Nvidia Corporation

H100 Tensor Core GPU

Hardware Models: H100 FIPS-1; H100 FIPS-2
Firmware Version: 570.36

FIPS 140-3 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.12

Prepared for:

Nvidia Corporation
2788 San Tomas Expressway
Santa Clara, CA 95051
United States of America

Phone: +1 408 486-2000
www.nvidia.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-3 cryptographic module security policy. More information is available on the module from the following sources:

- The Nvidia website www.nvidia.com contains information on the full line of services and solutions from Nvidia.

- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

Document Organization

ISO/IEC 19790 Annex B uses the same section naming convention as *ISO/IEC 19790* section 7 - Security requirements. For example, Annex B section B.2.1 is named “General” and B.2.2 is named “Cryptographic module specification,” which is the same as *ISO/IEC 19790* section 7.1 and section 7.2, respectively. Therefore, the format of this Security Policy is presented in the same order as indicated in Annex B, starting with “General” and ending with “Mitigation of other attacks.” If sections are not applicable, they have been marked as such in this document.

Table of Contents

1. General 6
1.1 Overview 6
1.2 Security Levels 6

2. Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 9
2.3 Excluded Components 10
2.4 Modes of Operation 11
2.5 Algorithms 11
2.6 Security Function Implementations 14
2.7 Algorithm Specific Information 16
2.8 RBG and Entropy 17
2.9 Key Generation 17
2.10 Key Establishment 17
2.11 Industry Protocols 18

3. Cryptographic Module Interfaces 19
3.1 Ports and Interfaces 19

4. Roles, Services, and Authentication 20
4.1 Authentication Methods 20
4.2 Roles 20
4.3 Approved Services 20
4.4 Non-Approved Services 24
4.5 External Software/Firmware Loaded 25

5. Software/Firmware Security 26
5.1 Integrity Techniques 26
5.2 Initiate on Demand 26

6. Operational Environment 27
6.1 Operational Environment Type and Requirements 27
6.2 Configuration Settings and Restrictions 27

7. Physical Security 28
7.1 Mechanisms and Actions Required 28

8. Non-Invasive Security 29

9. Sensitive Security Parameters Management 30
9.1 Storage Areas 30
9.2 SSP Input-Output Methods 30
9.3 SSP Zeroization Methods 30
9.4 SSPs 31

10. Self-Tests 37
10.1 Pre-Operational Self-Tests 37

10.2 Conditional Self-Tests 37
10.3 Periodic Self-Test Information 40
10.4 Error States 41
10.5 Operator Initiation of Self-Tests 41

11. Life-Cycle Assurance 42
11.1 Installation, Initialization, and Startup Procedures 42
11.2 Administrator Guidance 42
11.3 Non-Administrator Guidance 43
11.4 End of Life 43

12. Mitigation of Other Attacks 44

Appendix A. Acronyms and Abbreviations 45

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 9
Table 3: Modes List and Description 11
Table 4: Approved Algorithms - Copy Engine 12
Table 5: Approved Algorithms - GPU Service Processor 12
Table 6: Approved Algorithms - Security Controller 12
Table 7: Approved Algorithms - Root of Trust for Storage 13
Table 8: Vendor-Affirmed Algorithms 13
Table 9: Non-Approved, Allowed Algorithms with No Security Claimed 14
Table 10: Security Function Implementations 16
Table 11: Entropy Certificates 17
Table 12: Entropy Sources 17
Table 13: Ports and Interfaces 19
Table 14: Authentication Methods 20
Table 15: Roles 20
Table 16: Approved Services 24
Table 17: Mechanisms and Actions Required 28
Table 18: Storage Areas 30
Table 19: SSP Input-Output Methods 30
Table 20: SSP Zeroization Methods 31
Table 21: SSP Table 1 33
Table 22: SSP Table 2 36
Table 23: Pre-Operational Self-Tests 37
Table 24: Conditional Self-Tests 40
Table 25: Pre-Operational Periodic Information 40
Table 26: Conditional Periodic Information 41
Table 27: Error States 41
Table 28: Acronyms and Abbreviations 45

List of Figures

Figure 1: Module Block Diagram (with Cryptographic Boundary) 8
Figure 2: Nvidia H100 Tensor Core GPU (Top View) 9
Figure 3: Nvidia H100 Tensor Core GPU (Bottom View) 9

1. General

1.1 Overview

This is a non-proprietary Cryptographic Module Security Policy for the H100 Tensor Core GPU (version: 570.36) from Nvidia Corporation (Nvidia). This Security Policy describes how the H100 Tensor Core GPU meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-3 validation of the module. The H100 Tensor Core GPU is referred to in this document as H100 or the module.

1.2 Security Levels

The H100 Tensor Core GPU is validated at the FIPS 140-3 section levels shown in the table below.

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

Table 1: Security Levels

The module has an overall security level of 2.

2. Cryptographic Module Specification

2.1 Description

2.1.1 Purpose and Use

H100 is part of the complete NVIDIA data center solution that incorporates building blocks across hardware, networking, software, libraries, and optimized AI models and applications from the NVIDIA NGC™ catalog. The second-generation Multi-Instance GPU (MIG), built-in NVIDIA confidential computing, and NVIDIA NVLink Switch System allows the H100 to securely accelerate workloads.

2.1.2 Module Type

The H100 Tensor Core GPU 570.36 is a Hardware module.

2.1.3 Module Embodiment

The H100 Tensor Core GPU is a Single Chip embodiment.

2.1.4 Module Characteristics

The module does not have any additional characteristics.

2.1.5 Cryptographic Boundary

The cryptographic boundary of the module is defined by the external edge of the chip casing.

Figure 1 illustrates a block diagram of the H100 GPU.

