

# Non-Proprietary FIPS 140-2 Security Policy

---

**Google Inc.**

## **Delta Cryptographic Module**

**Hardware version: Delta [Configuration 0]; [Configuration 1]; [Configuration 2] with components ARM Cortex-M7 CPU, RR16FFGL\_111UHD32768X39M16B8W0R1E1L1P0D0L16, RR16FFGL\_111HS16384X8M16B8W1R1E1L0P0D0A0U20 and RR16FFGL\_111HS32768X8M16B8W1R1E1L0P0D0A0U20**

**Firmware version: Delta-gqfips-1.2**

**Date: 03/05/2019**

Prepared By:



2400 Research Blvd, Suite 395  
Rockville, MD 20850  
tel: +1 (703) 375-9820  
info@acumensecurity.net  
www.acumensecurity.net

## 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 Communications Security Establishment Canada (CSE) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 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 Delta Cryptographic Module from Google Inc. 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.

Delta may also be referred to as 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 Inc. 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.

## Table of Contents

|   |    |
|---|----|
| Introduction .....                                  | 2  |
| Disclaimer.....                                     | 2  |
| Notices .....                                       | 2  |
| 1. Introduction .....                               | 5  |
| 1.1 Scope.....                                      | 5  |
| 1.2 Overview .....                                  | 5  |
| 2. Security Level .....                             | 5  |
| 3. Cryptographic Module Specification.....          | 6  |
| 3.1 Cryptographic Boundary .....                    | 6  |
| 4. Cryptographic Module Ports and Interfaces.....   | 7  |
| 5. Roles, Services and Authentication.....          | 7  |
| 5.1 Roles.....                                      | 7  |
| 5.2 Services .....                                  | 7  |
| 5.3 Authentication .....                            | 8  |
| 6. Physical Security.....                           | 8  |
| 7. Operational Environment .....                    | 8  |
| 8. Cryptographic Algorithms and Key Management..... | 9  |
| 8.1 Cryptographic Algorithms .....                  | 9  |
| 8.1.1 Allowed Algorithms.....                       | 9  |
| 8.1.2 Non-Approved Algorithms .....                 | 10 |
| 8.2 Cryptographic Key Management .....              | 10 |
| 8.3 Key Generation and Entropy.....                 | 11 |
| 8.4 Zeroization .....                               | 12 |
| 9. Self-tests.....                                  | 12 |
| 9.1 Power-On Self-Tests.....                        | 12 |
| 9.2 Conditional Self-Tests .....                    | 13 |
| 10. Guidance and Secure Operation .....             | 14 |
| 10.1 Usage of AES GCM in the module .....           | 14 |
| 11. Glossary.....                                   | 15 |

## List of Tables

|   |    |
|---|----|
| Table 1 - Security Level .....                                    | 5  |
| Table 2 - Physical Port and Logical Interface Mapping .....       | 7  |
| Table 3 - Approved Services and Role allocation .....             | 8  |
| Table 4 - Non-Approved Services and Role allocation .....         | 8  |
| Table 5 - Crypto Engine Hardware Implementation Algorithms .....  | 9  |
| Table 6 - Hotplug Firmware Implementation Algorithms .....        | 9  |
| Table 7 - Offload Engine Hardware Implementation Algorithms ..... | 9  |
| Table 8 - Embedded Titan Chip Algorithms .....                    | 9  |
| Table 9 - Allowed Algorithms .....                                | 9  |
| Table 10 - Non-Approved Algorithms .....                          | 10 |
| Table 11 - Approved Keys and CSPs Table .....                     | 10 |
| Table 12 - Public Keys .....                                      | 11 |
| Table 13 - Approved Service to Key/CSP Mapping .....              | 11 |
| Table 14 - Power-up Self-tests .....                              | 13 |
| Table 15 - Conditional Self-tests .....                           | 13 |
| Table 16 - Glossary of Terms .....                                | 15 |

## List of Figures

|                                      |   |
|--------------------------------------|---|
| Figure 1 - Delta Block Diagram ..... | 6 |
|--------------------------------------|---|

# 1. Introduction

## 1.1 Scope

This document describes the cryptographic module security policy for the Google Inc. Delta Cryptographic Module (Hardware version: Delta [Configuration 0]; [Configuration 1]; [Configuration 2]) cryptographic module with firmware Delta-gqfips-1.2 (also referred to as the “module” hereafter). It contains 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 Delta Cryptographic Module is a Network Interface Card (NIC) connected to a host device over PCIe, which is designed to support Ethernet and IP networking. The Delta module contains cryptographic hardware and firmware support, which allows data packets to be encrypted and decrypted using AES-GCM-128 at "line rate", while supporting a very large number of simultaneous Security Associations.

