Google, LLC.

River Redux Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
March 3rd, 2026

Prepared by:

www.lightshipsec.com

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 7
2.4 Modes of Operation 7
2.5 Algorithms 8
2.6 Security Function Implementations 10
2.7 Algorithm Specific Information 11
2.8 RBG and Entropy 11
2.9 Key Generation 11
2.10 Key Establishment 11
2.11 Industry Protocols 12
3 Cryptographic Module Interfaces 13
3.1 Ports and Interfaces 13
4 Roles, Services, and Authentication 14
4.1 Authentication Methods 14
4.2 Roles 14
4.3 Approved Services 14
4.4 Non-Approved Services 17
4.5 External Software/Firmware Loaded 17
4.6 Bypass Actions and Status 17
5 Software/Firmware Security 18
5.1 Integrity Techniques 18
5.2 Initiate on Demand 18
5.3 Additional Information 18
6 Operational Environment 20
6.1 Operational Environment Type and Requirements 20
7 Physical Security 21
7.1 Mechanisms and Actions Required 21
8 Non-Invasive Security 22
9 Sensitive Security Parameters Management 23

9.1 Storage Areas 23
9.2 SSP Input-Output Methods 23
9.3 SSP Zeroization Methods 23
9.4 SSPs 23
9.5 Transitions 25
10 Self-Tests 26
10.1 Pre-Operational Self-Tests 26
10.2 Conditional Self-Tests 26
10.3 Periodic Self-Test Information 28
10.4 Error States 30
11 Life-Cycle Assurance 31
11.1 Installation, Initialization, and Startup Procedures 31
11.2 Administrator Guidance 31
11.3 Non-Administrator Guidance 31
12 Mitigation of Other Attacks 32

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 7
Table 3: Modes List and Description 8
Table 4: Approved Algorithms - 9
Table 5: Approved Algorithms - [Titan-BPN Cryptographic Module] 9
Table 6: Vendor-Affirmed Algorithms 9
Table 7: Security Function Implementations 11
Table 8: Entropy Certificates 11
Table 9: Entropy Sources 11
Table 10: Ports and Interfaces 13
Table 11: Roles 14
Table 12: Approved Services 17
Table 13: Mechanisms and Actions Required 21
Table 14: Storage Areas 23
Table 15: SSP Input-Output Methods 23
Table 16: SSP Zeroization Methods 23
Table 17: SSP Table 1 24
Table 18: SSP Table 2 25
Table 19: Pre-Operational Self-Tests 26
Table 20: Conditional Self-Tests 28
Table 21: Pre-Operational Periodic Information 29
Table 22: Conditional Periodic Information 29
Table 23: Error States 30

List of Figures

Figure 1: River Redux Cryptographic Module (Block Diagram) 6
Figure 2: River Redux Cryptographic Module (Front) 7

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the Google, LLC. River Redux Cryptographic Module (running firmware version River-gqfips-1.3), hereafter referred to as, “River” or “the module”. It contains the security rules under which the module must operate and describes how the module meets the requirements as specified in FIPS PUB 140-3 for an overall Security Level 1 cryptographic module.

1.2 Security Levels

The table below reflects the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

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

Table 1: Security Levels

The Module has an overall security level of 1.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module is a Network Interface Card (NIC) housed on a host device, which is designed to support Ethernet and IP networking. The 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.

The module will forward packets from the Host via PCIe link to the main Ethernet link, and from the main Ethernet link to the Host via the PCIe link. River will also forward packets from the Host Management Controller (HMC) Ethernet link to the main Ethernet link, and packets that match rules configured by the HMC from the main Ethernet link to the NC-SI HMC link.

The module executes two operational firmware images which are loaded externally. The Flash memory is solely used by the module and the embedded Titan-BPN Cryptographic Module for the purposes of validating, loading and updating firmware images.

