PrismPlus Cryptographic Module

Broadcom, Inc.

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.2

Date: January 17, 2025

Table of Contents

List of Tables

List of Figures

Glossary Of Terms

Appliance-Host	Storage Server (Initiator) or Storage Device (Target) with a PrismPlus Adaptor
AUTH_ELS	Fibre Channel Messaging Protocol that maps IKEv2 to the Fibre Channel ELS (Extended Link Service) Protocol.
Connection	Communication between a Host Initiator Entity on a Storage Server Appliance and a Remote Target Entity on Storage Device Appliances
Connection Table	The **Connection Table (**aka Remote Peer Information (RPI) Table) contains Encryption Parameters including Enable/Bypass Encryption, Algorithms to be used and Traffic Selectors (types of frames to be encrypted) for a **connection**. These RPI fields can be considered an extension to the SADB and are required by the Encrypt/Decrypt HW Engines
EDIF	Encrypted Data In Flight
Factory-Host	Factory Host system with PrismPlus Adaptor that runs the Factory Process to configure the Adaptor in Approved Mode.
Fibre Channel	Fibre Channel (FC) is a high-speed data transfer protocol providing in-order, lossless delivery of raw block data. Fibre Channel is primarily used to connect computer data storage to servers in storage area networks (FC-SAN) in commercial data centers.
Fibre Channel Frame	Frames are units of transfer in Fibre Channel akin to Packets in Ethernet.
Initiator	Entity (e.g., Driver) on a **Storage Server Appliance** that makes data requests on behalf of Applications from networked data resources.
Remote Peer Information (RPI) Table	This **connection table** contains Encryption Parameters including Enable/Bypass Encryption, Algorithms to be used and Traffic Selectors (types of frames to be encrypted) for a **connection**. These RPI fields can be considered an extension to the SADB and are required by the Encrypt/Decrypt HW Engines
Security Association Database (SADB)	Contains Encryption/Decryption Keys and other parameters required by the Encrypt/Decrypt HW Engines. The SADB contains CSPs (Encrypt/Decrypt Keys and other parameters) for EDIF
Service Layer Interface (SLI)	The Service Level Interface (SLI) provides a standard set of control structures, commands, and responses to accomplish the transfer of data between a host system and an external network through a tightly coupled port. The SLI documents detail the control structures.
Storage Appliance	A Storage Server Appliance or a Storage Device Appliance
Storage Peer	The Remote Appliance with which **connection** has been established for data transactions
Storage Server Appliance	A type appliance on a network that accesses networked data resources for applications
Storage Device Appliance	A type of appliance that provides data to, or manages data for, other network-connected computing devices.
Support Processor (SP)	On chip Support Processor handling on-chip configuration and management and Management Control Messages (MailBox Commands) from the Host.
Target	Entity (e.g., Driver) on a **Storage Device Appliance** that services data requests received on network.

Acronyms and Definitions

Acronym	Definition
APT	Adaptive Proportion Test
CSP	Critical Security Parameter
KAT	Know Answer Test
RCT	Repetition Count Test
RPI	Remote Peer Information
SADB	Security Association Database
SSP	Sensitive Security Parameter

1 General

This document defines the Security Policy for the **Broadcom Inc. PrismPlus Cryptographic Module**, hereafter denoted the Module. The PrismPlus ASIC based module is implemented on a PCIe Host Bus Adapter (HBA) and is assumed to operate within a **Storage Server Appliance** or a **Storage Device Appliance** operating in a **Fibre Channel Storage Area Network** (FC-SAN) environment.

The FIPS 140-3 security levels for the module are as follows:

Table 1 – Security Level of Security Requirements

ISO/IEC 24759 section	Security Requirement	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		1

2 Cryptographic Module Specification

The PrismPlus Cryptographic Module is a hardware module intended for use by US Federal agencies or other markets that require a FIPS 140-3 validated network encryption device. The module implemented on a PCIe Adapter is intended to be used in **Fibre Channel** based Storage Area Networks.

The module allows a **Connection** to be established between **one** of the multiple **Host Initiator** Entities (e.g., 256 Virtual Machine Drivers running on multiple CPU cores) on a **Storage Server Appliance** and **one** of the multiple Remote **Host Target** Entities (e.g., 1000s of Storage LUNs) on multiple **Storage Device Appliances** via one of the multiple Physical Ports (e.g., 4x 64GFC ports). The **Connection** facilitates transfer of data between a **Host Initiator** Entity on a **Storage Server Appliance** and **Host Target** Entity on a **Storage Server Appliance** using the FC (Fibre Channel) Protocol. The module allows multiple (1000s) of connections between Host Initiator Entities on a Storage Server Appliance and Host Target Entities on Storage Device Appliances.