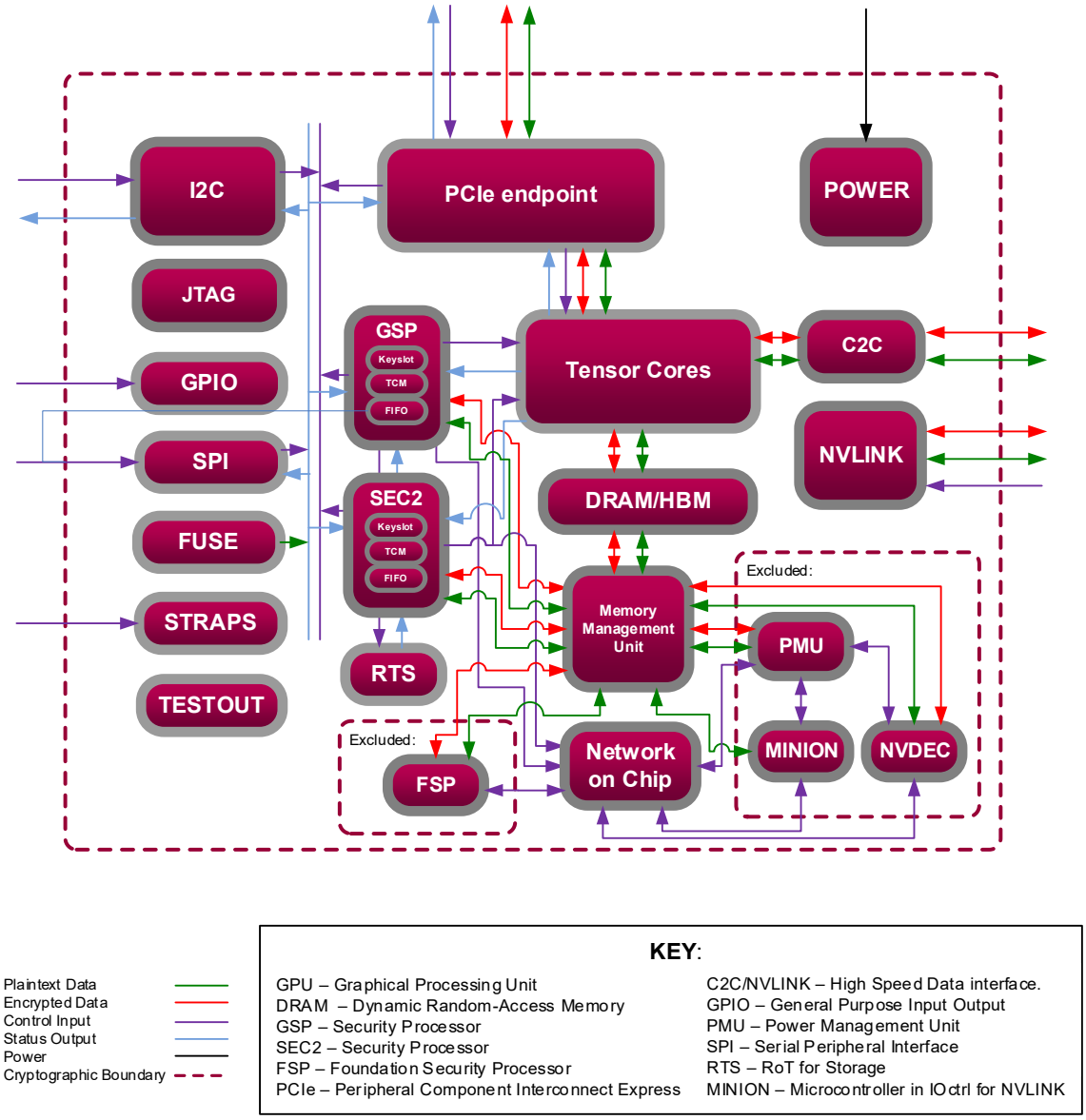

Figure 1: Module Block Diagram (with Cryptographic Boundary)

Figure 2 and Figure 3 below display the top and bottom views of the module, respectively.

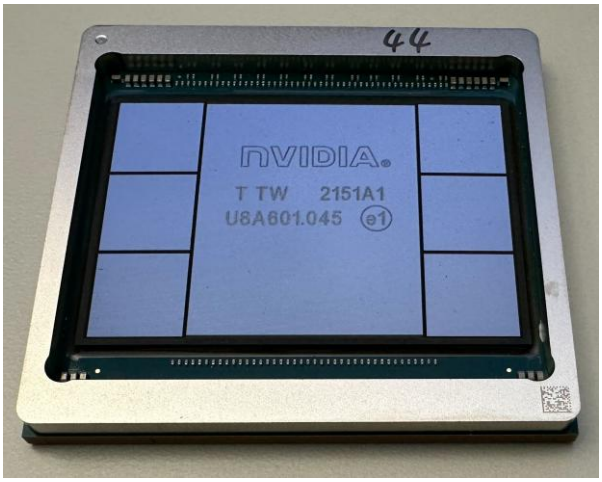

Figure 2: Nvidia H100 Tensor Core GPU (Top View)

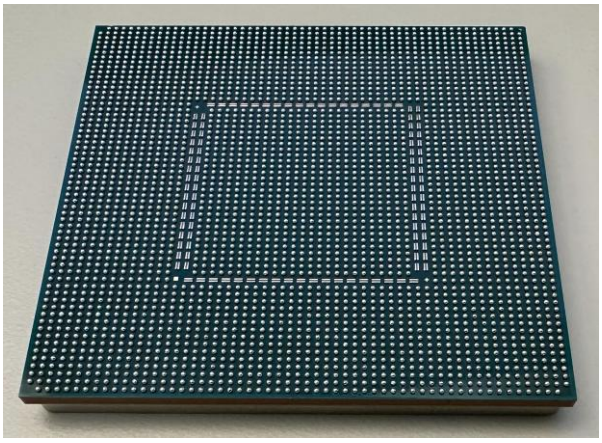

Figure 3: Nvidia H100 Tensor Core GPU (Bottom View)

2.2 Tested and Vendor Affirmed Module Version and Identification

2.2.1 Tested Module Identification – Hardware

The table below displays the tested operational environment of the hardware module.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
H100 FIPS-1	H100 FIPS-1	570.36	Nvidia H100	HBM2E
H100 FIPS-2	H100 FIPS-2	570.36	Nvidia H100	HBM3

Table 2: Tested Module Identification – Hardware

2.2.2 Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

This section is only applicable to software, firmware, and hybrid modules.

N/A for this module.

2.2.3 Tested Module Identification – Hybrid Disjoint Hardware

This section is only applicable to hybrid modules.

N/A for this module.

2.2.4 Tested Operational Environments – Software, Firmware, Hybrid

This section is only applicable to software, firmware, and hybrid modules.

N/A for this module.

2.2.5 Vendor-Affirmed Operational Environments – Software, Firmware, Hybrid

The vendor does not affirm any operational environments.

N/A for this module.

2.3 Excluded Components

The bulleted list below specifies the hardware components of the cryptographic module that are excluded from the security requirements, as well as the rationale for exclusion.

- Excluded Hardware Components
    - NVDEC: NVDEC is an independent ucoded block which is used for video decode acceleration. It has cryptographic functionality to handle DRM content. However, all cryptographic blocks are dedicated and located within this block. It does not provide any functionality or support to the GSP/SEC2 components and has an independent path for access to resources in the chip. The cryptographic functionality is not used in the module's services or to fulfill any of the module's security objectives.
    - Minion: This is an independent ucoded block to manage the NVLINK PHY programming. It has cryptographic functionality to authenticate and decrypt the firmware that is running on it. However, it provides no service or support to the GSP/SEC2 components and has an independent path to access

chip resources for its own functioning. The cryptographic functionality is not used in the module's services or to fulfill any of the module's security objectives.

- PMU: This is an independent ucoded block to manage the chip power management functions. It has cryptographic functionality to authenticate and decrypt the firmware that is running on it. However, it provides no service or support to GSP/SEC2 components and has an independent path to access chip resources for its own functioning. The cryptographic functionality is not used in the module's services or to fulfill any of the module's security objectives.

- FSP: FSP is an independent ucoded block that does not provide services to GSP/SEC2 and has dedicated crypto blocks located within the block. The cryptographic functionality is not used in the module's services or to fulfill any of the module's security objectives.

- Front Capacitors: The module includes package-level capacitors located along the package edges, used solely for decoupling and signal conditioning between internal die power/IO nets and the package pins. These components do not store or process SSPs, user data, or security-relevant control/status information.

These hardware components cannot be used to cause a compromise. Further, the module's physical security is maintained in the absence of these components. Thus, these hardware components have been excluded from the module validation.

2.4 Modes of Operation

2.4.1 Modes List and Description

The table below lists the mode of operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved	The only supported mode of operation of the module.	Approved	FIPS Mode ON; Devtools Mode ON

Table 3: Modes List and Description

2.5 Algorithms

2.5.1 Approved Algorithms

The module employs cryptographic algorithm implementations from the following sources:

- Copy Engine (Cert. A2733)
- GPU Service Processor (Cert. A2732, A4422)
- Security Controller (Cert. A2730, A4423)
- Root of Trust Storage for Storage (Cert. A4414)

The module implements the Approved algorithms listed in the table below.

