Microchip Technology, Inc.

NV-2108 Flashtec™ PCIe NVRAM Drive

Hardware Version: NV-2108

Firmware Version: 3.2.15.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2

Document Version: 0.8

Prepared for:

Microchip Technology, Inc.
2355 West Chandler Boulevard
Chandler, AZ 85224
United States of America

Phone: +1 480 792 7200
www.microchip.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the NV-2108 Flashtec™ PCIe[1] NVRAM[2] Drive from Microchip Technology, Inc. (hereafter referred to as Microchip). This Security Policy describes how the Microchip NV-2108 Flashtec™ PCIe NVRAM Drive meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[3] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The Microchip NV-2108 Flashtec™ PCIe NVRAM Drive is referred to in this document as “NV-2108” or “the module”

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Microchip website (https://www.microchip.com) contains information on the full line of products from Microchip.
- 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.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Microchip. Except for this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Microchip and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Microchip.

[1] PCIe – Peripheral Component Interconnect Express
[2] NVRAM – Non-volatile Random Access Memory
[3] U.S. – United States

2. Microchip NV-2108 Flashtec™ PCIe NVRAM Drive

2.1 Overview

Microchip is a leading developer of solid-state drives (SSD). The Microchip NV-2108 Flashtec™ PCIe NVRAM Drive is an 8 GB[4], 2.5-inch form factor NVRAM dual port drive that provides outstanding reliability, performance, and security. The Microchip NV-2108 is inserted directly into a DellEMC server at the factory or by the customer during installation. The hardware and firmware are pre-loaded, so all security features are available at start-up.

The Microchip NV-2108 supports cryptographic services that are performed using FIPS 140-2 validated algorithms. All data is encrypted using AES[5] 256-bit hardware-based encryption. Keys are generated using a FIPS-Approved DRBG[6] that is internal to the device on a Microchip ATECC608A chip.

The Microchip NV-2108 is a dual-host device accessible to a host appliance application through a well-defined set of APIs[7]. The APIs provided access to firmware that is used for device configuration and management. Figure 1 and Figure 2 below show the top and bottom view (respectively) of the Microchip NV-2108.

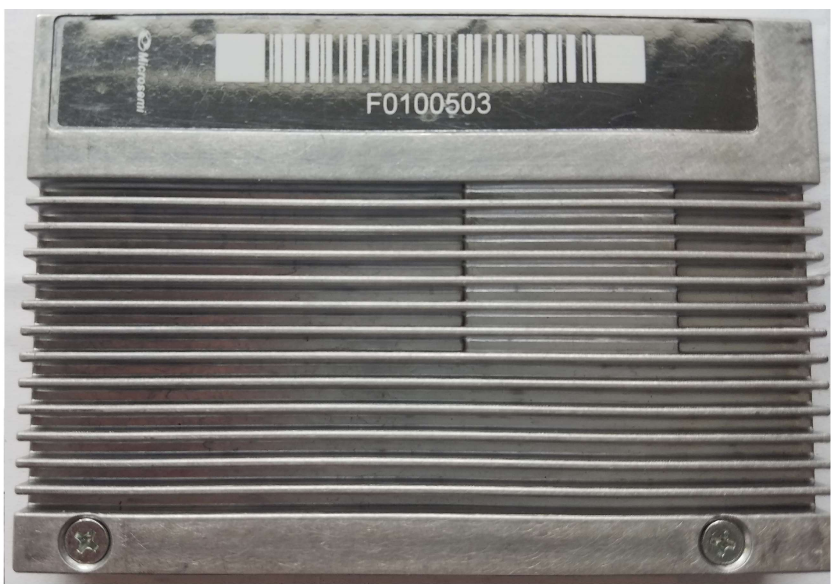

Figure 1 – Microchip NV-2108 (Top View)

[4] GB - GigaByte
[5] AES – Advanced Encryption Standard
[6] DRBG – Deterministic Random Bit Generator
[7] API – Application Programming Interface

Figure 2 – Microchip NV-2108 (Bottom View)

The NV-2108 is validated at the FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A[8]
7	Cryptographic Key Management	2
8	EMI/EMC[9]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

[8] N/A – Not Applicable
[9] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The NV-2108 Flashtec™ PCIe NVRAM Drive is a Hardware module with a multiple-chip embedded embodiment. The overall security level of the module is 2. The cryptographic boundary is defined as the entire NV-2108 device.