The module can be used to support **Data-in-Flight Encryption/Decryption** between Storage Appliances in a FC-SAN environment. Encryption decisions are made on a **connection basis**, whereby only a subset of the connections could be enabled for Encryption. If a **connection** is enabled for Encryption, only a subset of the Frame Types (e.g., Data Frames only, not Command/Status/Control/etc. Frames) could be enabled for Encryption. Note: Frames are units of transfer in Fibre Channel akin to Packets in Ethernet.

Please note that while the module includes an entropy source; the entropy source is not utilized in the current design and is reserved for future use.

Table 2 – Cryptographic Module Tested Configuration

Model	Hardware	Firmware version	Distinguishing Features
PrismPlus Cryptographic Module	G99-00139-01	14.2.338.0	PrismPlus ASIC, Flash implemented on a PCIe Adapter

2.1 Cryptographic Boundary

The module is a multiple-chip embedded embodiment. The cryptographic boundary is defined as a sub-region of the PCB depicted by the red dotted line in Figure 1, which encompasses the PrismPlus ASIC and Flash.

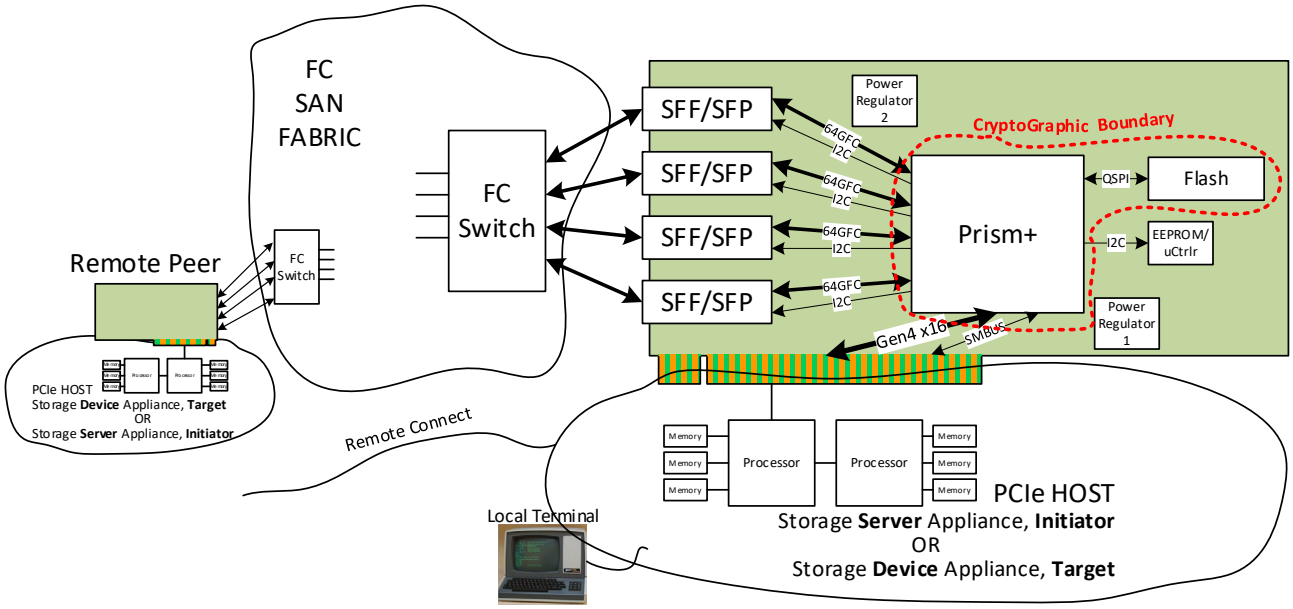

Figure 1 – Module Diagram

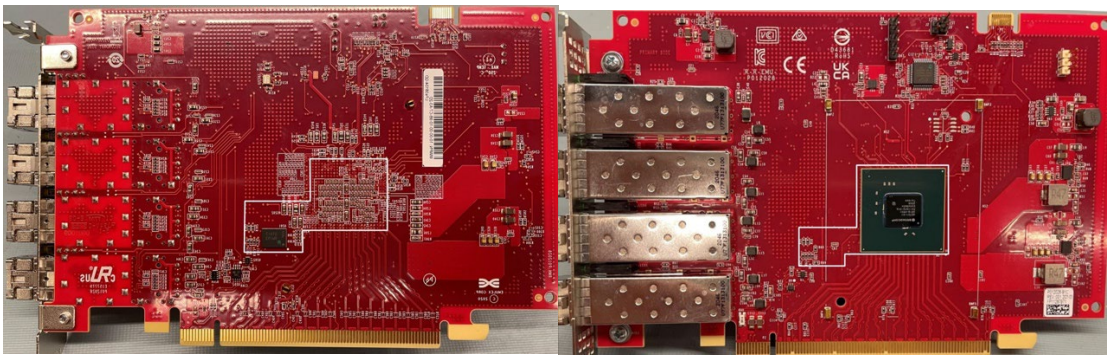

Figure 2 – Module Images (Bottom and Top)

2.2 Modes of Operation

The module supports an Approved mode of operation and assumes the Approved mode as soon as it is powered-on. The module does not support a non-Approved mode. Approved mode of operation requires FW Load, FW Integrity and Pre-Operational Self Tests to pass. All services are offered only in Approved mode of operation. If Firmware Integrity Tests or the Pre-Operational Self tests fail, the module will halt all operations and will need to be reset, unless the module has automatically done so. The module does not support a degraded mode of operation.

To verify that the module is in the Approved mode of operation, the operator may invoke the "Show Status" service. The Approved Security Service Indicator is provided by the successful completion of each service, as an implicit indicator for the use of an Approved service per IG 2.4.C, Example Scenario 2.

2.3 Security Functions

The module implements the approved cryptographic functions listed in **Table 3** below, which were tested on the ARM Cortex R4 processor internal to the module. The module does not support any non-Approved algorithms or non-Approved algorithms allowed in the approved mode. There are algorithms, modes, and keys that have been CAVP tested, but not used by the module; such unused algorithms, modes/methods, and key lengths are shown in this table with "Tested, but not used" specified in the Use/Function column.

