Rajant Corporation

Rajant In-Line Security Module (RiSM)

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.0
Date: September 23, 2025

200 Chesterfield Parkway ● Malvern, PA 19355 ● tel (484) 595-0233 ● fax (484) 595-0244
www.rajant.com

Table of Contents

List of Tables

List of Figures

Acronym	Definition
KAT	Know Answer Test
SSP	Sensitive Security Parameter
CSP	Critical Security Parameter
PSP	Public Security Parameter
NK	Network Key (pre-shared master key for an enclave)
TEK	Traffic Encryption Key
TKPK	Traffic Key Production Key
TKPK-L2	Traffic Key Production Key Level 2 (intermediate key production key)
IV	Initialization Vector
RiSM	Rajant In-Line Security Module
RiSM-MP	Rajant In-Line Security Module Management Protocol
POE	Power over Ethernet
CO	Crypto Officer
FW	Firmware (FW-1 or FW-2 refers to stage 1 boot or stage 2 application firmware)
LKEK	Local Key Encryption Key
PT	Plaintext
CT	Ciphertext
APT	Automatic Protocol Tunneling (Rajant’s proprietary tunneling protocol for BreadCrumb)
FPGA	Field Programmable Gate Array
SICOC	Self-initiated Cryptographic Output Capability
EDC	Error Detection Code

Table 1: Acronyms and Definitions

1 General

1.1 Overview

This document defines the Security Policy for the Rajant In-Line Security Module (RiSM), hereafter denoted the Module.

The RiSM is an in-line network encryption device capable of very high bandwidth over gigabit Ethernet and utilizes very low POE power. The Module is used to secure layer 2 Ethernet communications over the Rajant's Kinetic Mesh® wireless mesh networks. The Module is ruggedized and may be used in extreme environments to secure traffic between endpoints, subnets or a combination.

1.2 Security Levels

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

Table 2: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is a Hardware cryptographic module. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated in-line network encryption devices. The Module is intended to be used with Rajant's Kinetic Mesh® wireless mesh networks to secure traffic between endpoints and/or subnets.

The Module is an in-line network encryption device operating at layer 2 Ethernet. The module has two 10/100/1000 Ethernet interfaces and is powered using POE applied to either Ethernet ports. The plaintext (PT) interface of the Module, labeled POE IN, connects to a device or networking equipment that supports wired Ethernet (laptops, cameras, switches, servers, etc.) for sourcing or terminating unsecured traffic. The ciphertext (CT) interface, labeled POE OUT, connects to the mesh network. An example deployment is shown in Figure 1: RiSM Deployment Example.

The Module receives Ethernet traffic from protected device or network on the PT interface, encrypts and authenticates the payload and then transmits it over the CT interface to the mesh network. The Module receives secure traffic on the CT interface, authenticates and decrypts the payload and then transmits it over the PT interface to the protected device or network. The Rajant mesh network is capable of routing the traffic to its destination based solely on the Ethernet header.

All RiSM modules on the network that possess the pre-shared master key (NK) are considered part of a secure enclave. When modules in a secure enclave exchange data with one another, the data is authenticated using an authenticated encryption cipher (AES-GCM) on every packet exchanged between the participating modules. The TEK, ultimately derived from the pre-shared NK, is used for the AES-GCM cipher.
The module is managed using the management tool and procedures described in the latest version of the RiSM User Guide.