2.2.1 Approved and Non-Approved Algorithms

The module includes the following sources for cryptographic algorithm implementations:

- Microchip's ATECC608A, which runs on a Microchip AVR/ARM MCU[10] and provides a hardware-based DRBG
- Flash Controller (F32P08xG3), which provides a hardware-based 256-bit XTS[11]-AES implementation for encryption and decryption
- Microchip's device firmware, which provides all other cryptographic functions employed by the module, interacts directly with the module hardware without the use of a defined operating system

The module implements the FIPS-Approved algorithms listed in Table 2, Table 3, Table 4, and Table 5 below.

Table 2 – FIPS-Approved Algorithms (Microchip Firmware Cryptographic Library v1.01.01)

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C2171	AES[12]	FIPS PUB 197 NIST SP 800-38A	ECB[13]	256	Encryption/decryption *Used as a prerequisite for AES KW[14]*
		FIPS PUB 197 NIST SP 800-38F	KW	256	Key Wrap
C2171	HMAC[15]	FIPS PUB 198-1	SHA2-256-128 SHA2-256-192 SHA2-256	256	Message authentication *Used as a prerequisite for PBKDF[16]*
Vendor Affirmed	PBKDF	NIST SP 800-132	Option 1a with HMAC SHA2-256	256	Password-based key derivation
C2171	RSA[17]	FIPS PUB 186-4	PKCS[18] #1 v1.5	3072	Digital signature verification

[10] MCU – Microcontroller
[11] XTS – XEX-based tweaked-codebook mode with ciphertext stealing
[12] AES – Advanced Encryption Standard
[13] ECB – Electronic Codebook
[14] KW – Key Wrap
[15] HMAC – (keyed-) Hashed Message Authentication Code
[16] PBKDF – Password Based Key Derivation Function
[17] RSA – Rivest-Shamir-Adleman
[18] PKCS – Public Key Cryptography Standards

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C2171	SHS[19]	FIPS PUB 180-4	SHA2-256	-	Message digest *Used to hash the CO and User Authentication String* *Used as a prerequisite for PBKDF and RSA*

Table 3 – FIPS-Approved Algorithms (Microchip F32P08xG3 Flash controller ASIC – PCIe Port 0, Revision YE)

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C2172	AES	FIPS PUB 197 NIST SP 800-38A	ECB	256	Encryption/decryption *AES-ECB used as a prerequisite for AES-XTS*
		FIPS PUB 197 NIST SP 800-38E	XTS	256	Encryption/decryption *AES-XTS is used for storage application purposes only*

Table 4 – FIPS-Approved Algorithms (Microchip F32P08xG3 Flash controller ASIC – PCIe Port 1, Revision YE)

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C2173	AES	FIPS PUB 197 NIST SP 800-38A	ECB	256	Encryption/decryption *AES-ECB used as a prerequisite for AES-XTS*
		FIPS PUB 197 NIST SP 800-38E	XTS	256	Encryption/decryption *AES-XTS is used for storage application purposes only*

Table 5 – FIPS-Approved Algorithms (ATECC608A CryptoAuthentication Device)

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
C244[20]	AES	FIPS PUB 197 NIST SP 800-38A	ECB	128	Prerequisite for CTR based DRBG[21]

[19] SHS – Secure Hash Standard
[20] CAVP Cert #C244 supports additional algorithms that are not used by the module. Only the algorithms/modes used by the module are listed.
[21] DRBG – Deterministic Random Bit Generator

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
Vendor Affirmed	CKG[22]	NIST SP 800-133	-	-	Symmetric key generation
C244	DRBG	NIST SP 800-90Arev1	Counter-based (AES)	128	Deterministic random bit generation

