Non-Proprietary FIPS 140-2 Security Policy

Google LLC

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

Hardware version: 2.3.1

Date: March 29, 2022

Prepared By:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Introduction

Federal Information Processing Standards Publication 140-2 — 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 140-2 testing; the CMVP validates modules meeting FIPS 140-2 validation requirements. Validated is the term given to a module that is documented and tested against the FIPS 140-2 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 NVMe DPSC Module from Google LLC. provides an overview of the product and a high-level description of how it meets the overall Level 1 security requirements of FIPS 140-2.

The NVMe 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

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Google LLC. Non-Volatile Memory express (NVMe) Data Path Security Cluster (DPSC) Module (Hardware Version: 2.3) (also referred to as the "module" hereafter). It contains a specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

1.2 Overview

The NVMe DPSC Module consists of a sub-chip IP Block in the ARM Cortex-A53 based Google IN762 System-on-a-chip (SoC). The sub-chip module provides a virtual NVMe (vNMVe) block device to host hypervisor platforms and guest virtual machines (VMs). The NVMe DPSC consists of four (4) identical XTS-AES Encrypt and four (4) identical XTS-AES Decrypt engines, a keycache SRAM and a key cache arbiter.

2. Security Level

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	1

Table 1 - Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The physical boundary of the module is the single-chip physical embodiment of the IN762 SoC. The module's logical boundary is the hardware-based functionality contained within the NVMe DPSC IP Block at the sub-chip level. The module only supports a single mode of operation where only Approved cryptographic functions and services are available. The cryptographic boundary of the module and the relationship among the various internal components of the module are depicted in Figure 1 below.