Module Type: Hardware

Module Embodiment: MultiChipEmbed

Cryptographic Boundary:

The cryptographic boundary (indicated by dashed line) of the module is the Network Interface Card (NIC) containing the embedded Google, LLC. Titan-BPN Cryptographic Module (FIPS 140-3 Cert. #5166), and is shown in the figure below:

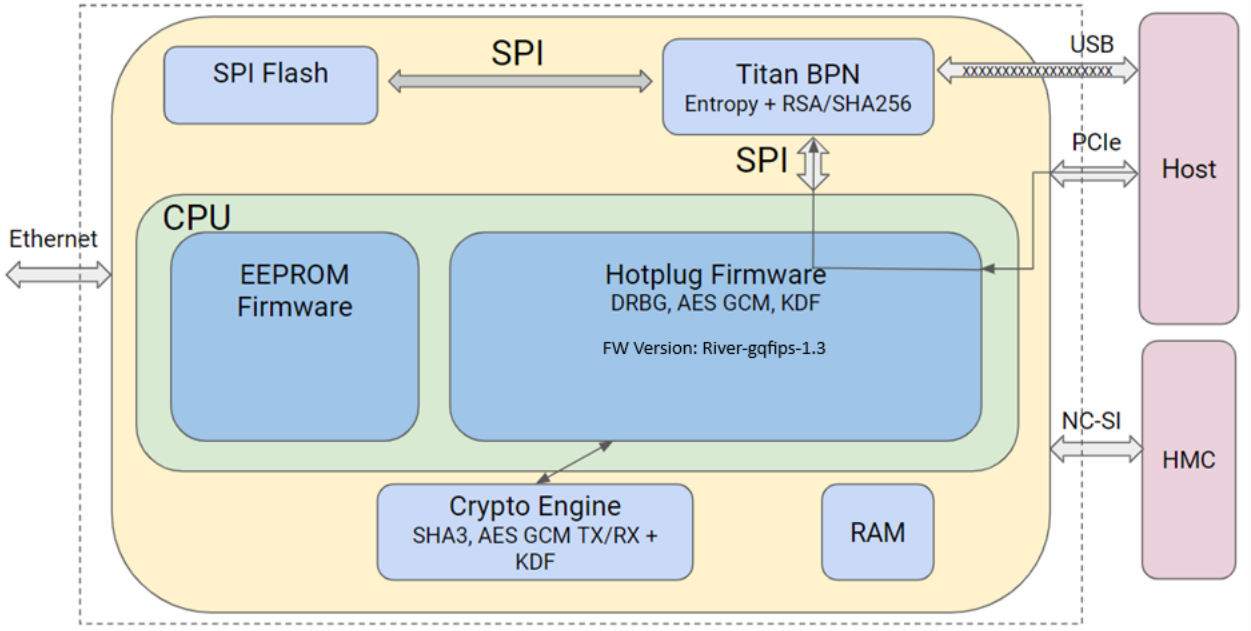

Figure 1: River Redux Cryptographic Module (Block Diagram)

All River Redux hardware versions (RiverHD-1.1, RiverQD-1.1 and RiverRD-1.1) are based on the same underlying hardware, therefore Figure 1 shows the block diagram applicable to all of them.

Tested Operational Environment's Physical Perimeter (TOEPP):

The module is a muti-chip embedded module as defined by FIPS 140-3.

All River Redux hardware versions (RiverHD-1.1, RiverQD-1.1 and RiverRD-1.1) are based on the same underlying hardware. The hardware versions contain non-security relevant differences related to pin straps on the NICs.

Figure 2: River Redux Cryptographic Module (Front)

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
River Redux Cryptographic Module	RiverHD-1.1, RiverQD-1.1 and RiverRD-1.1	River-gqfips-1.3	NIC Processor	

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

There are no components within the cryptographic boundary that are excluded from the FIPS 140-3 security requirements.

2.4 Modes of Operation

Modes List and Description:

The table below details the Modes of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	Operation mode where the module executes approved services	Approved	Global

Table 3: Modes List and Description

Mode Change Instructions and Status:

The embedded Titan-BPN Cryptographic Module (FIPS 140-3 Cert. #5166) performs the integrity check on both of River's operational firmware images prior to cryptographic functions being enabled. The River Redux Cryptographic Module also utilizes the output of the Titan-BPN Cryptographic Module's TRNG as its source of entropy for its Approved DRBG. The Titan-BPN Cryptographic Module is considered an embedded cryptographic module as it resides within River's cryptographic boundary as illustrated in Figure 1.

The embedded Titan-BPN Cryptographic Module (FIPS 140-3 Cert. #5166) first performs an RSA signature verification on the EEPROM firmware for the River Redux Cryptographic Module. If the signature verification operation is successful, the EEPROM firmware will be provided to River via the SPI interface. River boots use the EEPROM firmware. The Host (depicted in Figure 1) sends the hotplug firmware image to River. The header of the hotplug firmware image is also sent to the embedded Titan-BPN Cryptographic Module. The River Redux Cryptographic Module performs a CAST on its SHA-3 implementation prior to performing the integrity test on the hotplug firmware image. The Titan-BPN Cryptographic Module performs an RSA signature verification operation on the header of the hotplug firmware image. The River Redux Cryptographic Module verifies with Titan-BPN Cryptographic Module that the RSA signature verification operation has passed.

