# Macronix ArmorFlash MX78 series Cryptographic Module FIPS 140-2 Security Policy

Version : V1.02

Date : April 15, 2022

## Revision History

| Version | Description | Date |
|---|---|---|
| 1.00 | Update page 7, 14 | 2021/12/20 |
| 1.01 | Update page 4,9 | 2022/03/31 |
| 1.02 | Update page 7 | 2022/4/19 |

# Table of Contents

# 1 Introduction

## 1.1 Purpose

This is a non-proprietary security policy for the Macronix ArmorFlash MX78 series cryptographic module, hereafter denoted ArmorFlash. This Security Policy describes how the cryptographic module meets the requirements for a FIPS 140-2 level 2 validation as specified in the FIPS 140-2 standard. This Security Policy is part of the evidence documentation package to be submitted to the validation lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, please visit http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

## 1.2 Scope

This Security Policy specifies the security rules under which the cryptographic module operates its major properties. It does not describe the requirements for the entire system, which makes use of the cryptographic module.

## 1.3 Security Level

The module meets the overall requirements applicable to FIPS140-2 Security Level 2. In the individual requirement sections of FIPS 140-2 the following Security Level ratings are achieved:

| Section | Section Title | Level |
|---|---|---|
| 1 | Cryptographic Module Specification | 2 |
| 2 | Cryptographic Module Ports and Interfaces | 2 |
| 3 | Roles, Services, and Authentication | 3 |
| 4 | Finite State Model | 2 |
| 5 | Physical Security | 2 |
| 6 | Operational Environment | N/A |

| Section | Section Title | Level |
|---|---|---|
| 7 | Cryptographic Key Management | 2 |
| 8 | EMI/EMC | 2 |
| 9 | Self-tests | 2 |
| 10 | Design Assurance | 2 |
| 11 | Mitigation of Other Attacks | 2 |

Table 1 – Security Level per FIPS 140-2 Section

# 2 Cryptographic Module Specification

The ArmorFlash is intended for use in general purpose computing environments, as a device peripheral to the CPU, with the application controlling the usage of the module.
The ArmorFlash is a single chip cryptographic hardware module as defined in FIPS 140-2. The single silicon chip is encapsulated in a hard, opaque, production grade integrated circuit (IC) package. The security module supports SPI interfaces.

## 2.1 Cryptographic Module Boundary

The cryptographic boundary is defined as the perimeter of the IC package. The perimeter of the module forms the cryptographic boundary of this FIPS140-2 Security Level 2 compliant single-chip cryptographic module.

The module block diagram and logical boundary are shown as following.

