Google, LLC

Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation requirements. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

About this Document

This non-proprietary Cryptographic Module Security Policy for the Google, LLC Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module (Hardware Version: 2.4.27) provides an overview of the product and a high-level description of how it meets the overall Security Level 1 requirements per FIPS 140-3.

The Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module may also be referred to as “NMVe DPSC” or the “module” in this document.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Google, LLC shall have no liability for any error or damages of any kind resulting from the use of this document.

Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

The module claims an overall Security Level of 1 with all individual sections at a Security Level 1. The module does not implement any Non-Invasive Security mitigations or Mitigations of Other Attacks and thus the requirements per these sections are inapplicable. The module does not contain any firmware and thus the requirements per the Software/Firmware Security section too are inapplicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The NVMe DPSC Module is a sub-chip IP Block in the IN763 System-on-a-chip (SoC).

The Data Path Security Cluster (DPSC) is a hardware IP providing XTS-AES encryption to NVMe data in transit over the network. The cryptographic module accepts and stores cryptographic keys for multiple NVMe connections.

The DPSC contains 8 identical XTS-AES-256 decrypt engines, 8 identical XTS-AES-256 encrypt engines, key cache arbiter and key cache SRAM which is zeroised on reset. The data interfaces exposed to the NVMe Protocol Layer (NPL) within the NVMe Protocol Initiator (NPI) are read and write DMA interfaces. XTS keys are written to the module's SRAM via Control/Status Register (CSR) writes from the Integrated Management Complex (IMC) located outside of the module boundary. On-demand self- tests may be initiated from the CSR interace using an on-demand self-test trigger over a wire interface.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

The physical perimeter of the module is the single chip i.e., the IN763 SoC. The module's cryptographic boundary is the NVMe DPSC IP Block i.e., the Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module, a sub-chip within the IN763 SoC/single-chip. The module only supports a single mode of operation, the Approved mode, where only approved cryptographic functions and services are available.

Tested Operational Environment's Physical Perimeter (TOEPP):

The cryptographic boundary of the module and the relationship among the various internal components of the module have been depicted in Figure 1 below.

Figure 1: Block Diagram

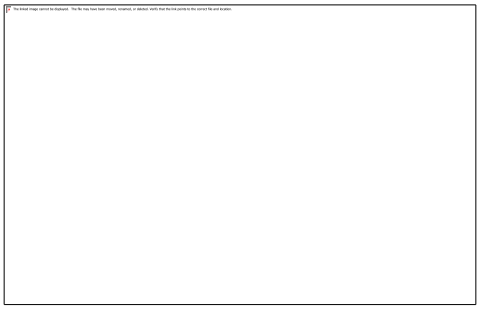

Figure 2: Single-chip picture

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
IN763 A0 SoC	2.4.27	N/A	N/A	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components have been excluded from the cryptographic boundary of the module.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	No configuration of the module or installation steps are required from the operator as stated in Section 11.1; When the module is powered on its self-tests are executed without any operator intervention; The module enters the Approved mode of operation automatically if the self-tests at boot complete successfully	Approved	The successful completion of self-tests indicates operation of the module in the Approved mode, bit[2] of the self_test_status register is set to 0

Table 3: Modes List and Description

Degraded Mode Description:

The module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-XTS Testing Revision 2.0	A6037	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Vendor-Affirmed Algorithms do not apply to the module.

Non-Approved, Allowed Algorithms:

Non-Approved, Allowed Algorithms do not apply to the module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Non-Approved, Allowed Algorithms with No Security Claimed do not apply to the module.

Non-Approved, Not Allowed Algorithms:

Non-Approved, Not Allowed Algorithms do not apply to the module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
XTS	BC-UnAuth BC-UnAuthDecrypt BC-UnAuthEncrypt	XTS encryption and decryption of data written into functional blocks before being offloaded to another subsystem	Direction:Encrypt, Decrypt	AES-XTS Testing Revision 2.0: (A6037)

Table 5: Security Function Implementations

2.7 Algorithm Specific Information

Per IG C.I, the module implements a check to verify that Key1!=Key2 for the AES-XTS implementation. This verification is performed prior to using the keys in encryption/decryption per the test listed in the Section 10.2 Conditional Self-Tests table of this document. The AES-XTS keys (i.e., Key_1 and Key_2) entered into the module shall be generated and/or established independently according to NIST SP 800-133rev2, Section 6.3. for an approved use of AES-XTS.