If both tests pass, the River Redux Cryptographic Module loads the hotplug firmware image and immediately executes its pre-operational self-tests. River requests entropy from the embedded Titan-BPN Cryptographic Module to initialize the Approved DRBG. No cryptographic functionality is available until all self-tests have passed and River indicates a status of "0" that it is running a FIPS validated firmware.

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A3409	Direction - Generation Key Length - 128	SP 800-38B
AES-CMAC	A5448	Direction - Generation Key Length - 128	SP 800-38B
AES-ECB	A3409	Direction - Encrypt Key Length - 128	SP 800-38A
AES-ECB	A5448	Direction - Encrypt Key Length - 128	SP 800-38A
AES-GCM	A3409	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5448	Direction - Encrypt IV Generation - External Key Length - 128	SP 800-38D
AES-GMAC	A3409	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128	SP 800-38D
AES-GMAC	A5448	Direction - Encrypt IV Generation - External Key Length - 128	SP 800-38D
Counter DRBG	A5448	Prediction Resistance - No Mode - AES-128 Derivation Function Enabled - No	SP 800-90A Rev. 1
KDF SP800-108	A3409	KDF Mode - Counter Supported Lengths - Supported Lengths: 128	SP 800-108 Rev. 1
KDF SP800-108	A5448	KDF Mode - Counter Supported Lengths - Supported Lengths: 128	SP 800-108 Rev. 1
SHA3-224	A3409	Message Length - Message Length: 8-51200 Increment 8	FIPS 202

Table 4: Approved Algorithms -

[Titan-BPN Cryptographic Module]

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-4)	A5419	Signature Type - PKCS 1.5 Modulo - 2048, 3072	FIPS 186-4
SHA2-256	A5419	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
SHA2-256	A5420	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4

Table 5: Approved Algorithms - [Titan-BPN Cryptographic Module]

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric	River Hotplug Cryptographic Module Firmware	FIPS 140-3 IG D.H/NIST SP 800-133r2 Sections 4 and 6

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Crypto Engine KDF	KBKDF	Key Derivation Function		KDF SP800-108: (A3409) AES-CMAC: (A3409) AES-ECB: (A3409)
Crypto Engine Authenticated Encryption	BC-Auth	Authenticated Encryption/Decryption		AES-GCM: (A3409) AES-GMAC: (A3409) AES-ECB: (A3409)
Crypto Engine Message Digest	SHA	Hashing		SHA3-224: (A3409)
Hotplug KDF	KBKDF	Key Derivation Function		KDF SP800-108: (A5448) AES-CMAC: (A5448) AES-ECB: (A5448)
Hotplug Authenticated Encryption	KTS-Wrap	Authenticated Encryption/Decryption		AES-GCM: (A5448) AES-GMAC: (A5448)
Hotplug Symmetric Key Generation	CKG	Symmetric Key Generation		Counter DRBG: (A5448) AES-ECB: (A5448) CKG: ()
Titan-BPN Library FW Verification	DigSig-SigVer	Digital Signature Verification [Titan-BPN Cryptographic Module]		RSA SigVer (FIPS186-4): (A5419) SHA2-256: (A5419)

Name	Type	Description	Properties	Algorithms
Titan-BPN TRNG Entropy Source	ENT-Cond ENT-ESV	Entropy Source [Titan-BPN Cryptographic Module]		SHA2-256: (A5420)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

Usage of AES-GCM in the module

The module's AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #3. The module utilizes a deterministically incrementing clock as a non-repetitive counter. The IV is 96 bits in length and is composed of a 32-bit name field and 64-bit non-repetitive counter. The IV counter will automatically pause transmission over the module's data output interface until the IV 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 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}.

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.

2.8 RBG and Entropy

The tables below detail the module ESV information.

Cert Number	Vendor Name
E187	Google, LLC.

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Titan-BPN TRNG Entropy Source	Physical	Titan Chip H1B3P	256 bits	256 bits	SHA2-256 (A5420)

Table 9: Entropy Sources

2.9 Key Generation

The module generates keys in accordance with FIPS 140-3 IG D.H. The cryptographic module performs Cryptographic Key Generation (CKG) for symmetric keys as per SP 800-133r2 (vendor affirmed) and using a DRBG compliant with SP 800-90A.