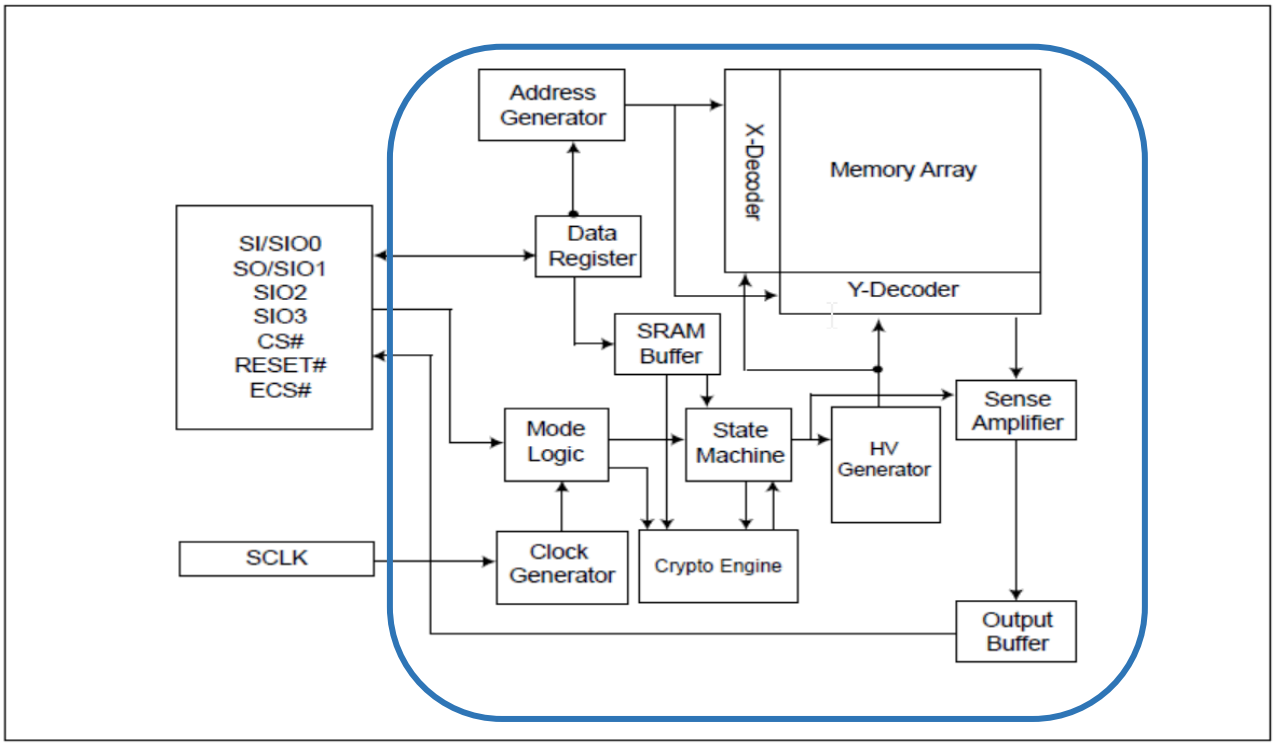


Figure 1 – Cryptographic Module Block Diagram

## 2.2 Hardware

The Module is a single-chip module that contains a Memory, X/Y-Decoder, Sense Amplifier, HV Generator, Address Generator, Data Register, SRAM, Mode Logic, Clock generator, State Machine and Crypto Engine. The boundary of the single-chip module is the edges and surfaces of the integrated circuit die. No components are excluded from the cryptographic boundary.

The module is available in configurations shown in table 2.

| Hardware Version | Voltage | Density |
|---|---|---|
| MX78U64A00F/ MX78U64B00G<br>MX78U128A00F/ MX78U128B00G<br>MX78U256A00F/ MX78U256B00G | 1.8V | 64Mb<br>128Mb<br>256Mb |
| MX78L64A00F/ MX78L64B00G<br>MX78L128A00F/ MX78L128B00G<br>MX78L256A00F/MX78L256B00G | 3.0V | 64Mb<br>128Mb<br>256Mb |

Table 2 – Cryptographic Module Configurations

The following figures show the physical form of the module.


Figure 2 – Top View

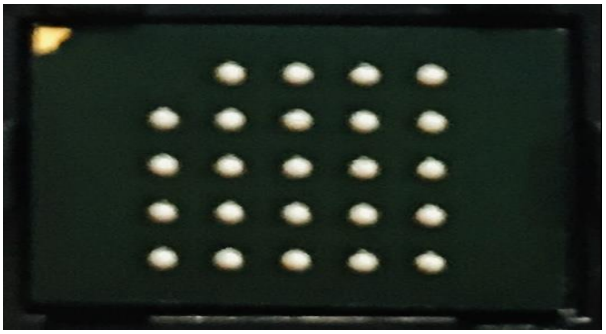

Figure 3 – Bottom View

This module comprises the following components.

- Memory
- X/Y-Decoder
- Sense Amplifier
- HV Generator
- Address Generator
- Data Register
- SRAM
- Mode Logic
- Clock Generator
- State Machine
- Crypto Engine that includes Random number generator, AES, HMAC, ECC CDH

### 2.3 FIPS Approved Mode of Operation

The module shall not contain a non-FIPS Approved mode of operation. Hence, as configured during production process, the module only operates in a FIPS Approved mode of operation. When the module is powered up and successfully completes the power up self-test, the module enters the FIPS approved mode of operation. The module does not implement bypass or maintenance modes.

## 2.4 FIPS Approved Security Functions

The following table gives the list of FIPS Approved security functions that are provided by the module.

| Security Function | Details | CAVP Cert. # |
|---|---|---|
| AES | ECB (e/d; 128, 256 ) ; CTR (e; 256) | C1928 |
| AES GCM | GCM (e/d; 128) | C1928 |
| AES CCM | CCM (e/d; 256) | C1928 |
| SHS | SHA-256 (BYTE-only) | C1928 |
| DRBG | CTR_DRBG (AES-256Key) | C1928 |
| HMAC | HMAC-SHA256 (Key Size Ranges Tested: KS<BS) | C1928 |
| CVL | ECC CDH Primitive (P-256) | C1928 |
| KBKDF | CTR | C1928 |

Table 3 – FIPS Approved Security Functions

Note:

Conforming to IG A.5, scenario #3: The AES GCM IV is constructed in its entirety internally deterministically, consisting of 96 bits as specified in SP800-38D, section 8.2.1.