2.8 RBG and Entropy

The module does not perform any SSP generation and thus an entropy source is not contained in/used by the module.

2.9 Key Generation

The module does not provide any SSP generation service or perform SSP generation for any of its Approved algorithms. The caller provides the keys for encryption and/or decryption. Keys are stored in hardware registers (write-only) by the Crypto Officer. Once the keys are written to the hardware registers, they are not readable from outside the module.

The cryptographic module does not provide any asymmetrical algorithms or SSP establishment

methods.

2.10 Key Establishment

The module does not support SSP establishment.

2.11 Industry Protocols

The module does not support any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
WrDMA0, WrDMA1	Data Input	DMA writes
Control/Status Register (CSR)	Data Input Control Input Status Output	Key cache writes, On-demand self-test trigger and status bit in return
RdDMA0, RdDMA1	Data Output	DMA read
Physical power connector	Power	Power provided to the module
SRAM test interface for Keycache SRAM, data input FIFO SRAM, and data output FIFO SRAM	None	Not active while the module is operational
Error interrupt interface	Status Output	Self-test error reporting

Table 6: Ports and Interfaces

The module does not support a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	None

Table 7: Roles

The module implements the Crypto Officer (CO) role alone. The module does not allow concurrent operators. The Crypto Officer role is implicitly assumed by the entity accessing services implemented by the module. The CO role has access to all services provided by the module. The Crypto Officer is responsible to set i.e. provide the key for the cipher operations.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Encryption	Supply an NVMe Protocol Data Unit (PDU) for encryption	Approved mode indicator and successful completion of the service	NVMe Protocol Data Unit (PDU)	Encrypted NVMe Protocol Data Unit (PDU)	XTS	CO - Key1: W,E - Key2: W,E
Decryption	Supply an NVMe PDU for decryption	Approved mode indicator and successful completion of the service	Encrypted NVMe Protocol Data Unit (PDU)	NVMe Protocol Data Unit (PDU)	XTS	CO - Key1: W,E - Key2: W,E - Optimized Decryption Key: W,E
Perform self-tests	On demand self-test execution on rebooting the module or restarting the module on-demand by using the self-test trigger from	Approved mode indicator and successful completion of the service	Power cycle, self-test trigger from external software	Status	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	external software					
Initialization	Module initialization	Approved mode indicator and successful completion of the service	Power	Status	None	CO
Perform zeroisation	Reboot/power-cycle of the module zeroises all SSPs as they are stored ephemerally in the SRAM	Approved mode indicator and successful completion of the service	Power cycle/reboot	N/A	None	CO - Key1: Z - Key2: Z - Optimized Decryption Key: Z
Show Status	Approved mode status provided by the module	Approved mode indicator and successful completion of the service	Execution of self-tests/services returns status	Status (successful completion of self-tests indicates operation of the module in the Approved mode, bit[2] of the self_test_status register is set to 0 and in case of an error, this bit is set to 1; Also, the key1_eq_key2 Interrupt Status register field is set to 1 in case of a failure in the AES-XTS conditional self-test)	None	CO

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show module's versioning information	Retrieval of the module ID and hardware version	Approved mode indicator and successful completion of the service	The module identifier can be obtained by reading the memory location 0x2021d00144 (devmem 0x2021d00144); The hardware version can be obtained by reading the memory location 0x2021D00150 (devmem 0x2021D00150)	Module identifier: 0x44505300 (ASCII value is "DPS"); Hardware version: 0x02040027 (Decimal value is 2.4.27)	None	CO

Table 8: 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

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

4.5 External Software/Firmware Loaded

The module does not support loading of firmware.

4.6 Bypass Actions and Status

The module does not support a bypass capability.