# 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

Delta is a hardware module with a multiple-chip embedded embodiment. The cryptographic boundary of the module includes the Network Interface Card (NIC) and the embedded Google, Inc. Titan Chip cryptographic module (FIPS 140-2 Cert. #3382) which is utilized to perform several cryptographic functions.

The Delta Cryptographic Module is a Network Interface Card (NIC) housed on a host device. The module boundary contains two independent CPUs (CPU 0 and CPU 1) and components shown within the dotted line shown in Figure 1 below. CPU 0 is associated with Host 0, while CPU 1 is associated with Host 1. The module can operate in the following validated configurations:

- Configuration 0 - Host 0 has provided a valid Hotplug firmware image to CPU 0. All associated self-tests have passed for CPU 0 and it executes while CPU 1 waits for a Hotplug firmware image.
- Configuration 1 - Host 1 has provided a valid Hotplug firmware image to CPU 1. All associated self-tests have passed for CPU 1 and it executes while CPU 0 waits for a Hotplug firmware image.
- Configuration 2 - Both Host 0 and Host 1 have provided Hotplug firmware images to their respective CPUs. All associated self-tests have passed and both CPUs execute. The cryptographic boundary of the module and the relationship among the various internal components of the module are depicted in Figure 1 below.

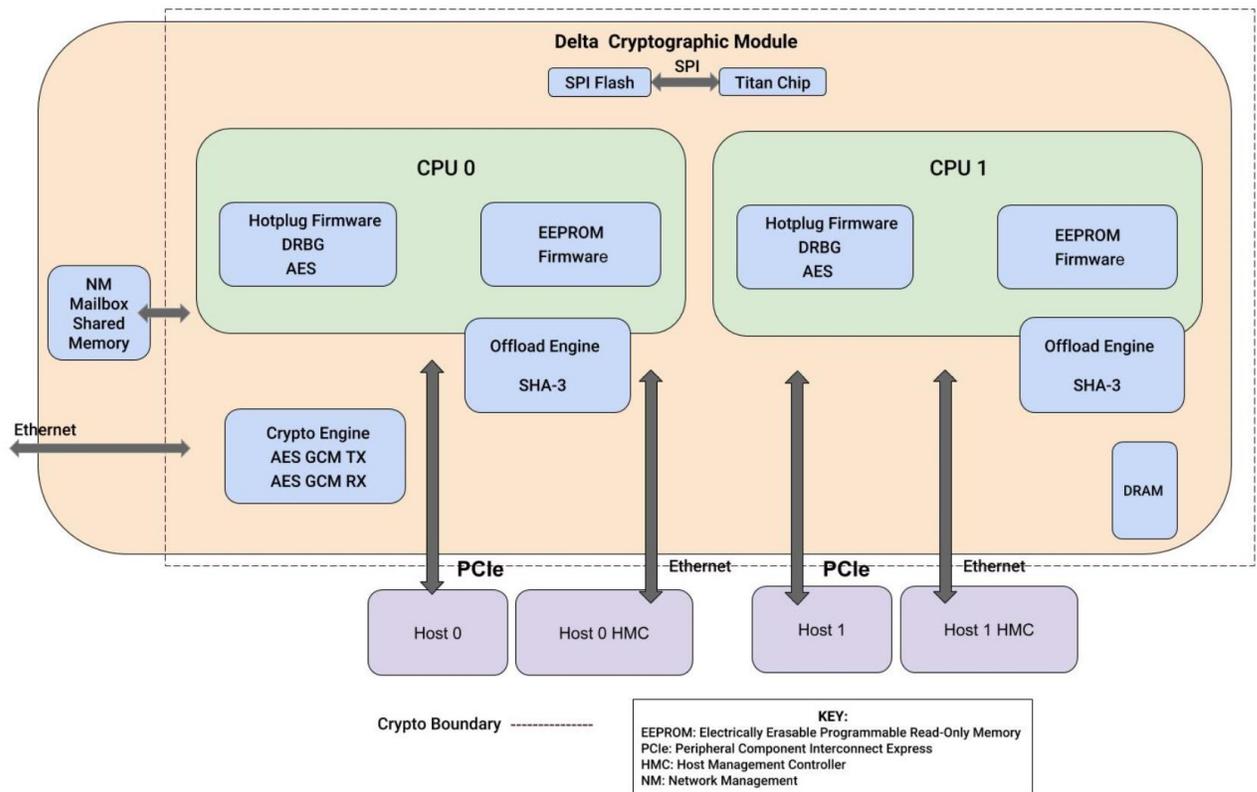


Figure 1 - Delta Block Diagram

The Delta Cryptographic Module will forward packets from the Hosts via PCIe links to the main Ethernet links, and from the main Ethernet link to the Hosts via the PCIe links. It will also forward packets from the HMC Ethernet link to the main Ethernet link, and packets that match rules configured by the HMCs from the main Ethernet link to the HMC links.