Copy Engine

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A2733	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A2733	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D

Table 4: Approved Algorithms - Copy Engine

GPU Service Processor

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A4422	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A4422	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
Counter DRBG	A4422	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A4422	Curve - P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4422	Curve - P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A2732	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-384	A4422	Key Length - Key Length: 128, 192, 256	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4422	Domain Parameter Generation Methods - P-384 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A4422	Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256 HMAC Algorithm - SHA2-384	SP 800-56C Rev. 2
RSA SigVer (FIPS186-5)	A2732	Modulo - 3072 Signature Type - pss	FIPS 186-5
SHA2-384	A4422	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 5: Approved Algorithms - GPU Service Processor

Security Controller

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A4423	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A4423	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
Conditioning Component AES-CBC-MAC SP800-90B	A4423	Key Length - 128	SP 800-90B
RSA SigVer (FIPS186-5)	A2730	Modulo - 3072 Signature Type - pss	FIPS 186-5
SHA2-384	A4423	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 6: Approved Algorithms - Security Controller

Root of Trust for Storage

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A4414	Message Length - Message Length: 800	FIPS 180-4

Table 7: Approved Algorithms - Root of Trust for Storage

Only the algorithms specified in the tables above are approved algorithms supported by the module in approved mode of operation

2.5.2 Vendor Affirmed Algorithms

The vendor affirms the following cryptographic security methods:

Name	Properties	Implementation	Reference
CKG Section 6.1 Symmetric	Key type:Symmetric	N/A	SP 800-133 Rev. 2 Section 6.1
CKG Section 4 Example 1 Asymmetric	Key type:Asymmetric	N/A	SP 800-133 Rev. 2 Section 4 Example 1
CKG Section 4 Example 2 Asymmetric	Key Type:Asymmetric	N/A	SP 800-133 Rev. 2 Section 4 Example 2

Table 8: Vendor-Affirmed Algorithms

2.5.3 Non-Approved, Allowed Algorithms

The module does not offer any non-approved, allowed algorithms.

N/A for this module.

2.5.4 Non-Approved, Allowed Algorithms with No Security Claimed

The table below lists the non-approved, allowed algorithms with no security claimed.

Name	Caveat	Use and Function
AES ECB (No Security Claimed)	No Security Claimed; AES-ECB is only used as a pre-requisite for the AES-GCM which is only used within an encrypted tunnel. (IG 2.4.A Scenario 2c)	Pre-requisite AES mode for the AES GCM implemented operating within an encrypted tunnel.
AES-GCM (No Security Claimed)	No Security Claimed; AES-GCM is used within an encrypted tunnel. (IG 2.4.A Scenario 2c)	AES-GCM for data transfer within an encrypted AES-GCM tunnel.
ECDSA KeyGen (No Security Claimed)	No Security Claimed; ECDSA KeyGen is used for key generation of key pairs used for the attestation report. (IG 2.4.A Scenario 2)	Generation of the ECDSA Key Pairs for the Attestation Report Service
ECDSA SigGen (No Security Claimed)	No Security Claimed; ECDSA SigGen is used for signature generation used for the attestation report. (IG 2.4.A Scenario 2)	Generation of the ECDSA signatures for the Attestation Report Service
HMAC-SHA2-256 (No Security Claimed)	No Security Claimed; SHA2-256 is only used as a pre-requisite for the KBKDF which is used as a conditioning component for the GSP_UDS_KDK and GSP_UDS1, and key derivation of AK_Seed_NonCA and GSP_UDS1. (IG 2.4.A Scenario 2)	Conditioning Component
KBKDF (SP800-108) (No Security Claimed)	No Security Claimed; KBKDF is used as a conditioning component for the GSP_UDS_KDK and GSP_UDS1, and key derivation of AK_Seed_NonCA and GSP_UDS1. (IG 2.4.A Scenario 2)	Conditioning Component
SHA2-256 (No Security Claimed)	No Security Claimed; SHA2-256 is only used as a pre-requisite for the KBKDF which is used as a conditioning component for the GSP_UDS_KDK and GSP_UDS1, and key derivation of AK_Seed_NonCA and GSP_UDS1. (IG 2.4.A Scenario 2)	Conditioning Component

Name	Caveat	Use and Function
SHA2-384 (No Security Claimed)	No Security Claimed; SHA2-384 is only used as a pre-requisite for the ECDSA SigGen which is used for signature generation used for the attestation report. (IG 2.4.A Scenario 2)	Pre-requisite hash algorithm for the ECDSA SigGen which is used for signature generation
SPDM KDF (No Security Claimed)	No Security Claimed; The SPDM KDF is used within an encrypted tunnel. (IG 2.4.A Scenario 2c)	SPDM KDF for use in SPDM protocol. Note that the SPDM protocol operates within an encrypted AES-GCM tunnel.

Table 9: Non-Approved, Allowed Algorithms with No Security Claimed

2.5.5 Non-Approved, Not Allowed Algorithms

The module does not offer any non-approved, not allowed algorithms.

N/A for this module.

2.6 Security Function Implementations

The table below lists the security function implementations for this module.

Name	Type	Description	Properties	Algorithms
AES-GCM for DMA	BC-Auth	256-bit AES-GCM used by the GPU -> CPU DMA Key and CPU -> GPU DMA Key for data transfer.	Publication:SP 800-38D	AES-ECB: (A4422) Key Length: 256 bits AES-GCM: (A4422) Key Length: 256 bits
AES-GCM for KMD	BC-Auth	256-bit AES-GCM used by the GPU -> CPU KMD Key and CPU -> GPU KMD Key for data transfer.	Publication:SP 800-38D	AES-ECB: (A2733, A4423) Key Length: 256 bits AES-GCM: (A2733, A4423) Key Length: 256 bits
AES-GCM for RPC	BC-Auth	256-bit AES-GCM used by the GPU -> CPU RPC Key and CPU -> GPU RPC Key for data transfer.	Publication:SP 800-38D	AES-ECB: (A4422) Key Length: 256 bits AES-GCM: (A4422) Key Length: 256 bits
AES-GCM for Secure Session Establishment	BC-Auth	AES-GCM used for obfuscating the SPDM operations.	Publication:SP 800-38D	AES-ECB: (A4422) Key Length: 256 bits AES-GCM: (A4422) Key Length: 256 bits
AES-GCM for SPDM	BC-Auth	AES-GCM used for obfuscating the SPDM operations.		AES ECB (No Security Claimed): () Key Length: 256 bits AES-GCM (No Security Claimed): () Key Length: 256 bits
AES-GCM for UMD	BC-Auth	256-bit AES-GCM used by the GPU -> CPU UMD Key and CPU -> GPU UMD Key for data transfer.	Publication:SP 800-38D	AES-ECB: (A2733, A4423) Key Length: 256 bits AES-GCM: (A2733, A4423) Key Length: 256 bits