Table 3 – Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2693	**AES [197]** (Specification for AES)	ECB [38A]	Key Sizes: 256	Supports GCM
#A2695	**AES [197]** (Specification for AES)	GCM [38D]	Key Sizes:256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt
#A2691	**RSA [186-4]** (Digital Signature Standard) RSA Cryptographic Standard	PKCS1_v1.5	n = 2048 SHA2-256	SigVer
#A2694	**SHS [180-4]** SHS (Secure Hash Standard)	SHA2-256	SHA2-256	Message Digest Generation

The module does not implement any KAS or KTS Security Function Implementations.

2.4 Overall Security Design

1. The module provides a single operator role: Cryptographic Officer Role.
2. An operator does not have access to any cryptographic services prior to assuming an authorized role.
3. The module allows the operator to initiate pre-operational and conditional self-tests by power cycling or resetting the module.
4. Pre-operational self-tests do not require any operator action.
5. Data output is inhibited during self-tests, FW loading, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

7. There are no restrictions on which CSPs are zeroized by the zeroization service.
8. The module does not support concurrent operators.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not have any proprietary external input/output devices used for entry/output of data.
12. The module does not output any plaintext CSPs.
13. The module does not output intermediate key values.
14. The module provides bypass services for connections.
15. AES GCM IV uniqueness: The AES GCM implementation meets Option 3 of IG C.H Key/IV Pair Uniqueness Requirements from SP 800-38D. The module uses the IV construction in Section 8.2.1 Deterministic Construction of SP800-38D for the 96bit IV that is used. 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.

2.5 Rules of Operation

The module is installed on a PCIe Adaptor that shall be installed either in a storage server appliance or a storage device appliance.

The module will power on in the Approved mode of operation.

3 Cryptographic Module Interfaces

The module's ports and associated FIPS defined logical interface categories are listed in **Table 4**. The ports are defined as the PCB traces crossing the perimeter of the physical cryptographic boundary. The module inhibits all control output upon entry into the error state.