The vendor affirms the following cryptographic security method(s):

- As per *NIST SP 800-132*, the module uses PBKDF2 option 1 for DPK[23] key establishment. The PBKDF2 for DPK establishment takes as input a 256-bit salt (all of which is generated by the module's DRBG) with a 32-byte authentication string and produces a random value of 256-bits. In addition, the function has a minimum iteration count of 1,000. The underlying pseudorandom function used in this derivation is HMAC SHA2-256. As required by section D.6 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*, keys derived from the PBKDF2 function are only used for storage applications.

- As per *NIST SP 800-133*, the module uses the FIPS-Approved counter-based DRBG specified in *NIST SP 800-90Arev1* to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified output from the DRBG. The module's DRBG is seeded via a hardware-based entropy source that is internal to the module.

In compliance with IG 7.14, the module generates cryptographic keys whose strengths are modified by available entropy.

The module employs the non-FIPS-approved algorithm implementations shown in Table 6, which are allowed for use in a FIPS-Approved mode of operation.

Table 6 – Allowed Algorithm Implementations

Algorithm	Caveat	Use
NDRNG[24]	-	Seeding for the DRBG

2.3 Module Interfaces

The module is embedded in a general-purpose computer or server. It connects to the host device via a dual-host PCIe connector. The design of this connector supports information flows in four logically distinct and isolated categories:

- Data Input
- Data Output
- Control Input

[22] CKG – Cryptographic Key Generation
[23] DPK – Data Protection Key
[24] NDRNG – Non-Deterministic Random Number Generator

- Status Output

The physical interface for the NV-2108 maps the FIPS 140-2 logical interfaces as shown in Table 7 below.

Table 7 – Module Interface Mappings

Physical Port/Interface	Quantity	Logical Port/Interface	Logical Path(s)
Dual-host PCIe connector (SFF-8639)	1	Data Input	• NVMe Queues 1-128 with opcode of write • NVMe Queue 0 (Admin commands) based on the opcode and sub type
		Data Output	• NVMe Queues 1-128 with opcode of read
		Control Input	• NVMe Queue 0 (Admin commands) based on the opcode and sub type • PCIe configuration messages (CFG_WR)
		Status Output	• PCIe configuration messages (CFG_RD)
		Power	-

2.4 Roles and Services

The sections below describe the module's roles and services and define any authentication methods employed.

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two roles that operators may assume:

- Crypto Officer (CO) – The CO role is responsible for monitoring the overall status of the module, updating the authentication key and zeroizing keys/CSPs.

- User – The User role is responsible for configuring the module and performing encrypt/decrypt operations.

2.4.2 Operator Services

Descriptions of the services available to the CO role and User role are provided in Table 8 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.
- Z – Zeroize: The CSP is zeroized (overwritten or removed from memory)

Table 8 – Mapping of Module Services to Roles, CSPs, and Type of Access

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Update authentication key	✓	✓	Update CO or User authentication key For User role, regenerate DPK and rewrap DEK[25]	API command plus parameters	Status output	CO Authentication String – R, X CO Authentication Key - W User Authentication String – R, X User Authentication Key - W DPK – W DEK - R, W CTR DRBG Entropy – R, W, X CTR DRBG Seed – W, X CTR DRBG "V" Value – W, X CTR DRBG "Key" Value – W, X
Encrypt Data (Write IO)		✓	Encrypt data received from the host to the device	API command plus parameters	Status Output; Encrypted Data	DEK – X
Decrypt Data (Read IO)		✓	Decrypt data sent from the device to the host	API command plus parameters	Status Output; Decrypted Data	DEK – X
Load firmware		✓	Download and activate firmware image	API command plus parameters	Status output	Firmware Load Key – R, X, W
Logout operator	✓	✓	Logout host from current authenticated state	API command plus parameters	Status output	N/A[26]
Backup		✓	Backup the device; Return information about the most recent backup	API command plus parameters	Status output	N/A
Restore		✓	Restore the device from a previous backup	API command plus parameters	Status output	N/A
Set Heartbeat Listening		✓	Start or stop device firmware listening to incoming host heartbeat messages	API command plus parameters	Status output	N/A
Set Device Configuration		✓	Set device configuration parameters	API command plus parameters	Status Output	N/A
Zeroize	✓		Zeroize keys and CSPs	API command plus parameters	Status Output	DEK – Z CO Authentication Key – Z User Authentication Key – Z
Zeroize (with PSID)	✓	✓	Zeroize keys and CSPs	API command plus parameters	Status Output	DEK – Z CO Authentication Key – Z User Authentication Key – Z