Name	Type	Description	Properties	Algorithms
CKG (GPU Service Processor)	CKG	Symmetric cryptographic key generation (GPU Service Processor).	Publication:SP 800-133 Rev. 2	CKG Section 6.1 Symmetric: () Counter DRBG: (A4422) AES-ECB: (A4422)
ECDSA KeyGen for AK_Pvt/Pub_NonCA	AsymKeyPair-KeyGen	ECDSA key generation for the AK_Pvt_NonCA and the AK_Pub_NonCA, which are used for signing and verifying the attestation report, respectively.	Publication:FIPS 186-5	ECDSA KeyGen (No Security Claimed): () Counter DRBG: (A4422) CKG Section 4 Example 2 Asymmetric: () AES-ECB: (A4422)
ECDSA KeyGen for ECDH	AsymKeyPair-KeyGen	ECDSA key generation for the Ephemeral ECDH key pair, which is used for shared secret computation.	Publication:FIPS 186-5	ECDSA KeyGen (FIPS186-5): (A4422) Counter DRBG: (A4422) CKG Section 4 Example 1 Asymmetric: () AES-ECB: (A4422)
ECDSA SigGen for AK_Pvt_NonCA	DigSig-SigGen	ECDSA signature generation for the AK_Pvt_NonCA, which is used to sign the attestation report.	Publication:FIPS 186-5	ECDSA SigGen (No Security Claimed): () Counter DRBG: (A4422) SHA2-384 (No Security Claimed): () AES-ECB: (A4422)
ECDSA SigGen for the device attestation certificate	DigSig-SigGen	ECDSA digital signature generation to sign "key exchange" messages.	Publication:FIPS 186-5	ECDSA SigGen (FIPS186-5): (A2732) Counter DRBG: (A4422) SHA2-384: (A4414) AES-ECB: (A4422)
Entropy Source	ENT-ESV	Entropy source with conditioning component.	Publication:SP 800-90B	Conditioning Component AES-CBC-MAC SP800-90B: (A4423) AES-ECB: (A4423)
HKDF for Secure Session Establishment	KAS-56CKDF	HKDF for Secure Session Establishment (SPDM).	Publication:SP 800-56C Rev. 2	KDA HKDF SP800-56Cr2: (A4422) HMAC-SHA2-384: (A4422) SHA2-384: (A4422)
HMAC for Data Transfer	MAC	HMAC for message authentication during data transfer.	Publication:FIPS 198-1	HMAC-SHA2-384: (A4422) SHA2-384: (A4422)
KAS-ECC-SSC	KAS-SSC	KAS-ECC-SSC used for ECDH, which is needed for the Secure Session Establishment service.	Publication:SP 800-56A Rev. 3	KAS-ECC-SSC Sp800-56Ar3: (A4422) ECDSA KeyGen (FIPS186-5): (A4422) SHA2-384: (A4422) Counter DRBG: (A4422) ECDSA KeyVer (FIPS186-5): (A4422) AES-ECB: (A4422)

Name	Type	Description	Properties	Algorithms
KBKDF for AK_Seed_NonCA	KBKDF	Key-based key derivation of the AK_Seed_NonCA.	Publication:SP 800-108 Rev. 1	KBKDF (SP800-108) (No Security Claimed): () HMAC-SHA2-256 (No Security Claimed): () SHA2-256 (No Security Claimed): () Counter DRBG: (A4422) AES ECB (No Security Claimed): ()
KBKDF for GSP_UDS1	KBKDF	Key-based key derivation of the GSP_UDS1.	Publication:SP 800-108 Rev. 1	KBKDF (SP800-108) (No Security Claimed): () HMAC-SHA2-256 (No Security Claimed): () SHA2-256 (No Security Claimed): () Counter DRBG: (A4422) AES ECB (No Security Claimed): ()
RSA SigVer for Authentication	DigSig-SigVer	Used for certificate-based authentication.	Publication:FIPS 186-5	RSA SigVer (FIPS186-5): (A2732) SHA2-384: (A4423)
RSA SigVer for Firmware Integrity	DigSig-SigVer	Signature Verification for the firmware integrity tests.	Publication:FIPS 186-5	RSA SigVer (FIPS186-5): (A2732, A2730) SHA2-384: (A4422, A4423)
SHA for Conditioning Component	UNK	KBKDF is used as a vetted conditioning component for the GSP_UDS_KDK and GSP_UDS1 keys.	Publication:SP 800-108	KBKDF (SP800-108) (No Security Claimed): () SHA2-256 (No Security Claimed): () HMAC-SHA2-256 (No Security Claimed): ()

Table 10: Security Function Implementations

2.7 Algorithm Specific Information

The information below provides algorithm information of references to specifications.

2.7.1 AES GCM IV

All AES GCM IVs are 96 bits in size and constructed deterministically. This applies for each of the algorithm implementations:

- AES GCM IV Generation (GPU Service Processor)
- AES GCM IV Generation (Security Controller)
- AES GCM IV Generation (Copy Engine)

As per I.G. C.H Key/IV Pair Uniqueness Requirements from SP 800-38D, AES GCM IV implements scenario 4.

2.8 RBG and Entropy

The table below specifies the module's entropy certificates. Please note that SECHUB and SEC2 refer to the Security Processor.

Cert Number	Vendor Name
E201	NVIDIA

Table 11: Entropy Certificates

The table below specifies the module's entropy sources.

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Nvidia Random Number Generator (NVRNG)	Physical	H100(SECHUB)	128 bits	128 bits	Conditioning Component AES-CBC-MAC SP800-90B (A4423)

Table 12: Entropy Sources

The DRBG requests 384 bits from the entropy source, resulting in 256 bits of entropy strength.

2.9 Key Generation

The module uses the following methods for key generation:

- CKG
- ECDSA KeyGen

As per *IG D.H* and *SP 800-133rev2*, the module uses an Approved Counter DRBG to generate random values and seeds that are used for asymmetric and symmetric key generation. The generated seed is an unmodified output from the Counter DRBG.

2.10 Key Establishment

2.10.1 Key Agreement Information

The module supports the following key agreement methods:

- KAS-ECC-SSC Sp800-56Ar3 (Elliptic curve Diffie-Hellman) and KDA HKDF SP800-56Cr2: Per FIPS 140-3 Implementation Guidance D.F, this key agreement method claims Scenario 2 path (2).

2.10.2 Key Transport Information

The module does not support any key transport methods.

2.11 Industry Protocols

The module supports the following industry protocol:

- SPDM

The SPDM protocol is implemented within an AES-GCM encrypted tunnel. No parts of the SPDM protocol have been tested by the CAVP and CMVP.

3. Cryptographic Module Interfaces

3.1 Ports and Interfaces

The H100 Tensor Core GPU is a single-chip processor embedded in a general-purpose computer or server. It connects to the host device via a PCIe connector. The design of this connector supports information flows in four logically distinct and isolated categories:

- Data Input
- Data Output
- Control Input
- Status Output

A mapping of the FIPS-defined interfaces, the host device's physical interfaces, and the module's logical interfaces can be found in the table below.

Physical Port	Logical Interface(s)	Data That Passes
C2C pins	Data Input Data Output	User Mode Application Data
GPIO pins	Control Input	GPIO are General Purpose Input/Output ports that allow the system to control H100. Things like Voltage Regulators, Fans, and LEDs are connected to GPIOs. No user data goes over the GPIOs.
I2C pins	Control Input Status Output	I2C is a low bandwidth control path H100. It allows the system BMC (Baseboard Management Controller) to perform system maintenance tasks like querying H100 temperature and other telemetry. No User Mode Application Data flows across I2C.
NVLINK pins	Data Input Data Output Control Input	NVLINK allows for fast transfer of User Mode Application Data between multiple H100s.
PCIe pins	Data Input Data Output Control Input Status Output	PCIe endpoint is the primary control port for the H100. All host interactions go through the PCIe endpoint, including User Mode Application data, Kernel Mode Data, and Host configuration commands.
Power pins	Power	N/A
SPI pins	Control Input	Used to read in firmware.
Straps pins	Control Input	Straps are board level settings that configure physical properties of the GPU. These are not dynamically modifiable.