Table 4 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
PCIe Intf.(16 lane):	Control In; Data In; Data Out; Status Out; Control Out	**Control In**: IO Commands, Management Control Messages, PCIE_RESET_N; **Data In**: Plaintext Data, Status Information from Host; **Data Out**: Plaintext Data to Host; **Status Out**: Good or Error Status Response from Adapter to Host; **Control Out**: I/O Commands from received from connection peers
SMBus Interface:	Control In; Status Out	Used for connection to BMC (Baseboard Management Controller) on server. **Control In:** MCTP Control Messages, NCSI and PLDM Server Management commands are received. Adapter status queries and config commands received from Server Management software; **Status Out:** Response to MCTP Control Messages, NCSI and PLDM Server Management commands. Adapter sends out status via response to MCTP, NCSI and PLDM Status commands.
I2C General Purpose(x1):	Control Out; Data In	1x Connect to External uController. Always Enabled. **Control Out:** Reset uController, Download uController Firmware update from external Flash to the EEPROM; **Data In:** Check current uController Firmware version, Get uController EEPROM Slot details where uController Firmware can be installed, Get Power Consumption details
I2C General Purpose(x2):	N/A	Disabled
Fibre Channel (4x):	Control In; Data In; Data Out; Status Out; Control Out	**Control In**: I/O Commands from connection peers; **Data In**: Plaintext data, ciphertext data, encrypted cryptographic keys and CSPs, authentication data from connection peer. IO Command Status information in from connection peer; **Data Out**: Plaintext data, ciphertext data, encrypted cryptographic keys and CSPs; **Status Out**: IO Command Status information out to connection peer; **Control Out**: I/O Commands to connection peers
I2C SFP Master (x4):	Data In; Control Out	The I2C SFF/SFP interface is used to control and monitor the Fibre Channel Link Transceivers. **Data In**: SFP performance data, temperature status, SFP Revision Number, SFP Vendor Specific Data etc. are read over the I2C interface; **Control Out**: Control Commands to control SFP operational parameters.

Physical Port	Logical Interface	Data that passes over port/interface
GPIO (x73):	Data In; Status Out; Control In; Control Out	GPIO pins are normally used for misc. controls and status inputs. **Control Out:** SFP, Misc Control Signals; **Status Out:** Status LEDs; **Control In:** Config Control Signals; **Data In**: SFP, Misc Status Signals
Proc. UARTs (Qty. 2):	N/A	Disabled.
Test and Debug IOs	N/A	Disabled.
JTAG Interface:	N/A	Disabled.
Power	Power; Control Out	**Power**: Power in from PCIe interface via Power Regulators; **Control Out:** SVS signal to Control ASIC core Voltage based on process corner

4 Roles, Services and Authentication

4.1 Assumption of Roles and Related Services

The module supports a single operator role, the Cryptographic Officer (CO) Role. The services that are available to the Cryptographic Officer are described later in the document.

Table 5 lists all services supported by the module in the CO Role.
The module does not support authentication; the CO role is implicitly assumed.
The module does not support a maintenance role.
The module supports a Bypass Capability.
The module does not support concurrent operators.
The module does not support a self-initiated cryptographic output capability.

Bypass
On a **connection** between a Host Initiator Entity on a Storage Server Appliance and Host Target Entity on a Storage Device Appliance, encryption can be enabled or disabled. A Bypass capability is defined.
A **connection** could be established to start operating in a non-protected mode with Encrypted Data In Flight (EDIF) disabled. It could then transition to operating in a protected mode with EDIF, once encryption parameters and traffic selectors have been negotiated with the peer entity by the host.
The following conditions need to be met in the transition to encrypted mode of operation for a connection:

a. The module receives a command with encryption parameters and Traffic Selectors, to enable a connection to move to an encrypted mode of operation.
b. The module will verify the integrity of the governing bypass information in the **connection table** aka Remote Peer Information (RPI) table through an approved integrity technique (SHA2-256) immediately preceding modification of the governing information and generates a new integrity value using the Approved integrity technique immediately following the modification. A failure in this test is considered fatal for the adapter. The adapter is internally reset by the FW triggering a restart that includes reloading the FW and re-running all the pre-operational self-tests.
c. The module performs a conditional Bypass SP-to-SP internal loopback self-test to check that the module is in a valid operational state for the connection. Check that specific types of frames targeted for encryption for the connection are correctly encrypted and decrypted after the SADB requested in the command for the connection is installed. A failure in this test is considered fatal for the adapter. The adapter is internally reset by the FW triggering a restart that includes reloading the FW and re-running all the pre-operational self-tests.