[25] DEK – Data Encryption Key
[26] N/A – Not Applicable

2.4.3 Additional Services

The module provides services for which the operator is not required to assume an authorized role. Table 9 lists the services for which the operator is not required to assume an authorized role. None of these services disclose or substitute cryptographic keys and CSPs or otherwise affect the security of the module.

Table 9 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Show Status	Return device status	API command plus parameters	Status Output	N/A
Show Log Pages	Return device log information	API command plus parameters	Status Output	N/A
Perform Self-Tests On-Demand	Perform self-tests on demand	Power cycle Or API command plus parameters	Status Output	N/A
Zeroize (with PSID)	Zeroize keys and CSPs	API command plus parameters (PSID); Power cycle	Status Output	DEK – Z CO Authentication Key – Z User Authentication Key – Z
Initialize device	Perform initialization between the host and the device	API command plus parameters	Status Output	N/A
Get Device Configuration	Get device configuration parameters	API command plus parameters	Status Output	N/A
Set FIPS Security Parameters	Provision FIPS security parameters for device operation. Set CO and User authentication key; Generate DPK and DEK	API command plus parameters	Status output	CO Authentication String – R, X CO Authentication Key – W User Authentication String – R, X User Authentication Key - W DPK – W DEK – W CTR DRBG Entropy – R, W, X CTR DRBG Seed – W, X CTR DRBG “V” Value – W, X CTR DRBG “Key” Value – W, X
Authenticate User	Authenticate the User between the host and device	API command plus parameters	Status output	User Authentication String – R User Authentication Key – R, X
Authenticate CO	Authenticate the CO between the host and device	API command plus parameters	Status output	CO Authentication String – R CO Authentication Key – R, X
Get Device Information	Get device statistical data; Get a list, count, and the unique identifier of all devices in the system; Get a device feature list	API command plus parameters	Status output	N/A

2.4.4 Authentication

The module supports role-based authentication. The CO and User each have a unique 32-byte authentication string, which is entered through the host. The authentication string is sent in the API command to authenticate the operator to the module:

- CO Authentication – `PMC_NVRAM_FIPS_crypto_officer_authenticate`
- User Authentication – `PMC_NVRAM_FIPS_user_authenticate`

For an operator to change roles, they must first log out of the current role they have assumed using the `PMC_NVRAM_FIPS_auth_logout` command. Once logged out, the operator may perform unauthenticated services or re-authenticate to the module using the correct authenticate API command.

The module supports a single authenticated user per port. If an operator attempts to authenticate to a port while another role is logged in to it, access will be denied, and an error returned.

All operators must set a 32-byte authentication string (the calling application is responsible for enforcing the length of the authentication string). All 256 characters in the ASCII[27] table are allowed.

The chance of a random attempt falsely succeeding is:

=1 per 256^{32} possible passwords
=1 per 1.16×10^{77}

which is a lesser probability than 1 per 1,000,000 as required by FIPS 140-2.

The fastest PCIe connection from the host application to the module is 1000 MB/s . At most 60,000 MB per minute (60,000 MB * 8 Mb = 480,000Mb or 4.8×10^{11} bits per minute) of data can be transmitted in one minute. The password is 32 bytes (8 bits per byte x 32 bytes = 256 bits), meaning 1.875×10^{9} passwords can be passed to the module (assuming there is no overhead). This equates to a $1{:}6.1755781 \times 10^{67}$ chance of a random attempt will succeed, or a false acceptance will occur in a one-minute period, which is less than the required probability.