4.7 Cryptographic Output Actions and Status

The module does not support self-initiated cryptographic output.

5 Software/Firmware Security

5.1 Integrity Techniques

The module is implemented entirely in hardware and is non-modifiable. Therefore, the integrity test requirements do not apply in accordance with IG 5.A. Per the allowance in the IG, instead, the module implements the AES-XTS Known Answer Tests (KAT) i.e. Cryptographic Algorithm Self-Tests (CAST) and is designed to execute the same on every boot.

5.2 Initiate on Demand

The AES-XTS Known Answer Tests (KAT) i.e. Cryptographic Algorithm Self-Tests (CAST) can be initiated on demand by rebooting the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The module is a sub-chip cryptographic subsystem implemented within a single-chip embodiment. No firmware is implemented in the module.

The module resides within the following single chip:

- IN763 SoC

6.2 Configuration Settings and Restrictions

The module is implemented entirely in hardware and is thus non-modifiable, i.e., configuration of the module is infeasible.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Standard passivation applied on the IN763 SoC; The SOC/single chip is commercial grade in regard to power and voltage ranges, temperature, reliability, and shock and vibration	None	None

Table 9: Mechanisms and Actions Required

The module is a sub-chip cryptographic subsystem implemented as part of the IN763 SoC, which is the physical perimeter of the module. The IN763 SoC is a production grade single-chip with a standard passivation applied and hence conforms to the Security Level 1 requirements for this section.

8 Non-Invasive Security

8.1 Mitigation Techniques

The module does not implement any non-invasive security mitigations and thus the requirements per this section do not apply to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Key cache SRAM	Temporary/ephemeral storage	Dynamic

Table 10: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input via direct CSR interface	External endpoint	Key cache SRAM	Plaintext	Manual	Electronic	

Table 11: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroised on reset	SSPs stored in key cache SRAM	Temporarily/ephemerally stored SSPs zeroised on reset	Operator Initiated

Table 12: SSP Zeroization Methods

All the SSPs are stored in the on-chip key cache SRAM (i.e. static registers). The key cache is write-only and cannot be read from outside of the module. When the operator performs a reset of the IN763 SoC, it will zeroise all SSPs contained within the module. The key cache logic on reset will auto-initialize the on-chip SRAM and key valid bits. The key cache is initialized with all zeroes, and the key valid bits will be cleared to indicate that the key registers are invalid.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Key1	Bulk encryption Key	256 bits - 256 bits	Symmetric Key - CSP			XTS
Key2	Tweak Key	256 bits - 256 bits	Symmetric Key - CSP			XTS
Optimized Decryption Key	Decryption key	256 bits - 256 bits	Symmetric Key - CSP			XTS

Table 13: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Key1	Input via direct CSR interface	Key cache SRAM:Plaintext	Until reset	Zeroised on reset	Key2:Paired With
Key2	Input via direct CSR interface	Key cache SRAM:Plaintext	Until reset	Zeroised on reset	Key1:Paired With
Optimized Decryption Key	Input via direct CSR interface	Key cache SRAM:Plaintext	Until reset	Zeroised on reset	Key1:Derived From

Table 14: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
AES-XTS - Encrypt	256 bits; Encrypt	KAT	SW/FW Integrity	bit[2] of the self_test_status register field is set to 0	AES-XTS 256 encryption (forward cipher function) performed per boot
AES-XTS - Decrypt	256 bits; Decrypt	KAT	SW/FW Integrity	bit[2] of the self_test_status register field is set to 0	AES-XTS 256 decryption (inverse cipher function) performed per boot

Table 15: Pre-Operational Self-Tests

The module is implemented entirely in hardware and is non-modifiable. Therefore, the pre-operational firmware integrity test requirements do not apply. In accordance with IG 5.A, the module instead is designed to execute the AES-XTS Known Answer Tests (KAT) i.e. Cryptographic Algorithm Self-Tests (CAST) on every boot. These tests do not require operator intervention to run.

