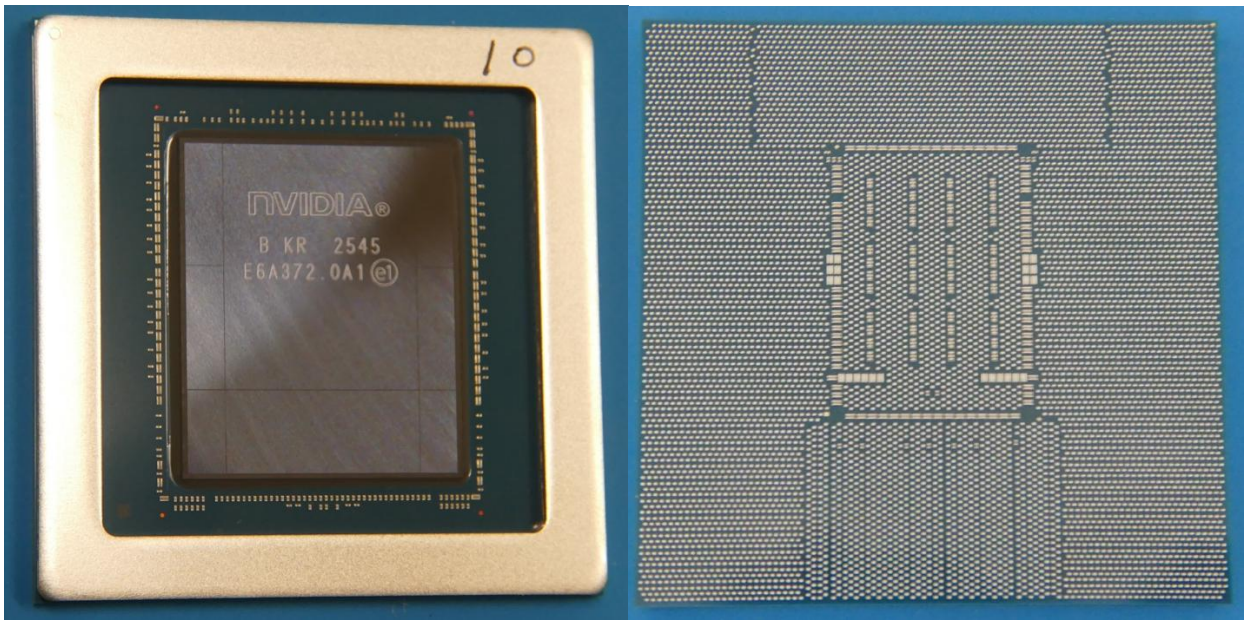


Figure 3: TB500-M

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Vera CPU (TB500-P)	0x00000014	N/A	NVIDIA Peregrine 4.1	N/A
Vera CPU (TB500-M)	0x00000014	N/A	NVIDIA Peregrine 4.1	N/A

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:

The module supports only the approved mode of operation. When the module starts up successfully, after passing all the pre-operational self-tests and conditional cryptographic algorithm self-tests (CASTs), the module is operating in the approved mode of operation.

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered after successful completion of the conditional cryptographic algorithm self-tests performed in lieu of the pre-operational integrity test, in accordance with AS10.19	Approved	Successful completion of service

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

The following table lists the approved algorithms implemented by the module, as well as the associated CAVP certificates.

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-5)	A7686	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
LMS SigVer	A7686	Specific Capabilities - LMS Modes - LMS_SHA256_M24_H20	SP 800-208
SHA2-256	A7543	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A7543	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:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
ECDSA Signature Verification	DigSig-SigVer	Signature verification using ECDSA		ECDSA SigVer (FIPS186-5):

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
				(A7686) SHA2-384: (A7543)
LMS Signature Verification	DigSig-SigVer	Signature verification using LMS		LMS SigVer: (A7686) SHA2-256: (A7543)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 SP 800-208

The module implements LMS signature verification as defined in SP 800-208. No other algorithms defined in SP 800-208 are implemented in the module. Per IG C.N Resolution 1, the module must therefore only comply with the requirements in Section 8.2 of SP 800-208.

In compliance with these requirements, the module implements exactly one LM-OTS parameter set (LMOTS_SHA256_N24_W4) and exactly one LMS parameter set (LMS_SHA256_M24_H20). The LM-OTS parameter set and the LMS parameter set supported by the module use the same hash function (SHA-256/192).

2.8 RBG and Entropy

The module does not implement or utilize a random number generator and does not contain an entropy source.

2.9 Key Generation

The module does not provide any key generation services.

2.10 Key Establishment

The module does not provide any key establishment services.

2.11 Industry Protocols

The module does not implement any industry protocols.

© 2026 NVIDIA Corporation, 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

The ports and interfaces implemented in the module are shown in the table below. No Control Output interface is present as no such interface is implemented in the module.