2.10 Key Establishment

The tester verified from Table 6 of the [SP] that the vendor has provided documentation asserting that the key establishment techniques used are allowed in the Approved mode of operation per NIST SP 800-140D.

The module supports the following key wrapping technique specified in FIPS 140-3 IG D.A and IG D.G

- AES GCM KTS (Approved authenticated symmetric encryption mode).

2.11 Industry Protocols

The module does not implement any industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The table below details the module Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
Ethernet	Data Input Data Output Control Input Status Output	TX/RX connection
PCIe	Data Input Data Output Control Input Status Output	Direct Connection to the Host
USB	None	Not used
Network Controller Sideband Interface (NC-SI) Slow Ethernet Link	Data Input Data Output Control Input Status Output	Direct connection to the Host Management Controller (HMC)
Power	Power	Power

Table 10: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module does not support authentication for roles.

N/A for this module.

4.2 Roles

The module supports two roles that an operator may assume: Crypto Officer (CO) role and User role. Roles are assumed implicitly based on the service accessed. The table below lists the Roles supported by the module.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None
User	Role	User	None

Table 11: Roles

4.3 Approved Services

The table below lists all Approved Services supported by the module. The abbreviations of the access rights to SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialization	Module Initialization	N/A	None	None	None	Crypto Officer
Show Version	Return the module version information	N/A	API command and parameters	Module Versioning Information	None	Crypto Officer
Show Status Information	Return module status to PCIe interface	N/A	API command and parameters	0 - FIPS compliant or 1 - Not a validated module	None	Crypto Officer
On-Demand Self-test	Initiate on-demand self-tests by power cycling the module	N/A	None	Pass or Fail status	Crypto Engine KDF Crypto Engine Authenticated Encryption Crypto Engine Message Digest	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Hotplug KDF Hotplug Authenticated Encryption Titan-BPN Library FW Verification Titan-BPN TRNG Entropy Source	
Zeroisation	Zeroise unprotected SSPs and key components	N/A	None	None	None	Crypto Officer - DRBG Seed: Z - DRBG V: Z - DRBG Key: Z - Master Key: Z - Rx Session Key: Z - Tx Session Key: Z - Exported Rx Session Key: Z
Perform Titan-BPN Service	Host can request RPC commands from the embedded Titan-BPN module via the module PCIe	N/A	Command and parameters	Success or Failure status	None	User
Load Firmware	Load a new Hotplug image firmware	Successful completion of service	Command and parameters	Image Loaded	Titan-BPN Library FW Verification	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Firmware Update	EEPROM Firmware Update	Successful completion of service	Command and parameters	Updated Firmware Image	Titan-BPN Library FW Verification	Crypto Officer
Send Plaintext Packet	Instruct Module to send plaintext packet	N/A	API command and parameters	Plaintext Packet	None	User
Send Encrypted Packet	Instruct Module to send encrypted packet	Successful completion of service	API command and parameters	Encrypted Packet	Crypto Engine Authenticated Encryption	User - Tx Session Key: W,E
Rotate Master Key	Instruct Module to rotate the Master Key	Successful completion of service	API command and parameters	Master Key rotated	Hotplug Symmetric Key Generation Titan-BPN TRNG Entropy Source	Crypto Officer - DRBG Seed: G,E - DRBG V: E - DRBG Key: E - Master Key: G
Derive RX Session ID and RX Session Key	Instruct Module to generate a new session key based on the Master Key	Successful completion of service	API command and parameters	RX Session ID and RX Session Key derived	Crypto Engine KDF Hotplug KDF	User - Master Key: E - Rx Session Key: G - Exported Rx Session Key: G,R
Set Configuration Data	Set PCIe configuration data	N/A	API command and parameters	Status	None	Crypto Officer
HMC Send Packet	Instruct Module to send plaintext packet	N/A	API command and parameters	Plaintext Packet	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
HMC Request Status Information	Return the ethernet interface status	N/A	API command and parameters	Ethernet interface status	None	User
HMC Set Configuration Data	Set ethernet interface configuration data	N/A	API command and parameters	Status	None	Crypto Officer

Table 12: Approved Services

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

N/A for this module.