These self-tests must be passed before the Crypto Officer can perform services. The self-tests can be run on demand by rebooting the module or by sending a self-test trigger signal bit from an external software.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-XTS Encrypt	256 bits; Encrypt	KAT	CAST	bit[2] of the self_test_status register field is set to 0	AES-XTS 256 encryption (forward cipher function) performed per boot	On every boot
AES-XTS Decrypt	256 bits; Decrypt	KAT	CAST	bit[2] of the self_test_status register field is set to 0	AES-XTS 256 encryption (inverse cipher function) performed per boot	On every boot
AES-XTS Key1!=Key2 check	256 bits, check for Key1 != Key2 per	Comparision of Key1 and Key2	CAST	key1_eq_key2 Interrupt Status register	Prior to use of an XTS key, the module	Prior to use of an XTS key

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	FIPS 140-3 IG C.I			field is set to '0' (0x0)	verifies that Key1!=Key 2 and the key is present in the keycache	

Table 16: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS - Encrypt	KAT	SW/FW Integrity	On every boot, On demand	Programmatically, Manually via reboot
AES-XTS - Decrypt	KAT	SW/FW Integrity	On every boot, On demand	Programmatically, Manually via reboot

Table 17: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Encrypt	KAT	CAST	On every boot, On demand	Programmatically, Manually via reboot
AES-XTS Decrypt	KAT	CAST	On every boot, On demand	Programmatically, Manually via reboot
AES-XTS Key1!=Key2 check	Comparision of Key1 and Key2	CAST	Prior to use of an XTS key, On demand	Programmatically, Manually via reboot followed by invoking either the Encryption/Decryption service

Table 18: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Hard Error state	Failure of the AES-XTS Cryptographic Algorithm Self-Tests causes the	Failure of Cryptographic Algorithm Self-	An operator can attempt to reset the state	bit[2] of the self_test_status

Name	Description	Conditions	Recovery Method	Indicator
	module to enter this state, where no functions can be executed; If any of the tests fail, the module will not initialize, and any output of the XTS engines will be driven to 0 (including the contents of the key cache)	Tests (including the Pre-operational self-tests)	by cycling the power; However, the repeated failure of a self-test may require the module to be replaced	register field is set to 1
Soft Error state	Failure of the AES-XTS Key1!=Key2 check per IG C.I causes the module to enter this state; The output of the module will be driven to 0 for a given payload; The encryption/decryption request will fail as a result of failure of this test	Failure of AES-XTS check for Key1!=Key2	The module will continue to process payload encryption and decryption operations if the subsequent keys are valid and not equal	key1_eq_key2 Interrupt Status register field is set to '1' (0x1)

Table 19: Error States

10.5 Operator Initiation of Self-Tests

The operator can initiate the AES-XTS Known Answer Tests by rebooting the module. The AES-XTS check for Key1!=Key2 per the FIPS 140-3 IG C.I, can be done by requesting the AES-XTS service from the module given that this check is performed prior to using the XTS keys provided by the caller/operator.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No configuration of the module or installation steps are required by the operator. When the module is powered on its AES-XTS Known Answer Tests are executed without any operator intervention. The module enters the Approved mode of operation automatically if the self-tests are completed successfully. If any of the self-tests fail during power-up, the module will transition to the Hard Error state. The status of the module can be determined by the availability of the module. If the module is available, it has passed all self-tests (i.e., self_test_status register bit[2] set to 0). If it is unavailable, it is in the error state or has not been properly initialized.

11.2 Administrator Guidance

Additional guidance does not apply for the operation of the module apart from that specified in Sections 2, 3 and other subsections under this section.

11.3 Non-Administrator Guidance

Additional guidance does not apply for the operation of the module apart from that specified in Sections 2, 3 and other subsections under this section.

11.4 Maintenance Requirements

Additional maintenance requirements do not apply to the module.

11.5 End of Life

A reset of the IN763 SoC can be used to zeroise all SSPs contained within the module. In other words, the module can be zeroised to securely sanitize it.

12 Mitigation of Other Attacks

The module does not mitigate any other attacks and thus the requirements per this section do not apply.