## 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:

| Physical Port                                      | FIPS 140-2 Logical Interface Mapping   | Description  |
|--|--|--|
| Ethernet   | Data Input and Output Interface<br>Status Output Interface<br>Control Input Interface  | TX/RX connection   |
| PCIe (x2)  | Data Input and Output Interface<br>Status Output Interface<br>Control Input Interface  | Direct Connections to Host 0 and Host 1  |
| Slow Ethernet Link (2x)                            | Data Input and Output Interface,<br>Status Output Interface<br>Control Input Interface | Direct connections to the Host Management Controllers (HMC) of Host 0 and Host 1 |
| Network Management Mailbox Shared Memory Interface | Data Input and Output Interface  | EMIF   |
| Power  | Power  | Provides power to the module   |

Table 2 - Physical Port and Logical Interface Mapping

## 5. Roles, Services and Authentication

### 5.1 Roles

The module does not provide any identification or authentication for any user that is accessing the device. Since the device does not provide any identification or authentication services, the level of access granted to any functionality of the module is implicitly determined by the service calling the module; the device itself makes no determination about the role itself.

### 5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 5, 6, 7 and 8:

| Service             | User | Crypto Officer |
|---------------------|------|----------------|
| Initialization      | ✓    | ✓              |
| On-Demand Self-test | ✓    | ✓              |
| Zeroization         | ✓    | ✓              |

| Service  | User | Crypto Officer |
|--|------|----------------|
| Host 0 and/or Host 1 via PCIe interface to module                              |      |                |
| Perform Titan Service (Host can request RPC commands via the module PCIe)      | ✓    | ✓              |
| Perform Firmware Update  |      | ✓              |
| Load Firmware  |      | ✓              |
| Instruct Module to Send Plaintext Packet                                       | ✓    | ✓              |
| Instruct Module to Send Encrypted Packet                                       | ✓    | ✓              |
| Instruct Module to Rotate Master Key   |      | ✓              |
| Write a value to video IP register   | ✓    | ✓              |
| Read a value from video IP register  | ✓    | ✓              |
| Request Status Information   | ✓    | ✓              |
| Set Configuration data   |      | ✓              |
| Host Management Controller via ethernet interface to module                    |      |                |
| Instruct Module to Send Packet   | ✓    | ✓              |
| Request Status Information   | ✓    | ✓              |
| Set Configuration data   |      | ✓              |
| Network Management via Mailbox API interface to module                         |      |                |
| Perform Titan Service (NM can request RPC commands via the module mailbox API) | ✓    | ✓              |
| Perform Firmware Update  |      | ✓              |
| Request Status Information   | ✓    | ✓              |
| Run Hardware Diagnostics   | ✓    | ✓              |

Table 3 - Approved Services and Role allocation

The module provides the following non-Approved services which utilize algorithms listed in Table 10:

| Service  |
|--|
| Derive RX Session ID and RX Session Key (using non-conformant KBKDF)                   |
| Receive Encrypted Packet via the TX/RX Ethernet interface (using non-conformant KBKDF) |

Table 4 - Non-Approved Services and Role allocation

### 5.3 Authentication

There is no operator authentication; assumption of role is implicit by the used service(s).

## 6. Physical Security

The module is a multi-chip embedded cryptographic module made with production grade components and standard passivation.

## 7. Operational Environment

The module does not provide a general-purpose operating system.