2.5 Physical Security

The NV-2108 is a multiple-chip embedded cryptographic module. The contents of the module, including hardware components, firmware, plaintext keys, and CSPs are all protected by the module enclosure. The module enclosure consists of a hard production-grade metal case that completely encloses all internal components. The module uses Microtrace tamper-evident labels to secure the enclosure. Any attempts to open the enclosure will break the labels, leaving visible evidence of the attempt. Any attempts to remove a label will leave a residue, providing visible evidence of the attempt. Removed labels cannot be reapplied to the enclosure.

All tamper-evident labels are applied to the NV-2108 at the factory prior to being installed into the host device. See section 3.1 below for instructions on verification of label placement.

[27] ASCII – American Standard Code for Information Interchange

As all deployments and environments have different requirements, tamper evident labels shall be inspected at a frequency defined by the CO. If the CO identifies evidence of tampering, remove the module from operation and contact Microchip Customer Support immediately.

2.6 Operational Environment

The operational environment of the module does not provide the module operator with access to a general-purpose operating system (OS). The module employs a non-modifiable operating environment. The module’s firmware (v3.2.15.0) runs on a fixed firmware core affinity. The firmware integrity test protects against unauthorized modification of the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 10.

Table 10 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Firmware Integrity Code	CRC[28]-16	Generated externally. Installed at the factory and via the host application whenever new firmware is downloaded	Never exits the module	Plaintext in EEPROM[29]	N/A	Verification during power-up firmware integrity check
Firmware Load Key	3072-bit RSA public key	Generated externally, input in plaintext form during the manufacturing process Updated when new firmware is loaded	Never exits the module	Plaintext in EEPROM	N/A	Verification during firmware load test
DPK	256-bit AES-KW key	Derived internally from the User authentication string (password) via PBKDF2 with HMAC SHA2-256.	Never exits the module	Plaintext in volatile memory (Ephemeral)	Zeroized after encrypting/decrypting the DEK	Encrypt/decrypt DEK
DEK	AES-XTS (2x256-bit AES-XTS key)	Generated internally via Approved DRBG	Never exits the module	Encrypted in EEPROM (Wrapped by DPK)	API call	Encryption/decryption
CO Authentication String	Alphanumeric string	Generated externally, input in plaintext form via the host application	Never exits the module	Plaintext in volatile memory (Ephemeral)	Zeroized once the CO Authentication Key is created	Derives the CO Authentication Key
CO Authentication Key	256-bit hash	Generated internally. Calculated as a hash of the CO authentication string.	Never exits the module	Plaintext in EEPROM	API call	Authenticate CO to the module

[28] CRC – Cyclic Redundancy Check
[29] EEPROM – Electrically Erasable Programmable Read-Only Memory

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
User Authentication String	Alphanumeric string	Generated externally, input in plaintext form via the host application	Never exits the module	Plaintext in volatile memory (Ephemeral)	Zeroized once the User Authentication Key and DPK are created	Derives the User Authentication Key Used in the PBKDF to generate the DPK
User Authentication Key	256-bit hash	Generated internally. Calculated as a hash of the User authentication string.	Never exits the module	Plaintext in EEPROM	API call	Authenticate User to the module
CTR DRBG Entropy[30]	256-bit value	Generated internally from NDRNG	Never exits the module	Plaintext in volatile memory	Overwritten when reseed counter is zero and a new instantiation is performed	Entropy input for seed generation of CTR DRBG
CTR DRBG Seed	256-bit value	Generated internally via Approved DRBG	Never exits the module	Plaintext in volatile memory	Overwritten when reseed counter is zero and a new instantiation is performed	Seed material for instantiation of CTR DRBG
CTR DRBG 'V' Value	128-bit value	Generated internally via Approved DRBG	Never exits the module	Plaintext in volatile memory	Overwritten when reseed counter is zero and a new instantiation is performed	Internal state value used with CTR DRBG
CTR DRBG 'Key' Value	128-bit AES key	Generated internally via Approved DRBG	Never exits the module	Plaintext in volatile memory	Overwritten when reseed counter is zero and a new instantiation is performed	Internal state value used with CTR DRBG