The module does not use DRBG to generate any key. NDRNG is a non-security function with no security claimed and is allowed to be used in Approved mode to feed seed to DRBG.

# 3 Cryptographic Module Ports and Interfaces

The physical port of ArmorFlash is the SPI bus. The logical interfaces and their mapping to

physical ports of the module are described below:

## 3.1 Physical Ports

| Contact (Pin) | Contact Assignments | I/O | Description |
|---|---|---|---|
| C2 | CS# | Input | Chip Select |
| B2 | SCLK | Input | Clock Input |
| A4 | RESET# | Input | Hardware Reset Pin |
| A5 | ECS# | Output | ECC Correction Signal |
| D3 | SI/SIO0 | Input/Output | Serial Data Input (for 1xI/O)/ Serial Data Input&Output (for 2xI/O or 4xI/O) |
| D2 | SO/SIO1 | Input/Output | Serial Data Output (for 1xI/O)/ Serial Data Input&Output (for 2xI/O or 4xI/O) |
| C4 | WP#/SIO2 | Input/Output | Write Protection Pin/ Serial Data Input&Output (for 4xI/O) |
| D4 | NC/SIO3 | Input/Output | No Connection/ Serial Data Input&Output (for 4xI/O) |
| B4 | VCC | Power | Power Supply |
| B3 | GND | Power | Ground |

Table 4– Physical Ports

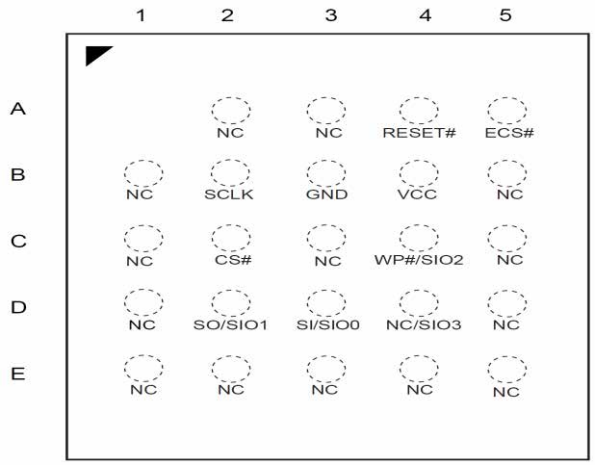


Figure 4 – Physical Ports

## 3.2 Logical Interfaces

| Logical Interface | Physical Port |
|---|---|
| Data Input | SIO0/ SIO1/ SIO2/ SIO3 |
| Data Output | SIO0/ SIO1/ SIO2/ SIO3 |
| Control Input | CS#/ RESET#/ SCLK/ SIO0/ SIO1/ SIO2/ SIO3 |
| Status Output | SIO0/ SIO1/ SIO2/ SIO3/ ECS# |
| Power | VCC, GND |

Table 5 – Logical Interfaces

The logical interfaces are kept logically separate when sharing a physical port by SPI (Serial Peripheral Interface) flash protocol defined by JEDEC standard. Information flows for the data input, data output, control input, and status output interfaces are encapsulated into SPI commands and multiplexed over the same physical interface. They do not use the same physical port at the same time. Basically all commands are initiated from the host(controller) to inform ArmorFlash what to do. The host(controller) will always act as master and ArmorFlash as a slave. The direction of the transmission is assumed to be known to both ArmorFlash and the host, and well defined in datasheet.

# 4 Roles, Services and Authentication

The module supports two roles, Crypto Officer (CO) and User, and enforces the separation of these roles by restricting the services available to each one. The cryptographic module enforces the separation of roles using identity-based operator authentication. One authentication is allowed per module reset, i.e., an operator must re-authenticate after a power down or reset.

## 4.1 Roles

- **Crypto Officer Role**

The CO role is authorized by using the identical root key with host and available after the root key has been established. This role is responsible for generating the secure session by SSGEN command. And use KCONF command to confirm the secure session on both of ArmorFlash and host are the symmetric.

- **User Role**

This role is authorized to read/write user data and use cryptographic services by using the symmetric secure session.