4.5 External Software/Firmware Loaded

The following firmware updates are supported within the defined cryptographic boundary:

- River EEPROM firmware upgrade: an approved RSA Signature Verification (2048/3072, SHA2-256) firmware load test operation is performed prior to a firmware upgrade.
- River Hotplug firmware upgrade: an approved RSA Signature Verification (2048/3072, SHA2-256) firmware load test operation is performed prior to a firmware upgrade.

4.6 Bypass Actions and Status

Data is processed by the module using a shift-register based FIFO control queue. One of the FIFO output bits is a bypass signal bit which controls whether the data in a packet will be encrypted (exclusive encryption service status indicated by a “0”) or processed in plaintext by the module (exclusive bypass service status indicated by a “1”).

For the module to switch from an exclusive bypass service (plaintext packet transmission) to an exclusive cryptographic service (encrypted packet transmission) two independent internal actions must be performed for the packet to be sent. If one of the actions are not performed, the module will discard the packet.

The module implements a conditional bypass test in the form of a parity verification test. This test is performed by the module at the beginning of processing a packet to be transmitted over the ethernet (data output) interface.The test checks for a parity bit on the control structure of the data for the duration of the packet being processed by the module.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by the following steps:

- EEPROM firmware Verification: the River EEPROM firmware is attested by the Titan-BPN Chip by verifying the RSA signature of the firmware image, using the public key loaded in factory.
- Hotplug firmware Verification: the River Hotplug firmware is attested by the Titan-BPN Chip by verifying the RSA signature contained in the firmware image header, using the public key uploaded from the Host along with the firmware image.
- Hotplug firmware Integrity: the integrity of the River Hotplug firmware is verified by comparing a SHA3-224 digest value calculated at boot time with the SHA3-224 digest value stored in the firmware image header.

5.2 Initiate on Demand

All integrity tests are performed as part of the pre-operational self-tests, which are executed when the module is initialized. The integrity tests can be invoked on demand by power cycling the module, which will perform (among others) all firmware integrity tests.

5.3 Additional Information

The temporary values generated during the module's integrity tests are zeroised upon completion of the integrity tests.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The module is designed to accept only controlled firmware changes that successfully pass the software/firmware load test.

How Requirements are Satisfied:

The limited operational environment of the module prevents users from accessing SSPs which they are not authorized to access. There is no logical or physical access to the SSPs.

As per ISO/IEC 19790:2012 7.6.3:

- The cryptographic module has control over its own SSPs.
- The operational environment provides the capability to separate individual application processes from each other to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs, regardless if this data is in the process memory or stored on persistent storage within the operational environment.
- The module operates in a limited operational environment, therefore no restrictions or modifications to the configuration of the operational environment are possible.
- Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

7 Physical Security

7.1 Mechanisms and Actions Required

The module is a multiple-chip embedded cryptographic module made with production grade components, standard passivation techniques.

Mechanism	Inspection Frequency	Inspection Guidance
N/A	N/A	N/A

Table 13: Mechanisms and Actions Required

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The table below lists Sensitive Security Parameters (SSPs) storage areas for the module. Section 9.4 below selects from the storage areas listed and specifies the appropriate parameter in the "Storage" column if applicable to a specific SSP.

Storage Area Name	Description	Persistence Type
RAM	Volatile memory	Dynamic
Flash	SPI Flash	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

The table below lists SSP input and output methods for the module. Section 9.4 below selects from the input and output methods listed and specifies the appropriate parameter in the "Inputs/Outputs" column if applicable to a specific SSP.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PCI-e Input	Host	RAM	Plaintext	Manual	Electronic	
PCI-e Output	RAM	Host	Plaintext	Manual	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The table below lists SSP zeroisation methods for this module. Section 9.4 below selects from the zeroisation methods listed and specifies the appropriate parameter in the "Zeroization" column if applicable to a specific SSP.