Table 13: Ports and Interfaces

The module also includes two ports that are disabled during normal module operation:

- JTAG – JTAG is the port that is used for silicon debug and manufacturing.
- TESTOUT – This port is used to read out device status during manufacturing.

4. Roles, Services, and Authentication

4.1 Authentication Methods

The module supports role-based authentication; operators explicitly assume an authorized role based on the authentication credentials used. Module operators authenticate to the module using a certificate. The strength calculations for each of the authentication mechanisms are provided in the table below.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Certificate-based authentication	The mechanism provides mutual authentication between the requester (CPU which can assume the CO or User role) and responder (GPU which is the module).	RSA SigVer for Authentication	1/2^128	2/2^128

Table 14: Authentication Methods

4.2 Roles

The module Crypto Officer (CO) that authorized operators can assume. The CO role performs cryptographic initialization or management functions and general security services.

The module also supports the following role(s):

- User – The User role performs general security services, including cryptographic operations and other approved security functions.

The table below lists additional information about the supported roles.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	Certificate-based authentication
User	Role	User	Certificate-based authentication

Table 15: Roles

4.3 Approved Services

Descriptions of the services available are provided in the table below.

The keys and Sensitive Security Parameters (SSPs) listed in the table indicate the type of access required using the following notation:

- 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
Attestation Report	Generate and retrieve attestation report.	Global FIPS Indicator: "FIPS Mode ON"	Host runs verified tool	On Success: Report Error Code: SPDM Payload embedded error code.	ECDSA KeyGen for AK_Pvt/Pub_NonCA ECDSA SigGen for the device attestation certificate ECDSA SigGen for AK_Pvt_NonCA Entropy Source KBKDF for AK_Seed_NonCA KBKDF for GSP_UDS1 SHA for Conditioning Component	User - AK_Pub_NonCA: G,R,E - AK_Pvt_NonCA: G,E - AK_Seed_NonCA: G,E - DRBG 'Key' Value: G,E - DRBG 'V' Value: G,E - DRBG Entropy Input: G,E - DRBG Seed: G,E - GSP_UDS1: G,E - GSP_UDS_KDK: E - IK_Pvt: E
Data Transfer	Transfer data to and from module.	Global FIPS Indicator: "FIPS Mode ON"	SecureCE application invoked.	Error Code: Based on error type (e.g. Encryption/Decryption errors, HMAC errors etc.)	AES-GCM for RPC AES-GCM for DMA AES-GCM for KMD AES-GCM for UMD HMAC for Data Transfer	User - AES GCM IV: E - CPU -> GPU DMA Key: E - CPU -> GPU KMD Key: E - CPU -> GPU RPC Key: E - CPU -> GPU UMD Key: E - Data Transfer Key: E - GPU -> CPU DMA Key: E - GPU -> CPU KMD Key: E - GPU -> CPU RPC Key: E - GPU -> CPU UMD Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Self-tests On-demand	Performs pre-operational self-tests.	Global FIPS Indicator: "FIPS Mode ON"	Power cycle	Module operational on pass	RSA SigVer for Firmware Integrity	Unauthenticated - AES GCM IV: Z - AK_Pub_NonCA: Z - AK_Pvt_NonCA: Z - AK_Seed_NonCA: Z - CPU -> GPU DMA Key: Z - CPU -> GPU KMD Key: Z - CPU -> GPU RPC Key: Z - CPU -> GPU UMD Key: Z - DRBG 'Key' Value: Z - DRBG 'V' Value: Z - DRBG Entropy Input: Z - DRBG Seed: Z - Ephemeral ECDH Private Component: Z - Ephemeral ECDH Public Component: Z - Export Master Key: Z - Firmware Integrity Key: E,Z - GPU -> CPU DMA Key: Z - GPU -> CPU KMD Key: Z - GPU -> CPU RPC Key: Z - GPU -> CPU UMD Key: Z - SPDM Key Wrapping Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Secure Session Establishment	Establish a secure session.	Global FIPS Indicator: "FIPS Mode ON"	Secure establishment request	On Success: FINISH_RSP message is sent. Error Code: RPC Error Code	AES-GCM for SPDM AES-GCM for Secure Session Establishment CKG (GPU Service Processor) ECDSA KeyGen for ECDH Entropy Source HKDF for Secure Session Establishment KAS-ECC-SSC RSA SigVer for Authentication	Unauthenticated User - AES GCM IV: G,E - CPU -> GPU DMA Key: G - CPU -> GPU KMD Key: G - CPU -> GPU RPC Key: G - CPU -> GPU UMD Key: G - Data Transfer Key: G - DRBG 'Key' Value: G,E - DRBG 'V' Value: G,E - DRBG Entropy Input: G,E - DRBG Seed: G,E - ECDHE Secret: G,E,Z - Ephemeral ECDH Private Component: G,E - Ephemeral ECDH Public Component: G,R,W,E - Export Master Key: G,E - GH100 Key: W,E,Z - GPU -> CPU DMA Key: G - GPU -> CPU KMD Key: G - GPU -> CPU RPC Key: G - GPU -> CPU UMD Key: G - SPDM Key Wrapping Key: G,E
Show Status	Returns approved mode status.	Global FIPS Indicator: "FIPS Mode ON"	nvidia-smi conf_compute -q	Current state of operation	None	Crypto Officer
Show Versioning Information	Return module versioning information.	Global FIPS Indicator: "FIPS Mode ON"	nvidia-smi	Version details	None	Crypto Officer User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Zeroize	Zeroizes and de-allocates memory containing sensitive data by resetting GSP or SECHUB.	Global FIPS Indicator: "FIPS Mode ON"	SPDM session de-initialization	Zeroize all SSPs	None	Crypto Officer - AES GCM IV: Z - AK_Pub_NonCA: Z - AK_Pvt_NonCA: Z - AK_Seed_NonCA: Z - CPU -> GPU DMA Key: Z - CPU -> GPU RPC Key: Z - CPU -> GPU UMD Key: Z - DRBG 'Key' Value: Z - DRBG 'V' Value: Z - DRBG Entropy Input: Z - DRBG Seed: Z - Ephemeral ECDH Private Component: Z - Ephemeral ECDH Public Component: Z - Export Master Key: Z - GPU -> CPU DMA Key: Z - GPU -> CPU KMD Key: Z - GPU -> CPU RPC Key: Z - GPU -> CPU UMD Key: Z - GSP_UDS1: Z - GSP_UDS_KDK: Z - SPDM Key Wrapping Key: Z

Table 16: Approved Services

4.4 Non-Approved Services

The module does not offer any non-Approved services.

N/A for this module.

4.5 External Software/Firmware Loaded

Module firmware is loaded from an external source at power on. The module does not allow the operator to load firmware from an external source for upgrading the module firmware version.

5. Software/Firmware Security

5.1 Integrity Techniques

All FIPS firmware components within the cryptographic boundary are verified using an approved integrity technique implemented within the cryptographic module itself. The module implements a 3072-bit RSA digital signature verification with SHA2-384 for the firmware integrity tests of GSP and SEC2. The RSA implementations used for the firmware integrity check on the GSP firmware have been awarded CAVP certificate A2732 and for the SEC2 firmware A2730. The SHA implementations used to support the RSA implementations have also been awarded CAVP certificates for the GSP and SEC2 firmware, respectively: A4422 and A4423. The module's executable code is in the form of two compiled firmware images loaded onto the module, one for GSP and one for SEC2. The file name of the binary is NV_GPU_VBIOS_G520_0202_885. A firmware load test is to be considered inherently performed by the firmware integrity test after firmware is loaded into the module. Failure of the integrity check will cause the module to enter a critical error state.