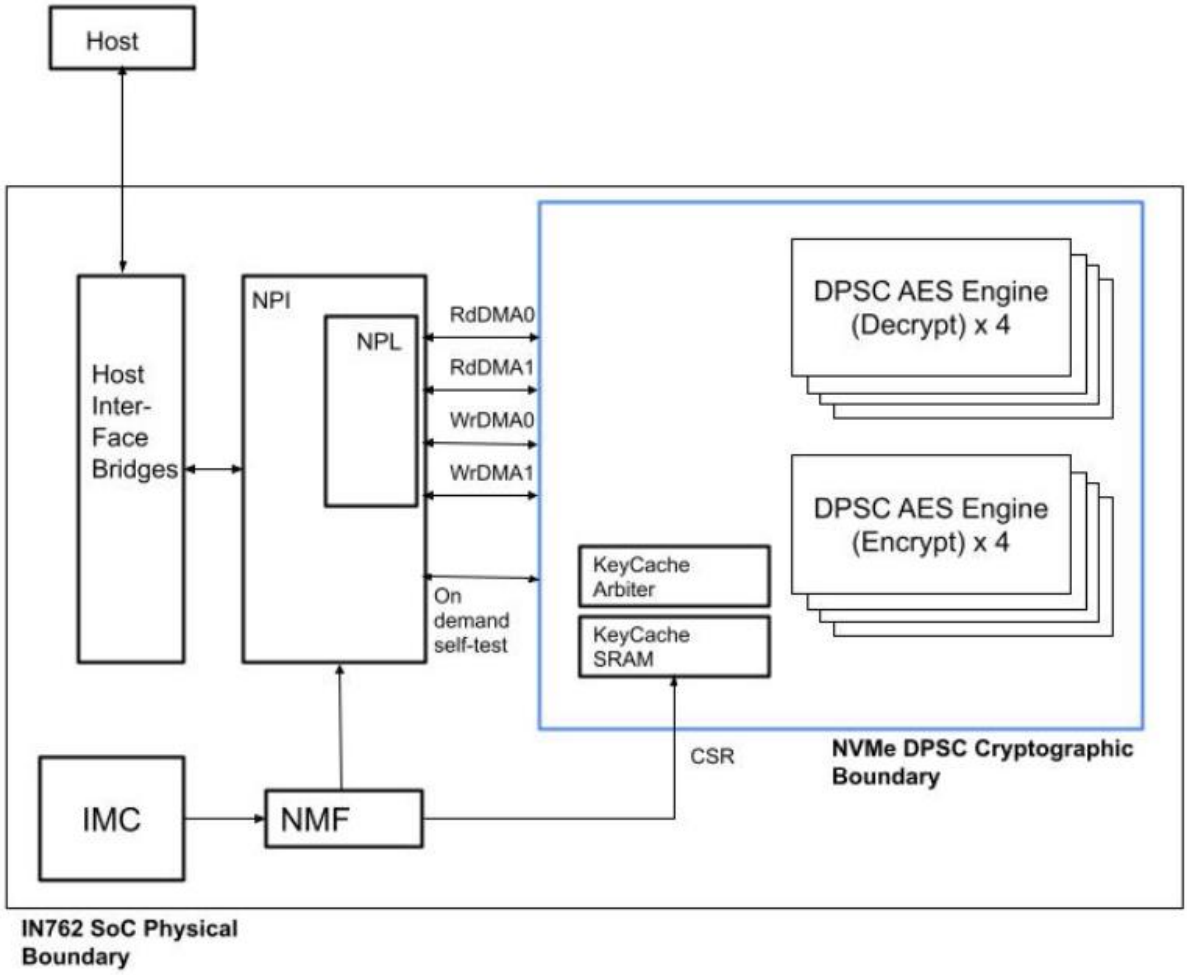

Figure 1 - NVMe DPSC Block Diagram

The module consists of the NVMe DPSC, which is an integral component of the NVMe Protocol Engine in the IN762 SoC. The NVMe Protocol Engine provides a means to allow the host OS to communicate with its storage through a standard PCIe-based NVMe/SSD driver while allowing the operator to provision that storage either locally or across the network.

NVMe DPSC provides XTS encryption and decryption of data written into functional blocks before being offloaded to another subsystem via the NIC Management Fabric (NMF), which is connected via an AMBA[1] on-chip system bus. DPSC includes 4 identical XTS-AES 256 decrypt engines, 4 identical XTS-AES 256 encrypt engines, key cache arbiter and key cache SRAM which is zeroized on reset. The data interfaces exposed to the NVMe Protocol Layer (NPI) 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 NPI using an on-demand self-test trigger over a wire interface.

4. Cryptographic Module Ports and Interfaces

The module provides the following number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Interface	Module Ports	Description
Data Input	WrDMA0, WrDMA1	Write DMA interfaces
	Control/Status Register (CSR)	Key cache writes
Data Output	RdDMA0, RdDMA1	Read DMA interfaces
Control Input	Wire interface	On-demand self-test trigger
	Control/Status Register (CSR)	Key cache writes
Status Output	Wire interface	On-demand self-test status bit
	Control/Status Register	Status output
Power Input	Physical power connector	Provides power to the module

Table 2 - Physical Port and Logical Interface Mapping

5. Roles, Services and Authentication

5.1 Roles

The module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto Officer roles. The module does not allow concurrent operators. The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the module. No further authentication is required. The Crypto Officer is responsible to set the key for the cipher operation.

5.2 Services

The module provides only Approved services which utilize algorithms listed in Table 5:

Service	Roles		CSP	CSP Access
	User	CO		R = Read W = Write X = Execute
Supply an NVMe Protocol Data Unit (PDU) for encryption	✔	✔	Key1 and Key2	R, W, X
Supply an NVMe PDU for decryption	✔	✔	Key1 and Key2	R, W, X

[1] ARM Microcontroller Bus Architecture

On-demand Self-Test (Self-Test is executed automatically when device is booted or restarted on-demand by using the self-test trigger from external software)	✔	✔	N/A	N/A
Initialization	✔	✔	N/A	N/A
Zeroization	✔	✔	Key1 and Key2	W
Status Output	✔	✔	N/A	N/A

Table 3 - Approved Services and Role allocation

5.3 Authentication

There is no operator authentication; assumption of role is implicit by the used service(s). The User and CO roles have access to all module services; there is no separation of role access.

6. Physical Security

NVMe DPSC is a sub-chip module implemented as part of the IN762 SoC, which is the physical boundary of the sub-chip module. The IN762 SoC is a single chip with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

7. Operational Environment

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

The module is tested in the following single-chip operational environment:

- Google IN762 SoC B0

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

The module implements the following approved algorithms in hardware:

Data Path Security Cluster (DPSC) AES Engine version 2.3.1 Algorithm Implementations					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
A1188	AES	256-bits	SP 800-38A	ECB[2]	Encryption, Decryption
	XTS[3]	256-bits	SP 800-38E	XTS	Encryption, Decryption

Table 4 - NVMe DPSC Approved Algorithms

8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 5. The CSP access policy is denoted in Table 3 above.