## 8. Cryptographic Algorithms and Key Management

### 8.1 Cryptographic Algorithms

The module implements the following approved algorithms in the firmware and hardware:

| Crypto Engine (Hardware Algorithm Implementation) |           |          |                                      |                        |   |
|---|-----------|----------|--------------------------------------|------------------------|---|
| CAVP Cert #                                       | Algorithm | Sizes    | Standard                             | Mode/Method            | Use                                       |
| 5656  | AES       | 128-bits | SP 800-38A<br>FIPS 197<br>SP 800-38D | ECB <sup>1</sup> , GCM | Encryption, Decryption,<br>Authentication |
| 5656  | KTS       | 128-bits | IG D.9                               | GCM                    | Authenticated Key Wrapping                |

Table 5 - Crypto Engine Hardware Implementation Algorithms

| Hotplug Cryptographic Module Firmware |           |          |                        |              |                        |
|---------------------------------------|-----------|----------|------------------------|--------------|------------------------|
| CAVP Cert #                           | Algorithm | Sizes    | Standard               | Mode/Method  | Use                    |
| 5659                                  | AES       | 128-bits | SP 800-38A<br>FIPS 197 | ECB          | Encryption, Decryption |
| Vendor Affirmed                       | CKG       | N/A      | SP 800-133             |              | Key Generation         |
| 2285                                  | DRBG      | 128-bits | SP 800-90Arev1         | AES CTR_DRBG | Random Bit Generation  |

Table 6 - Hotplug Firmware Implementation Algorithms

| Offload Engine (Hardware Algorithm Implementation) |           |       |            |             |         |
|--|-----------|-------|------------|-------------|---------|
| CAVP Cert #  | Algorithm | Sizes | Standard   | Mode/Method | Use     |
| 58   | SHA-3     | 224   | FIPS 180-4 | SHA3-224    | Hashing |

Table 7 - Offload Engine Hardware Implementation Algorithms

| Titan Chip Embedded Module <sup>2</sup> (Cryptographic Module Algorithm Implementation) |                |          |            |                        |   |
|---|----------------|----------|------------|------------------------|---|
| CAVP Cert #   | Algorithm      | Sizes    | Standard   | Mode/Method            | Use   |
| 4536  | SHS (hardware) | 256      | FIPS 180-4 | SHA-256                | Hashing, Keyed-Hash, Signature Verification |
| 4537  | SHS (firmware) | 256      | FIPS 180-4 | SHA-256                | Hashing, Keyed-Hash, Signature Verification |
| 3045  | RSA            | 2048-bit | FIPS 186-4 | Signature Verification | Signature Verification                      |
| 1529  | ECDSA          | P-256    | FIPS 186-4 | Signature Verification | Signature Verification                      |

Table 8 - Embedded Titan Chip Algorithms

#### 8.1.1 Allowed Algorithms

The module implements the following allowed cryptographic algorithms:

| Algorithm | Use  |
|-----------|--|
| NDRNG     | Residing in the embedded Titan Chip module |

Table 9 - Allowed Algorithms

<sup>1</sup> Crypto Engine only utilizes AES GCM. AES ECB was CAVP tested to demonstrate the forward cipher function.

<sup>2</sup> Not all algorithms/modes tested on the CAVP validation certificates for the Titan Chip are implemented in the module

### 8.1.2 Non-Approved Algorithms

The module implements the following algorithms which are considered non-Approved:

| Algorithm              | Use   |
|------------------------|---|
| KBKDF (non-conformant) | Used to derive a Session Key for the RX Decrypt functionality |

Table 10 - Non-Approved Algorithms

TX (AES GCM encryption) and RX (AES GCM decryption/authentication) were tested as part of the validation. However, the RX session keys are derived using a non-approved key derivation function.

## 8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 11:

| Keys and CSPs  | Description                    | Algorithm and Key Size    | Generation  | Input / Output Method                              | Storage                         | Zeroiation                                       |
|----------------|--------------------------------|---------------------------|---|--|---------------------------------|--|
| DRBG Seed      | SP 800-90A DRBG entropy input  | 128-bit value             | 512-bits externally loaded via SPI from Titan Chip, additional entropy provided from host | Input via direct interface. Never Exits the module | On-chip Volatile Memory         | Power cycle                                      |
| DRBG V         | SP 800-90A DRBG internal state | DRBG internal state value | Externally generated via SPI from Titan Chip TRNG, additional entropy provided from host  | Input via direct interface. Never Exits the module | On-chip Volatile Memory         | Power cycle                                      |
| DRBG Key       | SP 800-90A DRBG internal state | DRBG Key                  | Externally loaded via SPI from Titan Chip TRNG, additional entropy provided from host     | Input via direct interface. Never Exits the module | On-chip Volatile Memory         | Power cycle                                      |
| Master Key     | Used to generate per-SPI keys  | 128-bit, AES-ECB          | Generated via SP 800-90A DRBG   | Not Input or Output                                | On-chip Volatile Memory         | Power cycle; Before load of new firmware         |
| TX Session Key | Used to encrypt traffic        | 128-bit, AES GCM          | Externally loaded via PCIe interface from Host Appliance.                                 | Input via direct interface. Never Exits the module | On-die volatile memory register | Power cycle; Overwritten when Host sends new key |