The module does not implement any maintenance interface, thus there is no maintenance role defined.

## 4.2 Identification and Authentication

The module implements identity-based authentication which is identified by key ID entry by the operator.

In FIPS approved mode of operation, ArmorFlash uses a mechanism for mutual authentication that consists of:

1. Activate a secure session that is a derivation of user root key by SSGEN command.
2. Use KCONF command to confirm the secure session on both of ArmorFlash and host are the symmetric.
3. Use HSDA command to authenticate user identity by InMAC check in ArmorFlash before access user data.

The strength of the authentication mechanism conforms to the following specifications.

The probability that a random attempt will succeed using this authentication method is:

1/2^128 = 2.94E-39 (for any of AES GCM-128, which has 128 bit key length)

The module enforces a maximum of 2^20 failed authentication attempts. If the maximum failure authentication reached, the module will be halted state. The probability that a random attempt will succeed over a one minute interval is: 2^20/2^128 = 3.08E-33. This is significantly lower than the requirement of 1/100000.

### 4.3 Services

The services provided by the module to each role in terms of commands are specified in the table below (for a brief description of the services see table “Services Description” hereinafter).

| Services (Commands) | Crypto Officer | User |
|---|---|---|
| SSGEN | V | |
| KCONF | V | |
| PGRD | V | V |
| INFRD | V | V |
| SPRWR | V | V |
| NGEN | V | V |
| MC | V | V |
| HSDA | | V |
| SSEND | V | V |
| KZERO | V | V |
| ODTEST | V | V |
| RST | V | V |

Table 6 – Roles and Services

Details of Services are given in the following table as well as the CSPs access when performing the services.

| No. | Service (Command) | Service Description | CSPs /Keys | Type of Access |
|---|---|---|---|---|
| 1. | SSGEN | Generate a secure session | Root key/Session key | Use/ Generate |
| 2. | SSGEN | Generate a secure session | Root key/Session key | Use/ Generate |
| 3. | KCONF | Key confirmation for as session key | Session key | Use |
| 4. | PGRD | Read plaintext data from data memory or configuration memory | NA | |
| 5. | INFRD | Read ArmorFlash device information | NA | |
| 6. | SPRWR | Write security profile | NA | |
| 7. | NGEN | Generate Nonce from the internal Random Number Generator and import host Nonce | NA | |
| 8. | MC | Increment the non-volatile Monotonic Counter and/or return the counter value | NA | |
| 9. | HSDA | Highly Secure Data Access | Session key | Use |
| 10. | SSEND | End a secure session | Session key | Zeroize |
| 11. | KZERO | Key zeroization | Root key | Zeroize |
| 12. | ODTEST | On-demand health test | NA | |
| 13. | RST | Reset | All violate CSPs/Keys | Zeroize |

Table 7 – Services

## 5 Physical Security

ArmorFlash is an automotive grade, single-chip standalone cryptographic module as defined by FIPS 140-2 and is designed to meet level 2 physical security requirements. It employs physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module. All hardware within the cryptographic boundary is protected.

### 5.1 Physical Security mechanisms as required by FIPS 140-2

The module uses standard passivation techniques and is encapsulated in a hard opaque package to prevent direct observation of internal security components.

## 6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements do not apply to the module in this validation because the module operates in a non-modifiable operational environment.

## 7 Cryptographic Key Management

### 7.1 Critical Security Parameters and Public Keys

The following table provides a list and description of all CSPs and public keys managed by the module.

| CSP/ Public Key | Type | Generate/ Input | Output | Storage | Zeroization | Use |
|---|---|---|---|---|---|---|
| SP800-90A DRBG seed | 384-bit seed value | Generated by the NDRNG | None | Volatile Memory | Power cycle | Used within the SP800-90A DRBG |
| SP800-90A DRBG internal state (“V” and “Key”) | 128-bit AES state V and 256-bit AES key | Generated by the CTR_DRBG | None | Volatile Memory | Power cycle | Internal state of the SP800-90A DRBG |
| Root key (KDK) | Symmetric 256-bit HMAC key | Preloaded in factory | None | Non-Volatile Memory | KZERO command | Used to derive Session key |
| Session key (AES) | Symmetric 128-bit AES key | Key Establishment by automated Key-Derivation Methods | None | Volatile Memory | Power cycle | Encryption / Decryption |
| Session key (HMAC) | Symmetric 256-bit HMAC key | Key Establishment by automated Key-Derivation Methods | None | Volatile Memory | Power cycle | Used to generate HMAC message authentication code |

Table 8 – Critical Security Parameters and Public Keys

### 7.2 Key Generation and Diversification

The root key is defined to be the output of the first step of extraction-then-expansion key-derivation procedure in the key-establishment scheme which has been established in factory. The session key is part of secret keying material derived from the second step of extraction-then-expansion.