Keys and CSPs	Description	Algorithm and Key Size	Generation	Input / Output Method	Storage	Zeroization
Key1	Bulk encryption Key	256-bit value	N/A. Provided by calling device	Input via direct CSR interface. Never Exits the module	Key cache SRAM	Zeroized on reset
Key2	Tweak Key	256-bit value	N/A. Provided by calling device	Input via direct CSR interface. Never Exits the module	Key cache SRAM	Zeroized on reset

Table 5 - Approved Keys and CSPs

8.3 Key Generation

The module does not provide any key generation service or perform key 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 software) by the Crypto Officer or User. 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 key establishment methods.

8.4 Key Storage and Zeroization

All keys and CSPs are stored in 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 IN762 SoC, it will zeroize all CSPs contained within the module.

[2] Crypto Engine only utilizes AES XTS. AES ECB is not callable in NVMe. It tested under ACVTS to demonstrate the forward cipher function as required in the CAVP FAQ.

[3] AES-XTS implementation is used for storage purposes only.

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. Self-tests

FIPS 140-2 requires self-tests to ensure the correctness of the cryptographic functionality at start-up. Some functions require conditional tests during normal operation of the module.

If any of the tests fail, the module will return an error code and transition to an error state where no functions can be executed. An operator can attempt to reset the state by cycling the power. However, the repeated failure of a self-test may require the module to be replaced.

9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. 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). The module will enter an error state and no services can be accessed by the operator.

The module implements the following power-on self-tests in the NVMe DPSC Module:

Type	Test Description
Encrypt KAT	XTS-AES 256 encryption (forward cipher function)
Decrypt KAT	XTS-AES 256 decryption (inverse cipher function)

Table 6 - Power-On Self-Tests

The module performs all power-on self-tests automatically when it is initialized. Power-on self-tests must pass before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module or by sending a self-test trigger signal bit from external software.

Note: The module is implemented entirely in hardware and is non-modifiable. Therefore, the integrity test requirements do not apply.

9.2 Conditional Self-Tests

Conditional self-tests are run under specific conditions, such as during key generation. Though the module does not perform key generation, per IG A.9, the module implements the following conditional tests:

Type	Test Description
Key Equality Check (Encrypt)	Prior to use of an XTS key, the module verifies that Key1!=Key2 and the key is present in the keycache.
Key Equality Check (Decrypt)	Prior to use of an XTS key, the module verifies that Key1!=Key2 and the key is present in the keycache.

Table 7 - Conditional Self-Tests

In the event that either of the above conditional tests fail, the output of the module will be driven to 0 for a given payload. However, the module will not enter an error state, rather the encryption or

decryption request will fail, and the module will continue to process payload encryption and decryption operations if the subsequent keys are valid and not equal.

9.3 Critical Function Tests

The module does not implement any specific critical function tests.

10. Mitigation of Other Attacks

No specific claims for this section.

11. Crypto Officer and User Guidance

No configuration of the module or installation steps are required from the operator. When the module is powered on its power-up self-tests are executed without any operator intervention. The module enters the Approved mode of operation automatically if the power-up self-tests complete successfully. If any of self-tests fail during power-up, the module will transition to an 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. If it is unavailable, it is in the error state or has not been properly initialized.

12. Glossary

Term	Description
AMBA	ARM Microcontroller Bus Architecture
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CSR	Control/Status Register
CTR	Counter
DMA	Direct Memory Access
DPSC	Data Path Security Cluster
ECB	Electronic Codebook
FIPS	Federal Information Processing Standards
IG	Implementation Guidance
IMC	Integrated Management Complex
KAT	Known answer test
NMF	NIC Management Fabric
NPI	NVMe Protocol Initiator
NPL	NVMe Protocol Layer
NVMe	Non-volatile Memory express
PDU	Protocol Data Unit
SoC	System On Chip
SRAM	Static Random Access Memory
SSD	Solid State Drive
VM	Virtual Machine
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Table 8 - Glossary of Terms