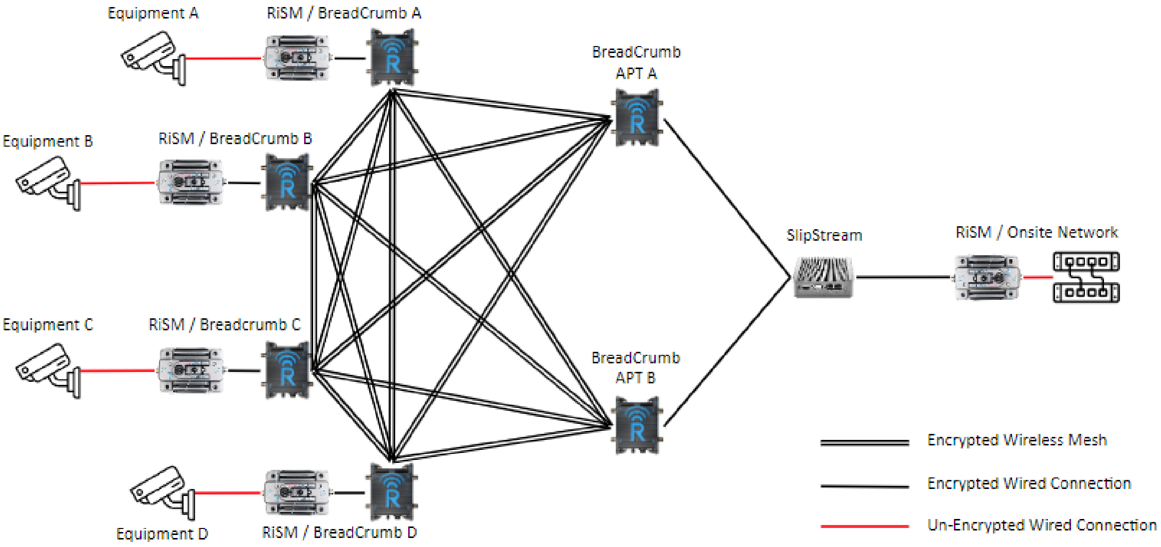


Figure 1: RiSM Deployment Example

Module Type: Hardware

Module Embodiment: MultiChipStand

Module Characteristics:

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 2: RiSM-1SPF. The cryptographic boundary is the physical mechanical enclosure outlined in red.

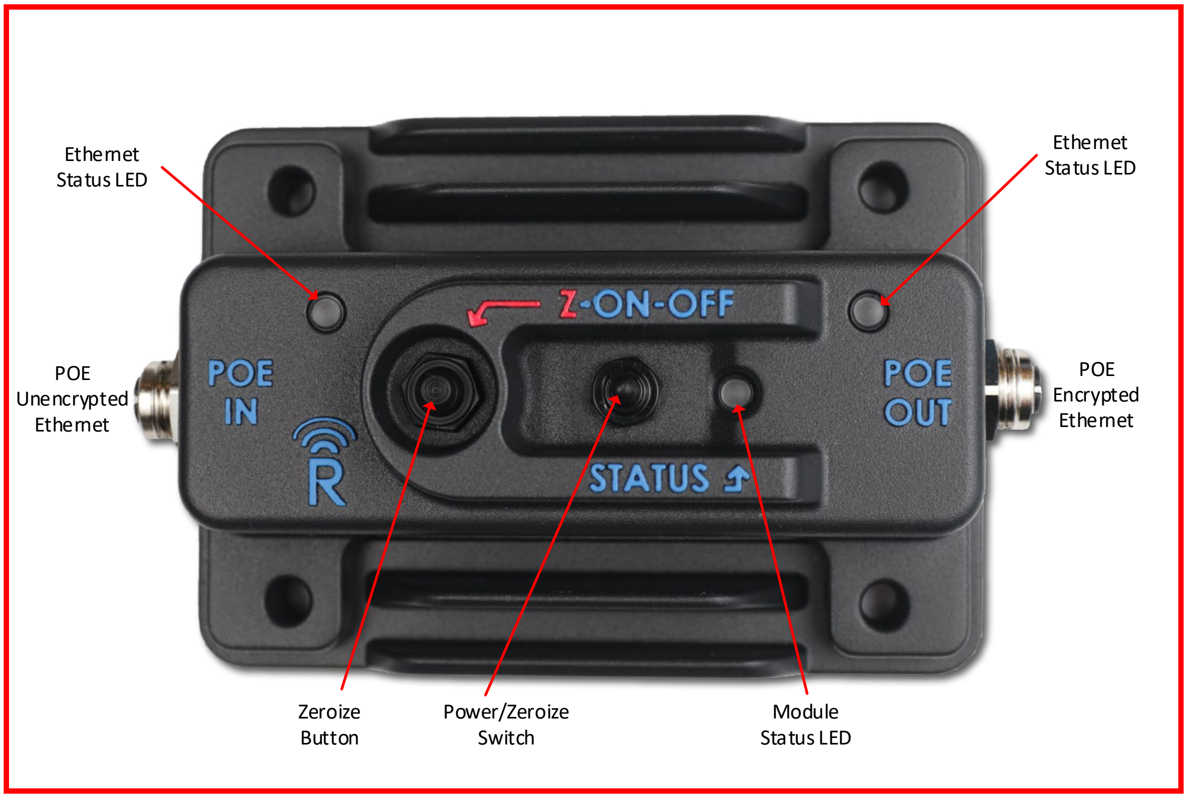


Figure 2: RiSM-1SPF

Tested Operational Environment's Physical Perimeter (TOEPP):