As a result of configuration changes, a **connection** can transition to outputting data in a non-protected form with EDIF disabled.
The following conditions need to be met in the transition to non-encrypted mode of operation for a connection that prevents the inadvertent bypass of plaintext data due to a single error:

a. The module receives a command for the connection, in order for the connection to move to a non-encrypted mode of operation.
b. The module will verify the integrity of the governing bypass information in the **connection table** aka Remote Peer Information (RPI) table through an approved integrity technique (SHA2-256) immediately preceding modification of the governing information and generate a new integrity value using the Approved integrity technique immediately following the modification. A failure in this test is considered fatal for the adapter. The adapter is internally reset by the FW triggering a restart that includes reloading the FW and re-running all the pre-operational self-tests.

c. The module performs a conditional Bypass SP-to-SP internal loopback self-test to check that the module is in valid operational state for the connection. Check that frames targeted for the connection are no longer encrypted and decrypted using the deactivated SADB. A failure in this test is considered fatal for the adapter. The adapter is internally reset by the FW triggering a restart that includes reloading the FW and re-running all the pre-operational self-tests.

Table 5 – Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Firmware Update	Firmware package and signature	Return Status: Success or Error
CO	Data-In-Flight Encryption	Plaintext Commands from Host, Plaintext FC Frame Data from Host	Encrypted FC Frames to FC links, Return Status: Success or Error
CO	Data-In-Flight Decryption	Plaintext Commands from Host, Encrypted FC Frames from FC Links	Plaintext FC Frame Data to Host, Return Status: Success or Error
CO	Self-Tests	Self-Tests are executed after Power On; Certain Self Tests are run on a continuous basis; Certain Self Tests are run on a conditional basis; Certain Self Tests are run on a periodic basis; Self-Tests can be run On-Demand by power cycling or resetting	Return Status: Success or Error, Self-Tests are executed after Power On
CO	Zeroize	Zeroizes SSPs, except SSP1 (RSA Public Key In ROM) on Reset, UnReg_SADB Command, UnReg RPI Command, Function reset	Return Status: Success or Error
CO	Host-based Storage Peer Key Management	Pass-Through Auth-ELS frames from Host; Pass-Through Auth-ELS frames from FC Links from Storage Peer	Pass-Through Auth-ELS frames to FC Links to Storage Peer; Pass-Through Auth-ELS frames to Host from Storage Peer
CO	Importing SADB from Host	Security Association Data Base with Plaintext Tx 256b key, Plaintext Rx 256b key, Plaintext 32b Tx Salt, Plaintext 32b Rx Salt	Return Status: Success or Error
CO	Link, Connection Management	Establishing and Monitoring connection between peers. See SLI Doc: FC Command Reference	Return Status: Success or Error
CO	Chip Management	Adapter Resource Provisioning; Configuration and Management of shared device resources: Functions, Queues, Exchanges, Connections etc. See SLI Doc: Adapter Management Commands.	Return Status: Success or Error
CO	Show Version	Command to Show Version	Return Adapter Version; Return Cryptographic Module Version; Return ASIC Part Number; Return FW Version
CO	Show Status	Read current Global Status: Approved Mode or Error State	Return Global Status
CO	Diagnostic Dump	Command to send Diagnostic Dump to Host	Diagnostic Dump - No SSPs dumped.

4.2 Services

All Approved services implemented by the module are listed in **Table 6** below. The module does not support any non-Approved services.

The following SSPs are declared:

SSP1: RSA Public Key stored in ROM
SSP2: Child_SA Tx key stored in Memory in SADB data structure
SSP3: Child_SA Rx key stored in Memory in SADB data structure
SSP4: Child_SA Tx Salt stored in Memory in SADB data structure
SSP5: Child_SA Rx Salt stored in Memory in SADB data structure

The SSPs modes of access shown in **Table 6** are defined as:

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 = Zeroize: The module zeroizes SSPs.