5.2 Initiate on Demand

The CO can initiate the pre-operational tests on demand by rebooting/power-cycling the module.

6. Operational Environment

6.1 Operational Environment Type and Requirements

The H100 Tensor Core GPU comprises a firmware driver that executes in a Non-Modifiable operational environment.

6.2 Configuration Settings and Restrictions

The operating system offers no mechanism whereby the operator can modify firmware components, nor can the operator load and execute software or firmware that was not included as part of the validation of the module.

7. Physical Security

7.1 Mechanisms and Actions Required

The H100 is implemented as a single-chip embodiment with seven dies in a single package. It is manufactured using standard integrated circuit manufacturing technologies, producing a device that meets all commercial-grade power, temperature, reliability, shock, and vibration specifications, and all integrated circuits are coated with commercial standard passivation.

The H100 physical package provides hardness, opacity, and tamper-evidence protection conforming to FIPS 140-3 Physical Security Level 2. The H100 achieves this level of protection by implementing a chip enclosure (IC package) that is both hard and opaque (refer to Figure 2 above). This type of IC package ensures that any physical tampering will always result in scratches, chipping, or other visible damage on the enclosure.

The module implements the following physical security mechanisms in the table below.

Mechanism	Inspection Frequency	Inspection Guidance
Enclosure (IC package)	6 months	Verify chip package not compromised or tampered.

Table 17: Mechanisms and Actions Required

8. Non-Invasive Security

This section is not applicable. There are currently no approved non-invasive mitigation techniques references in Annex F of *ISO/IEC 19790*.

9. Sensitive Security Parameters Management

9.1 Storage Areas

The table below lists sensitive security parameters (SSPs) storage areas for this module.

Storage Area Name	Description	Persistence Type
DRAM/HBM	DRAM/RAM stores SPDM Key Wrapping Key, Export Master Key, and ECDHE SSPs.	Dynamic
FIFO	FIFO stores DRBG SSPs.	Dynamic
Fuses	Fuses store GSP_UDS_KDK, IK_Pvt, and Firmware Integrity Key.	Static
Keyslot	Keyslot contains keys used for secure communication between the GPU and the CPU.	Dynamic
TCM	TCM stores ephemeral SSPs and non-SSPs.	Dynamic

Table 18: Storage Areas

9.2 SSP Input-Output Methods

The module does not have any SSP input or output methods.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key Establishment export	DRAM/HBM	External	Plaintext	Automated	Electronic	
Key Establishment import	External	DRAM/HBM	Plaintext	Automated	Electronic	
Public key export	TCM	External	Plaintext	Automated	Electronic	
Public key import	External	TCM	Plaintext	Automated	Electronic	

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The table below lists SSP zeroization methods for this module.

Zeroization Method	Description	Rationale	Operator Initiation
Reset	Upon SECHUB or GSP reset commands, the SSPs are zeroized.	Resetting the SECHUB and GSP overwrites the SSPs with zeroes, yielding them irretrievable.	Operator resets SECHUB and GSP using the following zeroization commands: /sys/bus/pci/drivers/nvidia/unbind sudo rmmod nvidia_uvm sudo rmmod nvidia
Session Termination	Upon session termination, the memory will be cleared.	Session termination overwrites the SSPs with zeroes, yielding them irretrievable.	Operator terminates session.
Zeroization after use (FIFO)	After use, SSPs stored in FIFO will be zeroized.	When done using the SSP, the SSP stored in FIFO is overwritten with zeroes, yielding it irretrievable.	Operator calls service and the SSPs used by this service are zeroized after use.

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization after use (TCM)	After use, SSPs stored in the TCM will be zeroized.	When done using the SSP, the SSP stored in the TCM is overwritten with zeroes, yielding it irretrievable.	Operator calls service and the SSPs used by this service are zeroized after use.

Table 20: SSP Zeroization Methods

9.4 SSPs

The module supports the keys and other SSPs listed in the table below. Please note the SSPs tables include entries that are not considered SSPs but are otherwise included for completeness everywhere they are referenced.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES GCM IV	Used as the initialization vector for symmetric keys that use AES-GCM.	96 bits - 96 bits	Initialization Vector - PSP	Other (IG C.H Scenario 4)		AES-GCM for DMA AES-GCM for SPDM AES-GCM for KMD AES-GCM for RPC AES-GCM for Secure Session Establishment AES-GCM for UMD
AK_Pub_NonCA	Used for the attestation report.	384 bits - N/A	Public - Neither	ECDSA KeyGen for AK_Pvt/Pub_NonCA		ECDSA SigGen for the device attestation certificate
AK_Pvt_NonCA	Used for the attestation report.	384 bits - N/A	Private - Neither	ECDSA KeyGen for AK_Pvt/Pub_NonCA		ECDSA SigGen for the device attestation certificate
AK_Seed_NonCA	Used as the DRBG seed when generating the AK_Pvt_NonCA and AK_Pub_NonCA	384 bits - N/A	Seed - Neither		KBKDF for AK_Seed_NonCA SHA for Conditioning Component	ECDSA KeyGen for AK_Pvt/Pub_NonCA
CPU -> GPU DMA Key	Used for secure communication between the CPU and GPU. DMAs initiated at both end points CPU-GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for DMA
CPU -> GPU KMD Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for KMD
CPU -> GPU RPC Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for RPC

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CPU -> GPU UMD Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for UMD
Data Transfer Key	Data transfer. Secure work launch HMAC key.	256 bits - 256 bits	Authentication - CSP		HKDF for Secure Session Establishment	HMAC for Data Transfer
DRBG 'Key' Value	DRBG state value	256 bits - 256 bits	State value - CSP	CKG (GPU Service Processor)		CKG (GPU Service Processor)
DRBG 'V' Value	DRBG state value	128 bits - 128 bits	State value - CSP	CKG (GPU Service Processor)		CKG (GPU Service Processor)
DRBG Entropy Input	DRBG entropy input	384 bits - 384 bits	Entropy Input - CSP	Entropy Source		CKG (GPU Service Processor)
DRBG Seed	DRBG seed value	384 bits - 256 bits	Seed - CSP	CKG (GPU Service Processor)		CKG (GPU Service Processor)
ECDHE Secret	Secure session establishment. Expanded with HKDF to derive SPDM ephemeral keys.	384 bits - 192 bits	Shared Secret - CSP		KAS-ECC-SSC	HKDF for Secure Session Establishment
Ephemeral ECDH Private Component	Secure session establishment. Used for shared secret computation.	384 bits - 192 bits	Private - CSP	ECDSA KeyGen for ECDH		KAS-ECC-SSC
Ephemeral ECDH Public Component	Secure session establishment. Used for shared secret computation.	384 bits - 192 bits	Public - PSP	ECDSA KeyGen for ECDH		KAS-ECC-SSC
Export Master Key	Secure session establishment. For deriving additional keys.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for Secure Session Establishment
Firmware Integrity Key	Used in firmware integrity check	3072 bits - 128 bits	Public Key - PSP	Pre-Loaded		RSA SigVer for Firmware Integrity
GH100 Key	Used for certificate-based authentication.	3072 bits - 128 bits	Public - PSP			RSA SigVer for Authentication
GPU -> CPU DMA Key	Used for secure communication between the CPU and GPU. DMAs initiated at both end points CPU-GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for DMA
GPU -> CPU KMD Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for KMD