### 7.3 Key Entry and Output

All CSP and secure keys are internal generated without entry and output.

### 7.4 Key Storage

The root key is defined to be the output of the first step of extraction-then-expansion key-derivation procedure in the key-establishment scheme, and it is stored in non-volatile memory. The session key is part of secret keying material derived from the second step of extraction-then-expansion, and it is stored in volatile memory.

### 7.5 Key Zeroization

The operator can use KZERO command with power-off/hardware reset to zeroize the module. The KZERO command will program CSP stored in non-volatile memory to all zeros. CSPs stored in volatile memory cannot be restored upon power-off or hardware reset.

### 7.6 RNG Seed Values

During power up initialization, the module use NDRNG to compute DRBG Seed. Any old seed values (which were randomized) are then overwritten with the new computed values. These seed values are temporarily exists in volatile memory and are zeroized by power cycling the module. These values are not accessible to any user.

### 7.7 Key/IV Pair Uniqueness Requirements from SP 800-38D

The module uses 64 bits of the IV field as a name and uses 32 bits as a deterministic non-repetitive counter for a combined IV length 96 bits. The name field includes an encoding of the module name and the name construction allows for at least 2^32 different names.
The counter part of the IV exhausts the maximum number of possible values for a given

session key (e.g., a 32-bit counter starting from 0 and increasing, when it reaches the maximum value of 2^32 -1) the module aborts the session.

Further, at least one of the IV restoration conditions is satisfied for the deterministic non-repetitive counter. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established.

# 8 Electromagnetic Interference/Compatibility (EMI/EMC)

The cryptographic module has been successfully tested and conformed to meet the EMI/EMC requirements according to FCC 47 CFR part 15, subpart B, class A, and received the corresponding certificate of conformity.

# 9 Self-Tests

The module performs both power-on and conditional self-tests. These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention. All data output via the output interface is inhibited while any power-up and conditional self-test is running

Self-Tests failure resulting in the module goes into an Error state. In the error mode, the module no longer responds to further commands, and output any data. One technique to remove the module from the mute mode is to perform reset on the module and start over

## 9.1 Power-up Self-Tests

Each time this cryptographic module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged.

Resetting the cryptographic module provides a means by which the operator can perform the power-up self-tests on demand.

These tests include:

- Cryptographic algorithm testing

Known Answer Tests (KATs) are conducted for each cryptographic algorithm in one mode of operation. Known input data and answers are stored in flash memory. KATs include following:

- ECC CDH
- HMAC
- AES-GCM
- AES-CCM
- KBKDF
- DRBG

KATs function by encrypting/decrypting, hashing a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the calculated output matches the expected (stored in OTPROM) value. The test fails when the calculated output does not match the expected value.

KATs for DRBG function by seeding with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The module also performs Continuous RNG tests for NDRNG described below.

If and only if all power-up self-tests are passed successfully, the cryptographic module performs the command procedure according to the first command and returns the corresponding response and status word via the data output interface and status output interface.

### 9.2 Conditional Self-Tests

- Continuous RNG Tests:

  A continuous RNG test is performed during each use of both DRNG and NDRNG to verify that it is not generating the same value. They are tested by repetition of serial output 1 block (16 bytes) random number to compare each subsequent generation of block with the previous generated block. If the comparison is equal then the module discards the random number and set a re-start up needed state.

# 10 Design Assurance

## 10.1 Configuration Management

Macronix O.I. (OPERATION PROCEDURE SPEC. – ENGINEERING CHANGE CONTROL) defines Design, Engineering or files change procedure. Besides, all the data and information are specified in the Reticle management system and Macronix Document Control Center.

## 10.2 Delivery and Operation

Macronix additional documents define and describe the steps necessary to deliver and operate the module securely.

## 10.3 Guidance Documents

Macronix confidential datasheet and application note defines the guidance for secure operation.

# 11 Mitigation of Other Attacks

This Cryptographic Module is protected against Fault Induction and Probing attacks by State of the Art hardware counter-measures.