Table 6 – Approved Services

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator
Firmware Update	The Adapter can download FW, signed using RSA 2048, from Host to **update** existing Flash code. The downloaded FW is only enabled for execution after the next reset cycle, if signature verification passes. Signature generation is a factory process that is authorized to release FW Updates.	RSA Signature Verification	SSP1: RSA Public Key stored in ROM	CO	E	Status Indicator: Success, Error
Data in Flight Encryption	The Module has capability to Encrypt Transmitted FC Frames based on Security Association parameters (Keys, Traffic Selectors) that have been negotiated for a connection	AES-GCM	SSP2: Child_SA Tx key stored in Memory in SADB data structure; SSP4: Child_SA Tx Salt stored in Memory in SADB data structure	CO	E, Z	Status Indicator: Success, Error

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator
Data in Flight Decryption	The module has capability to Decrypt Received FC Frames, and enforce encryption requirements based on Security Association parameters (Keys, Traffic Selectors) that have been negotiated for a connection.	AES-GCM	SSP3: Child_SA Rx key stored in Memory in SADB data structure; SSP5: Child_SA Rx Salt stored in Memory in SADB data structure	CO	E, Z	Status Indicator: Success, Error
Self-Tests	Self-Tests are executed after Power On Certain Self Tests are run on a continuous basis Certain Self Tests are run on a conditional basis Certain Self Tests are run on a periodic basis	AES-GCM; DRBG; ENT - RCT, APT RSA2048; SHA2-256	N/A	CO	N/A	Status Indicator: Success, Error
Zeroize	Zeroizes SSPs, except SSP1 (RSA Public Key, In ROM)	Zeroization process	SSP2: Child_SA Tx key stored in Memory in SADB data structure; SSP3: Child_SA Rx key stored in Memory in SADB data structure; SSP4: Child_SA Tx Salt stored in Memory in SADB data structure; SSP5: Child_SA Rx Salt stored in Memory in SADB data structure	CO	Z	Status Indicator: Success, Error
Host-based Storage Peer Key Management	The Host executes protocol (typically AUTH_ELS) for establishing Security Association with a Storage Peer that it wants to establish a connection with EDIF capability. The module provides pass-through facility for AUTH_ELS frames from Host to Peer. The module provides pass-through facility for Auth_ELS frames from Peer to Host.	No security functions on module used	N/A	CO	N/A	Status Indicator: Success, Error

Service	Description	Approved Security Functions	SSPs	Roles	Access rights	Indicator
Importing SADB from Host	The Host sends SADB parameters to module.	No security functions on module used	SSP2: Child_SA Tx key stored in Memory in SADB data structure; SSP3: Child_SA Rx key stored in Memory in SADB data structure; SSP4: Child_SA Tx Salt stored in Memory in SADB data structure; SSP5: Child_SA Rx Salt stored in Memory in SADB data structure	CO	Write	Status Indicator: Success, Error
Link, Connection Management	Establishing and Monitoring connection between peers. See SLI Doc: FC Command Reference	No security functions on module used	N/A	CO	N/A	Status Indicator: Success, Error
Chip Management	Adapter Resource Provisioning Configuration and Management of shared device resources: Functions, Queues, Exchanges, Connections etc. See SLI Doc: Adapter Management Commands.	No security functions on module used	N/A	CO	N/A	Status Indicator: Success, Error
Show Version	Provides the version ID of the running firmware. See SLI Doc: Adapter Management Commands.	No security functions on module used	N/A	CO	N/A	Status Indicator: Version Numbers
Show Status	Read current Global Status: Approved Mode or Error State.	No security functions on module used	N/A	CO	N/A	Status Indicator: Global Mode of Operation
Diagnostic Dump	Command to send Diagnostic Dump to Host. No SSPs are included in the dump.	No security functions on module used	N/A	CO	N/A	Status Indicator: Success, Error

5 Software/Firmware Security

The module is composed of the following major firmware components:

- SRB (Software Register Block) Processor FW
- ULP (Upper Layer Protocol) Processors FW
- SP (Support Processor) FW

The firmware components are protected with an RSA 2048 digital signature described in Table 3 – Approved Algorithms.

The operator can initiate the FW integrity test on demand by initiating a PCIe Reset or a Power Cycle.

6 Operational Environment

The module has a limited operational environment under the FIPS 140-3 definitions.

The module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-3 CMVP program will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the module defined by this Security Policy or covered by this validation.

7 Physical Security

The module asserts conformance with FIPS 140-3 Level 1 requirements only. The module is constructed of production grade components with a standard passivation applied to all.