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
GPU -> CPU RPC Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for RPC
GPU -> CPU UMD Key	Used for secure communication between the CPU and GPU.	256 bits - 256 bits	Symmetric Key - CSP		HKDF for Secure Session Establishment	AES-GCM for UMD
GSP_UDS1	Used as input to conditioning component, output is AK_Seed_NonCA.	256 bits - N/A	Symmetric Key - Neither		KBKDF for GSP_UDS1 SHA for Conditioning Component	KBKDF for AK_Seed_NonCA SHA for Conditioning Component
GSP_UDS_KDK	Used as input to conditioning component, output is GSP_UDS1.	256 bits - N/A	Symmetric Key - Neither	Pre-Loaded		KBKDF for GSP_UDS1
IK_Pvt	Used to sign AK_Cert_NonCA.	384 bits - N/A	Private - Neither	Pre-Loaded		ECDSA SigGen for the device attestation certificate
SPDM Key Wrapping Key	Secure session establishment. Used to wrap (encrypt) any SPDM secrets.	256 bits - 256 bits	Symmetric Key - CSP	CKG (GPU Service Processor)		AES-GCM for SPDM

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES GCM IV		TCM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	SPDM Key Wrapping Key:Used With Export Master Key:Used With GPU -> CPU RPC Key:Used With CPU -> GPU RPC Key:Used With GPU -> CPU UMD Key:Used With CPU -> GPU UMD Key:Used With GPU -> CPU KMD Key:Used With CPU -> GPU KMD Key:Used With GPU -> CPU DMA Key:Used With CPU -> GPU DMA Key:Used With
AK_Pub_NonCA	Public key export	TCM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	AK_Seed_NonCA:Derived From AK_Pvt_NonCA:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AK_Pvt_NonCA		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	AK_Seed_NonCA:Derived From AK_Pub_NonCA:Paired With
AK_Seed_NonCA		TCM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Zeroization after use (TCM)	GSP_UDS1:Derived From
CPU -> GPU DMA Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
CPU -> GPU KMD Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
CPU -> GPU RPC Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
CPU -> GPU UMD Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
Data Transfer Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
DRBG 'Key' Value		TCM:Plaintext	Stored in TCM until done being used or until GSP or SECHUB is reset.	Reset Zeroization after use (TCM)	
DRBG 'V' Value		TCM:Plaintext	Stored in TCM until done being used or until GSP or SECHUB is reset.	Reset Zeroization after use (TCM)	
DRBG Entropy Input		FIFO:Plaintext	Stored in FIFO until SSP is done being used or until GSP or SECHUB is reset.	Reset Zeroization after use (FIFO)	
DRBG Seed		FIFO:Plaintext	Until SSP is done being used.	Reset Zeroization after use (FIFO)	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ECDHE Secret		DRAM/HBM:Obfuscated	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	Ephemeral ECDH Private Component:Derived From Ephemeral ECDH Public Component:Derived From SPDM Key Wrapping Key:Wrapped By
Ephemeral ECDH Private Component		DRAM/HBM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	Ephemeral ECDH Public Component:Paired With
Ephemeral ECDH Public Component	Key Establishment import Key Establishment export	DRAM/HBM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	Ephemeral ECDH Private Component:Paired With
Export Master Key		DRAM/HBM:Obfuscated	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	SPDM Key Wrapping Key:Wrapped by ECDHE Secret:Derived From AES GCM IV:Used With
Firmware Integrity Key		Fuses:Plaintext		N/A	
GH100 Key	Public key import	TCM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	
GPU -> CPU DMA Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
GPU -> CPU KMD Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
GPU -> CPU RPC Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
GPU -> CPU UMD Key		Keyslot:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Derived From AES GCM IV:Used With
GSP_UDS1		TCM:Plaintext	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	GSP_UDS_KDK:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
GSP_UDS_KDK		TCM:Plaintext Fuses:Obfuscated	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Zeroization after use (TCM)	
IK_Pvt		TCM:Plaintext Fuses:Obfuscated	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Zeroization after use (TCM)	
SPDM Key Wrapping Key		DRAM/HBM:Obfuscated	Stored in TCM until session termination or until GSP or SECHUB is reset.	Reset Session Termination	ECDHE Secret:Wraps Export Master Key:Wraps AES GCM IV:Used With

Table 22: SSP Table 2

10. Self-Tests

The module performs pre-operational self-tests and conditional self-tests. Pre-operational tests are performed between the time the cryptographic module is instantiated and before the module transitions to the operational state. Conditional self-tests are performed by the module during module operation when certain conditions exist. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

10.1 Pre-Operational Self-Tests

The module performs the following pre-operational self-tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-5) (A2730)	3072-bit with SHA2-384 (A4423)	Firmware Integrity	SW/FW Integrity	On success module will proceed into normal operation, on fail module will halt.	Firmware integrity test on SEC2 firmware
RSA SigVer (FIPS186-5) (A2732)	3072-bit with SHA2-384 (A4422)	Firmware Integrity	SW/FW Integrity	On success module will proceed into normal operation, on fail module will halt.	Firmware integrity test on GSM firmware

Table 23: Pre-Operational Self-Tests

Please note that algorithms must pass their own CASTs before being used for the pre-operational firmware integrity tests.

10.2 Conditional Self-Tests

The module performs the following conditional self-tests:

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Decrypt (A2733)	256-bit	Comparison Test	CAST	On success module will proceed into normal operation, on fail module will halt.	Decrypt	Boot up
AES-GCM Decrypt (A4422)	256-bit	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Decrypt	Boot up
AES-GCM Decrypt (A4423)	256-bit	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Decrypt	Boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM Encrypt (A2733)	256-bit	Comparison Test	CAST	On success module will proceed into normal operation, on fail module will halt.	Encrypt	Boot up
AES-GCM Encrypt (A4422)	256-bit	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Encrypt	Boot up
AES-GCM Encrypt (A4423)	256-bit	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Encrypt	Boot up
Continuous health Test - Adaptive Proportion Test	N/A	Fault Detection	CAST	On success module will proceed into normal operation, on fail module will halt.	Continuous health Test - Adaptive Proportion Test on entropy source	Boot up
Continuous health Test - Repetitive Count Test	N/A	Fault Detection	CAST	On success module will proceed into normal operation, on fail module will halt.	Continuous health Test - Repetitive count test on entropy source	Boot up
Counter DRBG (A4422)	AES, 256-bit without derivation function	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	DRBG KAT	Boot up
DRBG Health Tests	AES, 256-bit without derivation function	Generate/Instantiate/Reseed	CAST	On success module will proceed into normal operation, on fail module will halt.	DRBG Health Tests	Boot up
ECDSA KeyGen (FIPS186-5) (A2732)	P-384	PCT	PCT	On success module will proceed into normal operation, on fail module will halt.	Sign/Verify	Boot up
ECDSA KeyGen (FIPS186-5) (A4422)	P-384	PCT	PCT	On success module will proceed into normal operation, on fail module will halt.	Sign/Verify	Boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigGen (FIPS186-5) (A2732)	P-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Sign	Boot up
KAS-ECC-SSC Sp800-56Ar3 (A4422)	P-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Shared Secret "Z" Computation	Boot up
KDA HKDF SP800-56Cr2 (A4422)	HMAC-SHA2-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Derive	Boot up
RSA SigVer (FIPS186-5) (A2730)	3072-bit; SHA2-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Verify	Boot up
RSA SigVer (FIPS186-5) (A2732)	3072-bit; SHA2-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Verify	Boot up
SHA2-384 (A4414)	SHA2-384	Comparison Test	CAST	On success module will proceed into normal operation, on fail module will halt.	Hash	Boot up
SHA2-384 (A4422)	SHA2-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Hash	Boot up, before the pre-operational self-test.
SHA2-384 (A4423)	SHA2-384	KAT	CAST	On success module will proceed into normal operation, on fail module will halt.	Verify	Boot up
Start-up health Test - Adaptive Proportion Test	N/A	Fault Detection	CAST	On success module will proceed into normal operation, on fail module will halt.	Start-up health Test - Adaptive Proportion Test and Repetitive count test on entropy source	Boot up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Start-up health Test - Repetitive Count test	N/A	Fault Detection	CAST	On success module will proceed into normal operation, on fail module will halt.	Start-up health Test - Repetitive count test on entropy source	Boot up