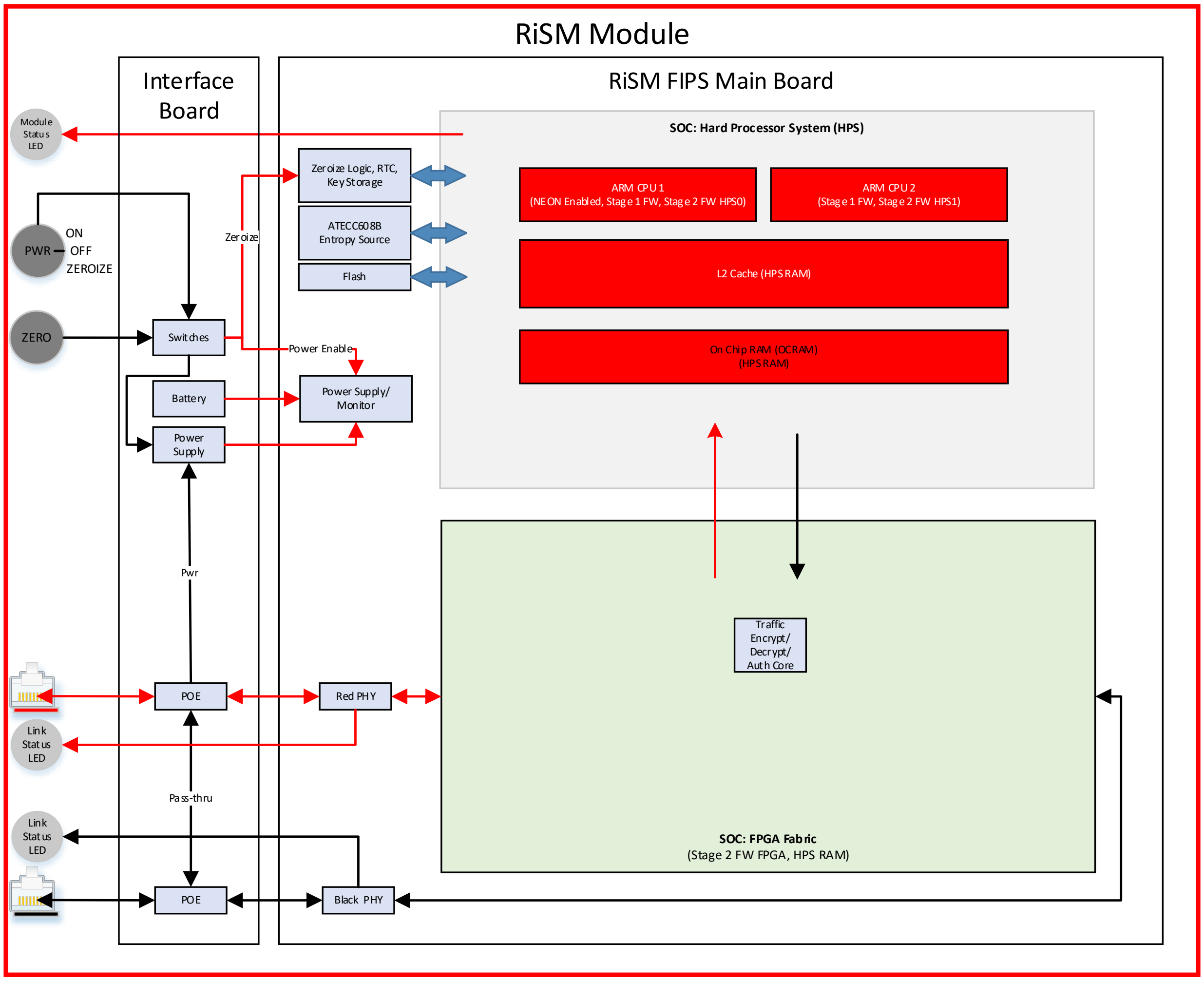


Figure 3: Block Diagram

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
Model: RISM-1SPF P/N: 23-100222-001	2.0	RISM_FIPS_02_03	ARM Cortex-A53 with NEON	