****Keys derived from the PBKDF2 function shall only be used for storage applications.***

[30] The min-entropy is 0.910582 bits per bit of entropic data, which far exceeds the entropy rate of 0.5 that is required seed the DRBG to its maximum security strength of 128 bits. When the DRBG requests 256 bits for its entropy input, it receives at least 128 bits of entropic material.

2.8 EMI / EMC

The module's host devices were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed automatically by the module when the module is first powered up and loaded into memory as well as conditionally. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The NV-2108 performs the following self-tests at power-up:

- Firmware integrity check – CRC-16 EDC[31]
- Firmware algorithm self-tests
    - AES-ECB encrypt and decrypt KATs
    - AES-KW (using AES-ECB) wrap and unwrap KATs[32]
    - SHA2-256 KAT
    - HMAC SHA2-256-128 KAT
    - PBKDF2 using HMAC SHA2-256 KAT
    - RSA Signature Verification (3072-bit)
- Hardware algorithm self-tests – Port 0
    - XTS-AES encrypt and decrypt KATs
- Hardware algorithm self-tests – Port 1
    - XTS-AES encrypt and decrypt KATs
- ATECC608A CryptoAuthentication Device
    - CTR DRBG KAT

The successful completion of all power-up self-tests is indicated in the FSM log page by the state: FSM_STATE_OPERATIONAL, and by an all-zeros security-test bit mask.

2.9.2 Conditional Self-Tests

The NV-2108 performs the following conditional self-tests:

- Firmware conditional self-tests
    - Firmware Load Test
- Hardware conditional self-tests – Port 0
    - AES-XTS duplicate key test
- Hardware conditional self-tests – Port 1
    - AES-XTS duplicate key test

[31] EDC – Error Detection Code
[32] KAT – Known Answer Test

The ATECC608A CryptoAuthentication Device continuously performs a Repetitive Count Test[33] (RCT) per *NIST SP 800-90B* section 4.4.1 and an Adaptive Proportion Test (APT) per *NIST SP 800-90B* section 4.4.2. These tests monitor the health of the entropy produced from the noise source and provide an error if the entropy drops below 0.8.

2.9.3 Critical Functions Self-Tests

The module performs the following DRBG health checks as specified in section 11.3 of *NIST SP 800-90Arev1* at power-up and conditionally when a random number is requested:

- Instantiate Function
- Generate Function
- Uninstantiate Function

The module does not perform a Reseed Function. If the reseed counter rolls over, the module performs the Instantiate Function, which erases the previous internal state and creates a new one. These tests are performed conditionally and at module power-up.

2.9.4 Self-Test Failures

The module integrity check (CRC-16 code verification) is performed during the bootup process. If the integrity check fails, all operations stop. The only action available from this state is to power-cycle the module, which will trigger the re-execution of the integrity test. If the failure persists, then Microchip Customer Support must be contacted.

During power-up the module executes the algorithm implementation power-up self-tests and the DRBG health checks. If any of these tests fail, the module enters a critical error state, and an error message is written to the log files. In this state, cryptographic operations are halted, and the module inhibits all data output from the module. The only action available from this state is to power-cycle the module, which will trigger the re-execution of the integrity test and power-up self-tests. If the failures persist, then Microchip Customer Support must be contacted.

If the conditional XTS-AES duplicate key test fails, the module writes a message to the log file and enters a critical error state. The module must be power cycled to clear the error state.