Physical Port	Logical Interface(s)	Data That Passes
Configuration Register	Control Input	Control signal to invoke service
Clock and Reset (CAR)	Control Input Status Output	Control signal to read module status, module status
CPU Registers	Data Output Control Input	Request to read Version Indicator Register, data from Version Indicator Register
DMA	Data Input	Signed data to be verified, public keys
Power Pins	Power	Power

Table 6: Ports and Interfaces

© 2026 NVIDIA Corporation, 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 support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 7: Roles

The Crypto Officer role is always implicitly assumed by the operator of the module. The module does not support concurrent operators.

4.3 Approved Services

The following convention is used to specify access rights to a SSP:

- **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 = Zeroize**: The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Signature Verification	Verify ECDSA and LMS signatures on First Mutable Code signed by NVIDIA (Stage 1) and OEM (Stage 2)	Success: The Clock and Reset interface status signal is low (0) upon successful Signature Verification and remains observable after the FMC is loaded and the module ceases operation. Failure: The Clock and Reset interface status signal is high (1), indicating Signature Verification failure and entry into the error state.	Signed First Mutable Code, Stage 2 public keys	Success (module ceases operation) or Fail (module enters Critical Error state)	ECDSA Signature Verification LMS Signature Verification	Crypto Officer - Stage 1 ECDSA Public Key: W,E - Stage 2 ECDSA Public Key: W,E - Stage 1 LMS Public Key: W,E - Stage 2 LMS

© 2026 NVIDIA Corporation, 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: W,E
Show Status	Logical signal read from Clock and Reset interface (0 indicates operational, 1 indicates error)	None	None	Module status	None	Crypto Officer
Show Version	Return the module version	None	None	Module version	None	Crypto Officer
Self-Test	Perform CASTs	None	None	Pass (services are available) or Fail (module enters Critical Error state)	ECDSA Signature Verification LMS Signature Verification	Crypto Officer
Zeroization	Zeroize unprotected SSPs in volatile memory	None	None	None	None	Crypto Officer - Stage 1 ECDSA Public Key: Z - Stage 2 ECDSA Public Key: Z - Stage 1 LMS Public Key: Z - Stage 2 LMS Public Key: Z

Table 8: Approved Services

4.4 Non-Approved Services

The module does not implement any non-approved services.

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.5 External Software/Firmware Loaded

The module does not support the loading of external software/firmware.

© 2026 NVIDIA Corporation, 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 ROM component of the module is stored in Mask ROM which meets the definition of Non-Reconfigurable Memory in IG 5.A. Data stored in this Mask ROM is guaranteed to not change or degrade for at least 10 years, exceeding the requirements of IG 5.A Resolution 1.

5.2 Initiate on Demand

Not applicable for this module.

© 2026 NVIDIA Corporation, 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: Non-Modifiable

The NVIDIA Vera PSC Cryptographic Module is a single-chip hardware module validated at Physical Security Level 2. The operational environment is non-modifiable.

© 2026 NVIDIA Corporation, 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	6 months	Verify chip package not compromised or tampered

Table 9: Mechanisms and Actions Required

The NVIDIA Vera PSC Cryptographic Module is a sub-chip enclosed in the NVIDIA Vera CPU, which is present in the packages shown in Figure 2 and Figure 3. These packages are made with production-grade components and conform to the Level 2 requirements for physical security.

At the time of manufacturing, the die is flip-chip attached to the package substrate with its active circuitry facing the substrate, making the internal circuitry neither visible nor accessible. The exposed bulk-silicon surface is opaque to visible light. Attempts to remove or penetrate the die are likely to damage the module and leave visible evidence, such as scratches, chips, or cracks. The die uses commercial-standard passivation.

© 2026 NVIDIA Corporation, 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 measures.

© 2026 NVIDIA Corporation, 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
ROM	Persistent storage for PSPs in non-reconfigurable memory (Mask ROM). Per IG 5.A Additional Comment 5, PSPs which are stored in non-reconfigurable memory are considered protected and are therefore not subject to zeroization requirements.	Static
RAM	Temporary storage for PSPs input to module	Dynamic

Table 10: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
DMA Input	Operator within TOEPP	RAM	Plaintext	Manual	Electronic	

Table 11: SSP Input-Output Methods

The module does not provide SSP output services. SSPs are provided by the operator within the tested operational environment's physical perimeter (TOEPP) via a single-chip TOEPP path, which is not considered SSP establishment by Table 1 of FIPS 140-3 IG 9.5.A.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off	SSPs in internal RAM and registers are zeroized	RAM and registers lose state upon loss of power	Operator powers off the module

Table 12: SSP Zeroization Methods

All data output is inhibited during zeroization.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Stage 1 ECDSA Public Key	Used as NVIDIA public key for Stage 1 signature verification on FMC using ECDSA P384	P-384 - 192 bits	Public Key - PSP	N/A (Pre-loaded in PSC-ROM)		ECDSA Signature Verification
Stage 2 ECDSA	Used as OEM public key for Stage 2 signature	P-384 - 192 bits	Public Key - PSP			ECDSA Signature Verification