Zeroization Method	Description	Rationale	Operator Initiation
Power Cycle	Zeroization by power cycling the module	Keys are automatically zeroised by a power cycle, which is acceptable at Security Level 1	Crypto Officer by power cycling the module

Table 16: SSP Zeroization Methods

9.4 SSPs

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Seed	NIST SP800-90A DRBG entropy input	512 - 512	Seed - CSP	Titan-BPN TRNG Entropy Source		Hotplug Symmetric Key Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG V	NIST SP800-90A DRBG internal state	N/A - N/A	Internal Value - CSP			Hotplug Symmetric Key Generation
DRBG Key	NIST SP800-90A DRBG internal state	N/A - N/A	Internal Value - CSP			Hotplug Symmetric Key Generation
Master Key	Used to generate Session Keys	128 - 128	Symmetric Key - CSP	Hotplug Symmetric Key Generation		Crypto Engine KDF Hotplug KDF
Rx Session Key	Used to decrypt traffic	128 - 128	Symmetric Key - CSP	Crypto Engine KDF		Crypto Engine Authenticated Encryption
Tx Session Key	Used to encrypt traffic	128 - 128	Symmetric Key - CSP			Crypto Engine Authenticated Encryption
Exported Rx Session Key	Passed to host over PCI-e to send to remote NICs for communication purposes	128 - 128	Symmetric Key - CSP	Hotplug KDF		Hotplug Authenticated Encryption

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed		RAM:Plaintext	Until power cycling the module	Power Cycle	
DRBG V		RAM:Plaintext	Until power cycling the module	Power Cycle	
DRBG Key		RAM:Plaintext	Until power cycling the module	Power Cycle	
Master Key		RAM:Plaintext	Until power cycling the module	Power Cycle	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Rx Session Key		RAM:Plaintext	Until power cycling the module	Power Cycle	Master Key:Derived From
Tx Session Key	PCI-e Input	RAM:Plaintext	Until power cycling the module	Power Cycle	
Exported Rx Session Key	PCI-e Output	RAM:Plaintext	Until power cycling the module	Power Cycle	Master Key:Derived From

Table 18: SSP Table 2

9.5 Transitions

Per FIPS 140-3 IG C.K, FIPS 186-4 CAVP tests performed are mathematically identical to FIPS 186-5 CAVP tests, therefore the module can claim FIPS 186-5 compliance for these tests.

10 Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module. The pre-operational and conditional self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

10.1 Pre-Operational Self-Tests

Pre-operational Self-Tests are run upon the power up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests are passed successfully. The design of the module ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition. The Pre-Operational Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A5419)	2048/3072-bit	Digital Signature Verification	SW/FW Integrity	Status Output	EEPROM Firmware Verification Integrity Test [Titan-BPN Cryptographic Module]
RSA SigVer (FIPS186-4) (A5419)	2048/3072-bit	Digital Signature Verification	SW/FW Integrity	Status Output	Hotplug Firmware Verification Integrity Test [Titan-BPN Cryptographic Module]
SHA3-224 (A3409)	N/A	Message Digest	SW/FW Integrity	Status Output	Hotplug Firmware Integrity Test
Bypass Test	N/A	Bypass	Bypass	Status Output	Pre-operational Bypass Test

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Conditional Self-Tests are run when an applicable security function or process is invoked. The Conditional Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A3409)	128-bit key	KAT	CAST	Successful initialization of the module	Encryption	Module Initialization
AES-CMAC (A3409)	128-bit key	KAT	CAST	Successful initialization of the module	MAC Generation	Module Initialization
KDF SP800-108 (A3409)	Counter CMAC-AES128	KAT	CAST	Successful initializatio	Key Derivation Function	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				n of the module		
AES-GCM (A3409)	128-bit key	KAT	CAST	Successful initialization of the module	Authenticated Encryption/Decryption	Module Initialization
SHA3-224 (A3409)	224-bit hash	KAT	CAST	Successful initialization of the module	Hash	Module Initialization
AES-ECB (A5448)	128-bit key	KAT	CAST	Successful initialization of the module	Encryption	Module Initialization
AES-CMAC (A5448)	128-bit key	KAT	CAST	Successful initialization of the module	MAC Generation	Module Initialization
KDF SP800-108 (A5448)	Counter CMAC-AES128	KAT	CAST	Successful initialization of the module	Key Derivation Function	Module Initialization
AES-GCM (A5448)	128-bit key	KAT	CAST	Successful initialization of the module	Authenticated Encryption/Decryption	Module Initialization
Counter DRBG (A5448)	As specified in NIST SP 800-90Ar1 Section 11.3	KAT	CAST	Successful initialization of the module	Instantiate, Generate and Reseed	Module Initialization
SHA2-256 (A5420)	256-bit hash	KAT	CAST	Successful initialization of the module	Hash [Titan-BPN Cryptographic Module]	Module Initialization
SHA2-256 (A5419)	256-bit hash	KAT	CAST	Successful initializatio	Hash [Titan-BPN Cryptographic Module]	Module Initialization