When a random number is requested, the ATECC608A CryptoAuthentication Device (crypto chip) is awakened. The firmware notifies the crypto chip to perform the DRBG KAT and DRBG Health Checks. The RCT and APT are run autonomously and run continuously. If there is an error on any of these tests, then an error is returned to the firmware. In this case, the firmware sends a request to the crypto chip to sleep, transitions to a soft error state, logs the error, and returns to a conditional self-test state to automatically retry the tests. This cycle is attempted up to five times. If there is a failure on the fifth attempt, the module transitions to a critical error state, an error message is recorded, and all data services are inhibited. The module must be restarted to clear the error state. When a status of "success" is returned for these tests, then the random number is generated.

[33] The ATECC608A CryptoAuthentication Device implements the RCT in compliance with IG 9.8

If the Firmware Load conditional self-test fails, the module enters a soft error state. No firmware is loaded, and a message is logged to the log files. Once the message is logged, the error state is cleared, and the module returns to the User Services state from which it was initiated.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Installation and Setup

The module is shipped to the customer in a non-configured state. The operator is responsible for the initial setup, configuration, and provisioning necessary to place the module in the FIPS-Approved mode of operation. The operator must read all applicable Microchip documentation prior to starting the installation.

The following sections provide references to step-by-step instructions for the setup, configuration, and provisioning of the NV-2108. If followed as per this guidance, once complete the module is ready to operate in a FIPS-Approved mode of operation.

3.1.1 Initial Setup

The module is inserted into the DellEMC server. The operator must confirm that the module is securely inserted into the slot and ready for operation. If the module is provided separately or not inserted correctly, the operator must inspect the module to ensure all tamper evident labels are in place. Figure 3 below shows the tamper evident label placement on the module.

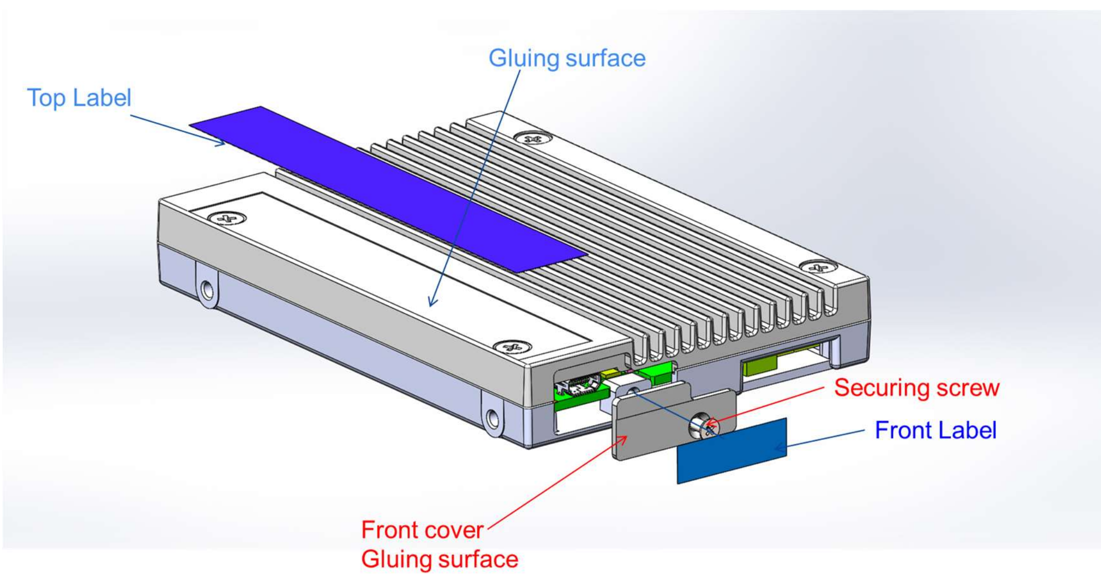

Figure 3 – Tamper Evident Label Placement

Once label placement is confirmed, the operator must perform the following steps to insert the module into the host server:

1. Ensure the host server is powered off. Disconnect the power and any network cables.
2. Select an available PCIe U.2 (SFF-8639) slot that is compatible with the module model.
3. Insert the module into the slot and press gently but firmly until it clicks into place.
4. Close the host server cabinet, reconnect the power cord and network cables, and power-up the system.