- Fault Induction

  The cryptographic module includes hardware protection in order for the chip not to operate in extreme conditions that may cause processing errors that could lead to revealing the values of cryptographic keys or secret elements. Extreme Conditions refer to abnormal temperature, external power supply and external clock supply. The cryptographic module implements temperature detector, voltage detector and using internal clock for cryptographic operation to be alert against operating in abnormal conditions such as extreme temperature, power and external clock, increasing its protection against fault induction.

- Probing attacks

The cryptographic module includes top metal shielding that is a grid of metal layer wires covering bottom peripheral circuits, CSPs and Keys. The shielding consists of dense metal wires routing with irregular pattern and probing attempt detection circuit.

# 12 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

## 12.1 General Security Rules

- The module only implements Approved mode.
- The module does not support a bypass capability.
- No hardware components of the cryptographic module are excluded from the security requirements of FIPS 140-2.
- The module restricts all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module.
- The module logically disconnects the output data path from the circuitry and processes when performing self-tests, key generation, key zeroization, or error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

## 12.2 Identification and Authentication Security Rules

- The module enforces Identity-Based authentication.
- The module provides two distinct operator roles: User role, and the Crypto Officer role.
- Authenticated operators are authorized to assume either supported role.
- The module does not support multiple concurrent operators.
- The module does not support a maintenance interface or role.

- When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
- The module contains the authentication data required to authenticate the operator for the first time.
- The module re-authenticates an operator when it is powered-up after being powered-off.
- The cryptographic module clears previous authentications on power cycle.

### 12.3 Access Control Security Rules

- While processing an operation, prior to returning a response, the module will ignore all other inputs to the module. No output is performed until the operation is completed, and the only output is the operation response.
- The module does not enter plaintext CSPs. Authentication data are entered in encrypted form. Authentication data is not output during entry.
- The module protects secret keys from unauthorized disclosure, modification, and substitution.
- The module generates all keys having at least 128-bits of strength.
- The module establishes all keys being at least as strong as the key being established.
- The module does not support manual key entry.
- The module does not have any external input/output devices used for entry/output of data.
- The module does not perform any cryptographic functions while key loading or in an error state.
- The module does not output of cryptographic keys, intermediate key values, CSPs, or sensitive data.
- The module provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
- The operator commands the module to perform the power-up self-test by cycling power

or resetting the module (pulse the RESET# pin low).

- Power-up self-test is automatically triggered.
- When the Power up Self-Tests fail the module would be in non-operative (“mute”) state.
- The module enters an error state if the Cryptographic Algorithm Test or Continuous Random Number Generator Test fails. This error state may be exited by powering the module off then on.

### 12.4 Physical Security Rules

- The opaque coating of module deters direct observation within the visible spectrum.
- The hard tamper-evident coating provides evidence of tampering, with high probability of causing serious damage to the chip while attempting to probe it or remove it from the module.
- The operator shall check of epoxy coating and contact plate, whether the module is physically intact.
- The operator shall check of film body, in particular opposite to the contact plate, whether the module is physically intact.
- The security provided from the hardness of the module's epoxy encapsulate is claimed at ambient temperature (20 to 25 degrees Celsius or 68 to 77 degrees Fahrenheit) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range.

### 12.5 Mitigation of Other Attacks Security Rules

This Cryptographic Module is protected against Fault Induction and Probing attacks, which is outside of the scope of FIPS 140-2.

## 13 References

[FIPS140-2] Security Requirements for Cryptographic modules, May 25, 2001

[IG] Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

## 14 Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CMVP | Cryptographic Module Validation Program |
| CSP | Critical Security Parameter |
| DRBG | Deterministic Random Bit Generator |
| ECC | Elliptic Curve Cryptography |
| EMC | Electromagnetic Compatibility |
| EMI | Electromagnetic Interference |
| FCC | Federal Communication Commission |
| FIPS | Federal Information Processing Standard |
| GND | Ground pin |
| HMAC | Keyed-Hash Message Authentication Code |
| KAT | Known Answer Test |
| NDRNG | Non-Deterministic Random Number Generator |
| OTPROM | One Time Programming Read Only Memory |
| RNG | Random Number Generator |
| ROM | Read Only Memory |
| SHA | Secure Hash Algorithm |
| SPI | Serial Peripheral Interface |
| VCC | IC power supply pin |