© 2026 NVIDIA Corporation, 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
Public Key	verification on FMC using ECDSA P384					
Stage 1 LMS Public Key	Used as NVIDIA public key for Stage 1 signature verification on FMC using LMS with SHA-256/192	384 bits (LMS/LMOTS with M/N=24) - 192 bits	Public Key - PSP	N/A (Pre-loaded in PSC-ROM)		LMS Signature Verification
Stage 2 LMS Public Key	Used as OEM public key for Stage 2 signature verification on FMC using LMS with SHA-256/192	384 bits (LMS/LMOTS with M/N=24) - 192 bits	Public Key - PSP			LMS Signature Verification

Table 13: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Stage 1 ECDSA Public Key		RAM:Plaintext ROM:Plaintext	RAM: until module power-off. ROM: Lifetime of the module. Considered protected due to ROM non-degradation (IG 5.A Additional Comment #5)	Power-off N/A	
Stage 2 ECDSA Public Key	DMA Input	RAM:Plaintext	Until module power-off	Power-off	
Stage 1 LMS Public Key		RAM:Plaintext ROM:Plaintext	RAM: until module power-off. ROM: Lifetime of the module. Considered protected due to ROM non-degradation (IG 5.A Additional Comment #5)	Power-off N/A	
Stage 2 LMS Public Key	DMA Input	RAM:Plaintext	Until module power-off	Power-off	

Table 14: SSP Table 2

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

All firmware in the module is stored in non-reconfigurable memory as defined in IG 5.A and is thus considered protected. Therefore, the module does not perform any pre-operational integrity tests. Instead, the conditional tests listed in the following section are performed prior to the module becoming operational.

10.2 Conditional Self-Tests

Each KAT involves the comparison of the calculated output of a cryptographic algorithm with a known answer hardcoded into the module. All KATs are automatically performed by the module at power-on before the module becomes operational. All data output is inhibited until all self-tests have completed successfully.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A7686)	P-384, SHA2-384	KAT	CAST	Module becomes operational	Signature Verification	Test runs at power-on
LMS SigVer (A7686)	LMS_SHA256_M24_H20, LMOTS_SHA256_N24_W4	KAT	CAST	Module becomes operational	Signature Verification	Test runs at power-on

Table 15: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A7686)	KAT	CAST	On Demand	Manually
LMS SigVer (A7686)	KAT	CAST	On Demand	Manually

Table 16: Conditional Periodic Information

10.4 Error States

If the module fails any conditional self-test or the Signature Verification service fails to verify the signature on the provided firmware, the module will enter the error state. When entering the error state, the module immediately initiates a reset during which all data output is inhibited and no requests can be processed.

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	Error state	CAST Failure Signature Verification Failure	Module Reset	Module resets automatically on error

Table 17: Error States

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.5 Operator Initiation of Self-Tests

On-demand self-tests can be invoked by power-cycling the module. This causes the module to perform all conditional cryptographic algorithm self-tests.

© 2026 NVIDIA Corporation, 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 module is pre-configured to operate as a validated module. No additional configuration of the module or installation steps are required from the operator.

11.2 Administrator Guidance

All the functions, ports, and logical interfaces described in this Security Policy are available to the Crypto Officer. There are no special procedures to administer the module.

11.3 Non-Administrator Guidance

There is no non-administrator guidance.

11.4 End of Life

All SSPs stored persistently in the module are PSPs stored in non-reconfigurable memory and are considered protected by IG 5.A Additional Comment 5.

To securely sanitize the module, the operator must first power off the module, which will erase all SSPs in volatile memory. The operator is then responsible for disposing of, decommissioning, or returning the device containing the module.

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

The NVIDIA Vera PSC Cryptographic Module does not claim any security mechanisms to mitigate other attacks.

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix A. Glossary and Abbreviations

CAR	Clock and Reset
CAST	Cryptographic Algorithm Self-Test
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DMA	Direct Memory Access
ECDSA	Elliptic-Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards Publication
FMC	First Mutable Code
FSM	Finite State Model
KAT	Known Answer Test
LM-OTS	Leighton-Micali One-Time Signature
LMS	Leighton-Micali Signature
NIST	National Institute of Science and Technology
OEM	Original Equipment Manufacturer
PSC	Platform Security Controller
PSC-ROM	Platform Security Controller Read-Only Memory
PSC-SE	Platform Security Controller Security Engine
PSP	Public Security Parameter
RAM	Random-Access Memory
RBG	Random Bit Generator
ROM	Read-Only Memory
SFI	Security Function Implementation
SHA	Secure Hash Algorithm
SoC	System on a Chip
SSP	Sensitive Security Parameter
TOEPP	Tested Operational Environment's Physical Perimeter

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

Appendix 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**
April 2026
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

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

SP800-208 **Recommendation for Stateful Hash-Based Signature Schemes**
October 2020
https://doi.org/10.6028/NIST.SP.800-208

SP800-140Br1 **NIST Special Publication 800-140Br1 - CMVP Security Policy Requirements**
November 2023
https://doi.org/10.6028/NIST.SP.800-140Br1

© 2026 NVIDIA Corporation, atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.