Table 24: Conditional Self-Tests

10.3 Periodic Self-Test Information

The module does not perform periodic self-tests automatically, but the operator may conduct self-tests on demand via the methods listed in Section 10.5 below. The tables below provide information regarding the pre-operational self-tests and conditional self-tests, respectively, that the operator can perform on demand:

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A2730)	Firmware Integrity	SW/FW Integrity	On Demand	Manually
RSA SigVer (FIPS186-5) (A2732)	Firmware Integrity	SW/FW Integrity	On Demand	Manually

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM Decrypt (A2733)	Comparison Test	CAST	On Demand and Continuous	Manually
AES-GCM Decrypt (A4422)	KAT	CAST	On Demand	Manually
AES-GCM Decrypt (A4423)	KAT	CAST	On Demand	Manually
AES-GCM Encrypt (A2733)	Comparison Test	CAST	On Demand and Continuous	Manually
AES-GCM Encrypt (A4422)	KAT	CAST	On Demand	Manually
AES-GCM Encrypt (A4423)	KAT	CAST	On Demand	Manually
Continuous health Test - Adaptive Proportion Test	Fault Detection	CAST	On Demand	Manually
Continuous health Test - Repetitive Count Test	Fault Detection	CAST	On Demand	Manually
Counter DRBG (A4422)	KAT	CAST	On Demand	Manually
DRBG Health Tests	Generate/Instantiate/Reseed	CAST	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A2732)	PCT	PCT	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A4422)	PCT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A2732)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4422)	KAT	CAST	On Demand	Manually
KDA HKDF SP800-56Cr2 (A4422)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-5) (A2730)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A2732)	KAT	CAST	On Demand	Manually
SHA2-384 (A4414)	Comparison Test	CAST	On Demand and Continuous	Manually
SHA2-384 (A4422)	KAT	CAST	On Demand	Manually
SHA2-384 (A4423)	KAT	CAST	On Demand	Manually
Start-up health Test - Adaptive Proportion Test	Fault Detection	CAST	On Demand	Manually
Start-up health Test - Repetitive Count test	Fault Detection	CAST	On Demand	Manually

Table 26: Conditional Periodic Information

10.4 Error States

The table below describes the error states of the module.

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	The module will no longer perform cryptographic services or output data over data output interfaces.	The module fails any self-test. The operator fails to authenticate to the module.	The module must be re-initialized by reboot/power-cycle of the host platform. If the module continues to experience self-test failures, contact Nvidia Corporation for assistance.	Bits set in a status register. Error logs are viewable after power cycling the module.

Table 27: Error States

10.5 Operator Initiation of Self-Tests

The operator may initiate self-tests on demand by rebooting or power-cycling the module.

11. Life-Cycle Assurance

The sections below describe how to ensure the module is operating in its validated configuration, including the following:

- Procedures for secure installation, initialization, startup, and operation of the module
- Maintenance requirements
- Administrator and non-Administrator guidance

The sections below describe how to ensure the module is operating in its validated configuration.

Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy)

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Secure Installation

The module is delivered to the operator pre-installed on a compatible circuit board. The Crypto Officer shall inspect the module to ensure that the IC package has not been compromised or tampered with. If the module has been compromised or tampered, the Crypto Officer shall not install the module and should contact Nvidia Custom Support for assistance.

No further installation action is required by the operator.

11.1.2 Configuration

There are no specific configuration steps the operator needs to perform.

11.1.3 Initialization

This module is designed to support vendor applications, and these applications are the sole consumers of the cryptographic services provided by the module. No end-user action is required to initialize the module for operation; the calling application performs any actions required to initialize the module before the end user can use the module.

11.2 Administrator Guidance

There are no specific management activities required of the CO role to ensure that the module runs securely. However, if any irregular activity is noticed or the module is consistently reporting errors, then Nvidia Customer Support should be contacted.

The following list provides additional guidance for the CO:

- The CO can initiate the pre-operational self-tests (as well as the conditional and critical functions self-tests that are performed pre-operationally) on demand for periodic testing of the module by rebooting-power-cycling the host platform.

- To determine the module's operational status, the Crypto Officer can invoke the module's Show Status service.

- To zeroize the module's SSPs, the Crypto Officer can invoke the module's Zeroize service.

- To review the module's versioning information, the Crypto Officer can invoke the module's Show Versioning Information service.

- The module firmware supports a debug mode that is disabled by default. Enabling the debug mode results in a non-compliant state.

11.3 Non-Administrator Guidance

If any irregular activity is noticed or the module is consistently reporting errors, then Nvidia Customer Support should be contacted.

The following list provides additional policies for the User role:

- Maintenance, including protection and zeroization, of any keys and CSPs that exist outside the module's cryptographic boundary are the responsibility of the end-user. For the zeroization of keys in volatile memory, module operators can reboot/power-cycle the host device.

- In the event that power to the module is lost and subsequently restored, a new key for use with the AES-GCM encryption/decryption shall be established by the User by invoking the "Secure Session Establishment" and "Data Transfer" services.

11.4 End of Life

All ephemeral or temporary keys can be sanitized via power cycle. The operator must ensure the power-off state has been transitioned to at module end of life, which is a maximum of 10 years.

12. Mitigation of Other Attacks

The module does not claim to mitigate any attacks beyond the FIPS 140-3 Level 2 requirements for this validation. Therefore, per *ISO/IEC 19790:2012* section 7.12, requirements for this section are not applicable.

Appendix A. Acronyms and Abbreviations

Table 28 provides definitions for the acronyms and abbreviations used in this document.

Table 28: Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
AK	Attestation Key
API	Application Programming Interface
BROM	Boot Read-only Memory
C2C	Client to Client
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DEP	Default Entry Point
DES	Data Encryption Standard
DH	Diffie-Hellman
DMA	Direct Memory Access
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference /Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
GPIO	General Purpose Input/Output
GPU	Graphical Processor Unit
GSP	GPU Service Processor
HMAC	(keyed-) Hash Message Authentication Code

Acronym	Definition
I2C	Inter-Integrated Circuit
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KMD	Kernel-mode Driver
KTS	Key Transport Scheme
KW	Key Wrap
KWP	Key Wrap with Padding
NIST	National Institute of Standards and Technology
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSS	Probabilistic Signature Scheme
RAM	Random Access Memory
RM	Remote Machine
RNG	Random Number Generator
RPC	Remote Procedure Call
RSA	Rivest, Shamir, and Adleman
SEC2/SECHUB	Security Processor
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
SPDM	Security Protocol and Data Model
SPI	Serial Peripheral Interface
TCM	Tightly Coupled Memory
UMD	User-mode Driver

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com