For additional information regarding initial setup of the module, please refer to the Microchip *Installation and User Guide*.

3.1.2 Initial Configuration

To configure the module in a FIPS-Approved mode of operation, the operator must set the CO and User operator Authentication Strings. These Authentication Strings must have a length of 32 bytes (the calling application is responsible for enforcing this criteria). All 256 characters in the ASCII table are allowed.

For additional information regarding initial configuration of the module, please refer to the Microchip *Installation and User Guide*.

3.1.3 Initial Provisioning

To provision the module for FIPS mode operation, the operator must send the `PMC_NVRAM_FIPS_set_security_parameters` command from the host appliance to the module. This command contains the CO and User Authentication Strings. This command generates the following:

a) CO Authentication Key
b) User Authentication Key
c) DPK (Ephemeral)
d) DEK

Once these security parameters are generated, the module moves into a FIPS-Approved general services operational mode. If the generation of any of these parameters fails, the module cannot move out of a provisioning state. The module must be rebooted, and provisioning retried.

3.2 Crypto Officer Guidance

The CO is responsible for ensuring that the module is operating in the FIPS-Approved mode of operation. When configured and operated according to the guidance in this Security Policy (including the previous instructions in section 3.1 above, the module only runs in the FIPS-Approved mode of operation.

3.2.1 Management

Once installed and configured, the CO is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. Please refer to the sections below for guidance that the CO must follow to ensure that the module is operating in a FIPS-Approved manner.

3.2.2 On-Demand Self-Tests

Although power-up self-tests are performed automatically during module power up, they can also be manually launched on demand. Self-tests can be executed on-demand by power-cycling the module.

3.2.3 Zeroization

The module's CSPs reside in volatile and non-volatile memory. All CSPs (except the Firmware Load Key) are zeroized by running the `PMC_NVRAM_FIPS_clear_security_params` command. Once the command executes successfully, the module must be power-cycled to rerun power-up self-tests and bring the module to a provisioning state where security parameters may be recreated.

3.2.4 Monitoring Status

The CO shall be responsible for regularly monitoring the module's status for the FIPS-Approved mode of operation. When configured according to the CO's guidance, the module only operates in the FIPS-Approved mode. Thus, the status of the module when operational is always in the FIPS-Approved mode.

The CO may check the status of the module by running the `PCM_NVRAM_info_get` command with the group parameter "NVRAM_INFO_GROUP_GENERAL". A value of "1" in the fips_mode field of the return structure indicates that the module is in FIPS mode.

3.3 User Guidance

The User role does not have the ability to configure sensitive information on the module. The User must be diligent to select strong passwords and must not reveal their password to anyone.

3.4 Additional Guidance and Usage Policies

This section notes additional policies below that must be followed by module operators:

- The operator sets the CO and User password in the calling application. The calling application is responsible for ensuring that the password is 32 bytes in length. If the password is not 32 bytes in length, the calling application must return an error and the operator must create a different password.

3.5 Non-FIPS-Approved Mode

When initialized, configured, and operated according to the guidance in this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

4. Acronyms

Table 11 provides definitions for the acronyms used in this document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
APT	Adaptive Proportion Test
ASCII	American Standard Code for Information Interchange
CAVP	Cryptographic Algorithm Validation Program
CCCS	Canadian Centre for Cyber Security
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CRC	Cyclical Redundancy Check
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DEK	Data Encryption Key
DPK	Data Protection Key
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
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
GB	GigaByte
GPC	General Purpose Computer
GUI	Graphical User Interface
HMAC	(keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Acronym	Definition
ID	Identifier
IDP	Identity Provider
IG	Implementation Guidance
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
KSK	Key Signing Key
KW	Key Wrap
LED	Light Emitting Diode
MAC	Media Access Control
MCU	Microcontroller
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
OS	Operating System
PBKDF2	Password-based Key Derivation Function 2
PCIe	Peripheral Component Interconnect Express
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standards
RAM	Random Access Memory
RCT	Repetitive Count Test
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
U.S.	United States
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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