8 Non-Invasive Security

The module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in **Table 7** below:

Table 7 – SSP Management Methods

Method	Description
G1	Generated external to the module and installed during manufacturing
G2	Unmodified output of the internal ENT (P) during power-up
G3	Derived from the DRBG input per [90Ar1]
G4	Generated external to the module on the host
S1	Stored in plaintext in volatile memory (RAM)
S2	Stored in ROM in plaintext
E1	Input in plaintext from the host
Z1	Zeroized by module power cycle or hard reset
Z2	Zeroized by overwriting with a fixed pattern when no longer required and by the zeroize command

9.1 Sensitive Security Parameters (SSP)

All SSPs used by the module are described in this section. All usage of these SSPs by the module is described in the services detailed in Section **4.2 Services**.

Table 8 – SSPs Management

SSP	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Estab-lishment	Storage	Zeroisation	Use / Related SSPs
SSP2: Child_SA Tx	256	AES-GCM [38D] /#A2695	G4 Generated External to the Module on the Host	E1 Input in Plaintext from the Host	N/A	S1 Stored in plaintext in volatile memory (RAM)	Z1 Zeroized by Module power cycle or hard reset Z2 Zeroized by overwriting with a fixed pattern, when no longer required, on UNREG_SADB command or UNREG_RPI command or PCIe Function Reset	Data in Flight Encryption. 256b key stored in memory in SADB data structure
SSP3: Child_SA Rx	256	AES-GCM [38D] /#A2695	G4 Generated External to the Module on the Host	E1 Input in Plaintext from the Host	N/A	S1 Stored in plaintext in volatile memory (RAM)	Z1 Zeroized by Module power cycle or hard reset Z2 Zeroized by overwriting with a fixed pattern, when no longer required, on UNREG_SADB command or UNREG_RPI command or PCIe Function Reset	Data in Flight Decryption. 256b key stored in memory in SADB data structure
SSP4: Child_SA Tx Salt	32	AES-GCM [38D] /#A2695	G4 Generated External to the Module on the Host	E1 Input in Plaintext from the Host	N/A	S1 Stored in plaintext in volatile memory (RAM)	Z1 Zeroized by Module power cycle or hard reset Z2 Zeroized by overwriting with a fixed pattern, when no longer required, on UNREG_SADB command or UNREG_RPI command or PCIe Function Reset	Data in Flight Encryption Tx 32b salt stored in memory in SADB data structure
SSP5: Child_SA Rx Salt	32	AES-GCM [38D] /#A2695	G4 Generated External to the Module on the Host	E1 Input in Plaintext from the Host	N/A	S1 Stored in plaintext in volatile memory (RAM)	Z1 Zeroized by Module power cycle or hard reset Z2 Zeroized by overwriting with a fixed pattern, when no longer required, on UNREG_SADB command or UNREG_RPI command or PCIe Function Reset	Data in Flight Decryption Rx 32b salt stored in memory in SADB data structure
SSP1: RSA Public Key	112	RSA /#A2691 SHA /#A2694	N/A	N/A	N/A	S2 Stored in ROM in plaintext	N/A	RSA 2048 Public Key for firmware signature verification

9.2 DRBG Entropy Source

The module supports an entropy source, which is not currently used.

Table 9 – Entropy Source

Entropy Sources	Minimum number of entropy bits	Details
N/A	N/A	N/A

10 Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-3, these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are available on demand by power cycling the module.

The self-tests error states and status indicator are described in table below:

Table 10 – Error States and Indicators

Error state	Description	Indicator
ES0	The module fails the RSA KAT OR the SHA2-256 KAT OR The module fails SRB Processor Firmware Integrity Test --- On any failure, the module will indicate an error and halt. No services are available in this state.	On Error: Error indication in SECURITY_ERROR register
ES1	The module fails SP processor FW Integrity Test or The module fails ULP FW Integrity Test or The module fails AES-GCM, Pre-Operational Bypass Test, DRBG KAT, SP800-90B RCT or APT self-tests --- On any failure, the module will indicate an error and reset.	On Error: READY bit set to 0 in PORT STATUS register with error details further provided in PORT ERROR1 and ERROR2 registers
ES2	The module fails bypass conditional self-test or The DRBG fails [90Ar1] Health Tests or The ENT fails the RCT and APT Continuous Health Tests. --- On any failure, the Module will indicate an error and reset.	On Error: READY bit set to 0 in PORT STATUS register with error details further provided in PORT ERROR1 and ERROR2 registers

The Module performs the following pre-operational self-tests:

Table 11 – Pre-Operational Self-Tests

Security Function	Method	Description	Error state
SRB Firmware integrity	SigVer, RSA2048, SHA2-256	The SRB processor module performs the SRB Firmware Integrity Test using RSA 2048 (CAVP Cert. #A2691) and SHA2-256 (CAVP Cert. #A2694).	ES0
SP FW Integrity	SigVer, RSA2048, SHA2-256	The SP processor module performs the SP Firmware Integrity Test using RSA 2048 (CAVP Cert. #A2691) and SHA2-256 (CAVP Cert. #A2694).	ES1
ULP FW Integrity	SigVer, RSA2048, SHA2-256	The SP processor module performs the ULP Firmware Integrity Test using RSA 2048 (CAVP Cert. #A2691) and SHA2-256 (CAVP Cert. #A2694).	ES1
Bypass	Activation switch testing	As a part of Pre-Operation Self-Test, the module verifies the data path by - Setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed, and - Setting the bypass switch to not provide cryptographic processing and verify that data transferred through the bypass mechanism is not cryptographically processed.	ES1

The module performs the following conditional self-tests:

Table 12 – Conditional Self-Tests

Security Function	Method	Description	Error state
RSA (CAVP Cert. #A2691)	KAT	Before executing the FW Integrity Test, the ROM based FW boot code executes the FIPS186-4 RSA Verify KAT with 2048-bit key.	ES0
SHS (CAVP Cert. #A2694)	KAT	Before executing the FW Integrity Test, the ROM based FW boot code executes the FIPS180-4 SHA2-256 KAT.	ES0
AES – GCM (CAVP Cert. #A2695)	KAT	SP800-38D GCM Encrypt KAT with 256-bit key. Please note the module does not employ the inverse function.	ES1
Bypass	Switch integrity	The module will verify the integrity of the governing bypass information in the **connection table** aka Remote Peer Information (RPI) table through an approved integrity technique (SHA2-256) immediately preceding modification of the governing information and generate a new integrity value using the Approved integrity technique immediately following the modification. On a transition from non-encrypted to encrypted mode, the module verifies the data path by: - Setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is encrypted. On a transition from encrypted to non-encrypted mode, the module verifies the data path by: - Setting the bypass switch to not provide cryptographic processing and verify that data transferred through the bypass mechanism is not encrypted.	ES2
ENT (ESV Cert. #E6)	RCT, APT	ESV Cert. #E6. "Startup" Tests (RCT, APT) as specified in [90B] section 4.4 Approved Continuous Health Tests. Results are available in the status register. The entropy source is only executed during self-tests.	ES1
DRBG (CAVP Cert. #A2696)	KAT	CTR_DRBG KAT with AES 256 Results are available in the status register. DRBG KAT (CAVP Cert. #A2696), which also covers the AES ECB (CAVP #A2692) implementation that is solely used within the DRBG. The DRBG and associated AES ECB implementations are only executed during self-tests.	ES1
DRBG Health Test	KAT	The Instantiation, Generate, and Reseed KAT is run before executing every Instantiate, Reseed, and Generate command.	ES2

Security Function	Method	Description	Error state
		The DRBG and associated AES ECB implementations are only executed during self-tests.	
ENT Health Test	RCT, APT	RCT and APT tests as specified in [90B] Section 4.4 Approved Continuous Health Tests are executed on an ongoing basis. The entropy source is only executed during self-tests.	ES2
Firmware Update	Signature Verification	RSA Signature Verification (CAVP Cert. #A2691) of firmware update packages using SSP1.	Transient error. Update rejected.

11 Life-Cycle Assurance

11.1 Procedures for Secure Installation, Initialization, Startup and Operation of the Module.

The cryptographic module does not require any installation activities as it is delivered to the customer installed on a PCIe Host Bus Adapter.

The PCIe Host Bus Adapter can be plugged into an appropriate PCIe slot on a server and is ready for operation on Power-On. All required configuration details are programmed at the factory.

The module will offer the declared services only in the Approved mode of operation. The module status can be determined by reading the READY status in the PORT_STATUS PCIe config register. If the module does not come up in the Approved mode of operation, it will have to be returned to the factory.

11.2 Administrator and Non-Administrator Guidance

The module Approved mode status can be monitored regularly by reading the READY status in the PORT_STATUS PCIe config register, which will be set to ‘1’ for Approved Mode.

All ephemeral keys used by the module are zeroized on reboot, loss of power, connection termination or by the supported Zeroize command.

12 Mitigation of Other Attacks

The module does not implement any mitigation method against other attacks.

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 13 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, October 7, 2022*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[90Ar1]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*