Table 11 - Approved Keys and CSPs Table

The following public keys are utilized by the module:

| Public Keys  | Description  | Algorithm and Key Size  | Generation                                  | Input / Output Method | Storage             |
|--|--|-------------------------|---|-----------------------|---------------------|
| Delta EEPROM Firmware Verification key                 | Used by Titan to verify Delta NIC EEPROM firmware images before loading  | 2048-bit RSA public key | Generated externally; loaded at the factory | Not Input or Output;  | Stored in SPI Flash |
| Delta Hotplug Firmware Verification key 1              | Used by Titan to verify Delta NIC hotplug firmware images before loading | 2048-bit RSA public key | Generated externally; loaded at the factory | Not Input or Output;  | Stored in SPI Flash |
| Delta Hotplug Firmware Verification key 2 <sup>3</sup> | Used to verify Delta NIC hotplug firmware images before loading          | 2048-bit RSA public key | Generated externally; loaded at the factory | Not Input or Output;  | Stored in Flash     |

Table 12 - Public Keys

The module implements the following access control policy on keys and CSPs in the module shown in the following table. The Access Policy is noted by R=Read, W=Write and X=Execute.

| Module Service  | CSP Access  | Rights (R/W/X) |
|---|---|----------------|
| Initialization  | N/A   | N/A            |
| On-Demand Self-test   | N/A   | N/A            |
| Zeroization   | All keys  | R/W            |
| Perform Titan Service (Host can request RPC commands via the module PCIe) | N/A   | N/A            |
| Perform Firmware Update   | Delta EEPROM Firmware Verification key; Delta Hotplug Firmware Verification key 1 | N/A            |
| Load Firmware   | Delta Hotplug Firmware Verification key 1   | R/W/X          |
| Instruct Module to Send Plaintext Packet                                  | N/A   | N/A            |
| Instruct Module to Send Encrypted Packet                                  | TX Session Key  | R/X            |
| Instruct Module to Rotate Master Key                                      | DRBG CSPs; Master Key   | R/W/X          |
| Write a value to video IP register  | N/A   | N/A            |
| Read a value from video IP register                                       | N/A   | N/A            |
| Request Status Information  | N/A   | N/A            |
| Set Configuration data  | N/A   | N/A            |

Table 13 - Approved Service to Key/CSP Mapping

### 8.3 Key Generation and Entropy

The module is a hardware module with an entropy-generating NDRNG inside the module's cryptographic boundary consistent with Scenario 1 (a) described in FIPS 140-2 IG 7.14. The module performs a CRNGT on the entropy input it receives. A total of 512-bits of entropy is requested by each

<sup>3</sup> This key is used as a back-up to Delta hotplug Firmware Verification Key 1

CPU. From this 256-bit is used as direct input into the module's Approved DRBG. 256 bits is twice as much as the largest key generated by the module.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (vendor affirmed). The resulting generated symmetric keys are the unmodified output from the SP 800-90A DRBG.

## 8.4 Zeroization

All secret keys are zeroized either at session termination or by power-cycling the module.

The output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

## 9. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the module integrity and 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 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. 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 Delta Cryptographic Module:

| Type                       | Test Description  |
|----------------------------|---|
| Integrity Test (Delta)     | <ul style="list-style-type: none"> <li>EEPROM image RSA 2048-bit (SHA-256) Signature Verification performed by the Titan Chip Cryptographic Module (FIPS 140-2 Cert. #3382)</li> <li>Hotplug image SHA-256-bit EDC performed by the Titan Chip Cryptographic Module (FIPS 140-2 Cert. #3382)</li> <li>Hotplug image 224-bit SHA-3 EDC</li> </ul>                  |
| Integrity Test (Titan)     | <ul style="list-style-type: none"> <li>SHA-256 EDC over the bootloader image and executable firmware image</li> </ul>   |
| Known Answer Tests (Delta) | <ul style="list-style-type: none"> <li>Hardware AES KAT (Encryption and Decryption. Size 128)</li> <li>Hardware AES GCM KAT (Encryption and Decryption. Size 128)</li> <li>Hardware SHA-3 KAT (SHA3-224)</li> <li>Firmware SHS KAT (SHA-256)</li> <li>Firmware AES KAT (Encryption and Decryption. Size 128)</li> <li>Firmware SP 800-90A CTR_DRBG KAT</li> </ul> |
| Known Answer Tests (Titan) | <ul style="list-style-type: none"> <li>ECDSA (signature verification. Curve: P-256)</li> <li>SHS (Firmware Implementation. SHA-256)</li> <li>SHS (Hardware Implementation. SHA-256)</li> <li>RSA (signature verification. 2048-bit)</li> </ul>  |