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				n of the module		
RSA SigVer (FIPS186-4) (A5419)	2048-bit	KAT	CAST	Successful initialization of the module	Signature Verification [Titan-BPN Cryptographic Module]	Module Initialization
Repetition Count Test (RCT)	4096 raw 1 bit samples	FD	CAST	Successful output of entropy bits	NIST SP 800-90B Section 4.4.1 [Titan-BPN Cryptographic Module]	Continuous
Adaptative Proportion Test (APT)	4096 raw 1 bit samples	FD	CAST	Successful output of entropy bits	NIST SP 800-90B Section 4.4.2 [Titan-BPN Cryptographic Module]	Continuous
Firmware Load Test	RSA SigVer (FIPS186-4) with 2048/3072-bit modulus	Load Test	SW/FW Load	Successful firmware update	Signature Verification [Titan-BPN Cryptographic Module]	Firmware Update Request
Bypass Test	N/A	Parity Verification Test	Bypass	Bypass Signal Bit	Bypass	Bypass Service Request

Table 20: Conditional Self-Tests

The module performs self-tests on all approved cryptographic algorithms supported in the approved mode of operation, using the tests shown in the table above. To ensure all conditional CASTs are performed prior to the first operational use of the associated algorithm, all CASTs are performed during the module's initial power-up sequence. The CASTs for algorithms used in the pre-operational firmware integrity test are performed prior to the integrity tests itself; all other CASTs are executed immediately after the successful completion of the firmware integrity tests.

Services are not available, and data output (via the data output interface) is inhibited during the applicable self-tests. If any of these tests fails, the module transitions to an error state.

10.3 Periodic Self-Test Information

Pre-operational self-tests can be run on-demand, for periodic testing, by power cycling the module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A5419)	Digital Signature Verification	SW/FW Integrity	On Demand	Power cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A5419)	Digital Signature Verification	SW/FW Integrity	On Demand	Power cycle
SHA3-224 (A3409)	Message Digest	SW/FW Integrity	On Demand	Power cycle
Bypass Test	Bypass	Bypass	On Demand	Power cycle

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A3409)	KAT	CAST	On Demand	Power cycle
AES-CMAC (A3409)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A3409)	KAT	CAST	On Demand	Power cycle
AES-GCM (A3409)	KAT	CAST	On Demand	Power cycle
SHA3-224 (A3409)	KAT	CAST	On Demand	Power cycle
AES-ECB (A5448)	KAT	CAST	On Demand	Power cycle
AES-CMAC (A5448)	KAT	CAST	On Demand	Power cycle
KDF SP800-108 (A5448)	KAT	CAST	On Demand	Power cycle
AES-GCM (A5448)	KAT	CAST	On Demand	Power cycle
Counter DRBG (A5448)	KAT	CAST	On Demand	Power cycle
SHA2-256 (A5420)	KAT	CAST	On Demand	Power cycle
SHA2-256 (A5419)	KAT	CAST	On Demand	Power cycle
RSA SigVer (FIPS186-4) (A5419)	KAT	CAST	On Demand	Power cycle
Repetition Count Test (RCT)	FD	CAST	On Demand	Entropy Bits Request
Adaptative Proportion Test (APT)	FD	CAST	On Demand	Entropy Bits Request
Firmware Load Test	Load Test	SW/FW Load	On Demand	Firmware Update Request
Bypass Test	Parity Verification Test	Bypass	On Demand	Bypass Service Request

Table 22: Conditional Periodic Information

10.4 Error States

If any of the Pre-operational Self-Tests or Conditional Self-Tests fail, the module will output an error status and enter an error state, where all data output is inhibited. Upon entering an error state, an operator can attempt to clear the error state by power cycling the module. If the error state cannot be cleared, the module must be returned to the manufacturer.

The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	The module's hard error state	POST or CAST Failure	Power cycle	Error Code
Soft Error	The module's soft error state	Firmware Load Test Failure	Revert to previous firmware	Error Code

Table 23: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

No configuration of the module or installation steps are required from the operator. No cryptographic services are provided until all operational firmware images have been successfully verified. When the module is powered on (or power-cycled) its self-tests are executed without any operator intervention. If any of the self-tests fail during power-up, the module transitions to an Error state.

11.2 Administrator Guidance

None.

11.3 Non-Administrator Guidance

None.

12 Mitigation of Other Attacks

The module does not offer mitigation of other attacks and therefore this section is not applicable.