Table 14 - Power-up Self-tests

The module performs all power-on self-tests automatically when it is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

## 9.2 Conditional Self-Tests

Conditional self-tests are test that run during operation of the module. Each module performs the following conditional self-tests:

| Type  | Test Description  |
|---|---|
| Continuous RNG Tests on Entropy Input (Delta) | Performed on entropy input provided by the bound Titan Chip Module  |
| DRBG Health Tests (Delta)                     | Performed on DRBG, per SP 800-90A Section 11.3. Required per IG C.1.  |
| EEPROM Firmware Upgrade Test (Delta)          | RSA 2048-bit Signature Verification operation performed by the Titan Chip Cryptographic Module (FIPS 140-2 Cert. #3382) |
| Bypass Check (Delta)                          | Conditional Bypass Check  |
| Continuous RNG Tests (Titan)                  | Performed on NDRNG per IG 9.8   |
| Firmware Load Test (Titan)                    | ECDSA Signature Verification operation performed prior to a firmware upgrade.   |

Table 15 - Conditional Self-tests

## 10. Guidance and Secure Operation

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 Delta cryptographic module is not considered to be in the Approved mode of operation until both operational firmware images have been successfully verified by the embedded Titan Chip cryptographic module.

The modules' cryptographic functions will only be available after all self-tests have passed successfully. If any of the self-tests fail the module will transition to an error state.

Use of the non-conformant algorithms listed in Table 10 will place the module in a non-approved mode of operation.

### 10.1 Usage of AES GCM in the module

The module utilizes a deterministically incrementing clock as a non-repetitive counter. The IV counter will automatically pause transmission over the data output interface until the IV it has a timer value greater than that of the previous IV. The module implements a 64-bit rollover (once every 213 days). Security Associations in the module are limited in lifetime to no more than about 2 days. Therefore, the vendor asserts that it is not possible for a Security Associations (and its key) to be used with the same IV more than once.

Per the requirements specified in Section 8 in NIST SP 800-38D, the probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data is no greater than  $2^{-32}$ .

The module conforms to FIPS 140-2 IG A.5 scenario #4. Per FIPS 140-2 IG A.5, in case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

## 11. Glossary

| Term   | Description   |
|--------|---|
| AES    | Advanced Encryption Standard                        |
| API    | Application Programming Interface                   |
| CAVP   | Cryptographic Algorithm Validation Program          |
| CKG    | Cryptographic Key Generation                        |
| CMVP   | Cryptographic Module Validation Program             |
| CRNGT  | Continuous Random Number Generator Test             |
| CSP    | Critical Security Parameter                         |
| CTR    | Counter   |
| DRAM   | Dynamic Random-Access Memory                        |
| DRBG   | Deterministic Random Bit Generator                  |
| ECB    | Electronic Codebook                                 |
| ECDSA  | Elliptic Curve Digital Signature Algorithm          |
| EDC    | Error Detection Code                                |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| FIPS   | Federal Information Processing Standards            |
| GCM    | Galois/Counter Mode                                 |
| HMC    | Host management controller                          |
| IG     | Implementation Guidance                             |
| IV     | Initialization vector                               |
| KAT    | Known answer test                                   |
| KBKDF  | Key-Based Key Derivation Function                   |
| KDF    | Key-Derivation Function                             |
| KTS    | Key Transport Scheme                                |
| NIC    | Network Interface card                              |
| NIST   | National Institute of Standards and Technology      |
| NDRNG  | Non-Deterministic Random Number Generator           |
| PCIe   | Peripheral Component Interconnect Express           |
| RAM    | Random Access Memory                                |
| RPC    | Remote Procedure Calls                              |
| RSA    | Rivest Shamir Adleman                               |
| RX     | Receiver  |
| SHA    | Secure Hash Algorithm                               |
| SHS    | Secure Hash Standard                                |
| SPI    | Serial Peripheral Interface                         |
| TRNG   | True Random Number Generator                        |
| TX     | Transmitter   |

*Table 16 - Glossary of Terms*