Table 3: 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

This section is not applicable.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The only supported mode of operation.	Approved	Module Status LED

Table 4: Modes List and Description

The Module only operates in Approved mode of operation and is shipped from the factory in this mode. The CO must follow the operational security procedures in this security policy to ensure the module is in Approved mode of operation prior to placing it in service. Approved mode of operation is indicated by a solid yellow, for Approved but un-keyed, or a solid green, for Approved and operational, module status LED after power-up. Data input and output interfaces are only enabled in the Approved and operational mode and no data is processed in any other modes.

Verification of the Approved mode of operation:

The Approved mode of operation is verified at reception of the Module by the CO role with the following steps.

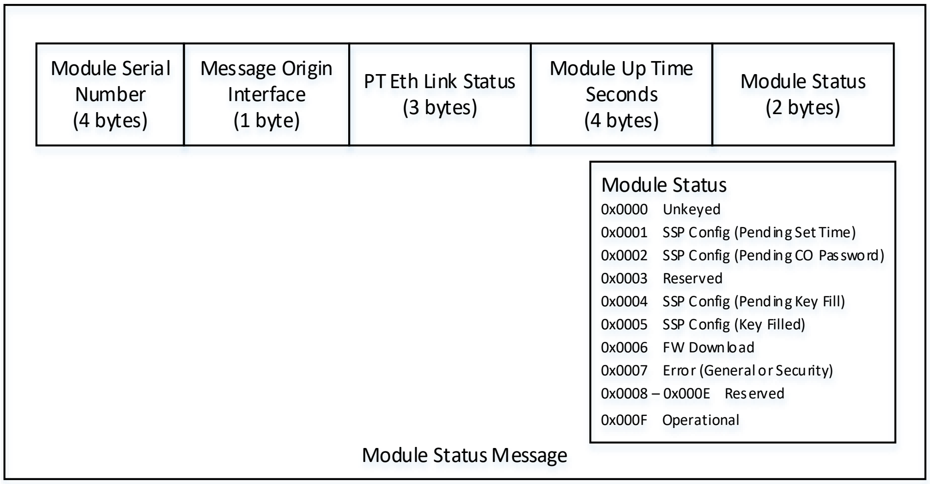
1. Inspect the module and confirm it is a FIPS validated module by matching the model and hardware version is as specified under the tested and vendor affirmed module version and identification section.
2. Inspect the module and confirm the physical security mechanism are as specified in the physical security section.
3. Connect a POE power source to the module’s PT interface (see Figure 2: RiSM-1SPF). The module status LED will indicate a solid cyan during the boot and FIPS self-test.
4. The module status LED will indicate a solid yellow after boot and successful completion of FIPS self-tests.
   Note: If the module status LED is a solid green then the module was previously configured for operation and requires a zeroize operation to revert it back to the default state. Perform a zeroize and verify module status LED is solid yellow after boot and successful completion of FIPS self-tests.
5. Establish a connection between the module’s PT interface and a general purpose PC running management tool. Use the management tool to query the module and verify the firmware version is as specified under the tested module identification section.

The status LED will indicate red for general errors or magenta for self-test and other security failures if the module fails to boot and complete FIPS self-tests successfully. The module will reboot automatically up to three times to automatically recover from errors, after which it will remain in the error state. Contact the manufacturer if it fails to enter Approved mode of operation after multiple power cycle and zeroize attempts.

Status	Color	Description
Solid Gray	●	Device is not powered or failed to boot
Solid Cyan	●	The module is in the process of booting up.
Solid Red	●	The module has encountered an error during its boot process.
Solid Magenta	●	The module has encountered a security critical error during its boot process.
Solid Yellow	●	The module is running in Approved mode and is not fully configured or keyed.
Solid Green	●	The module is running in Approved mode and is fully configured and operational.
Solid Blue	●	The module is applying a previously downloaded application FW image.
Blinking Yellow	⊗	The module is in a sensitive security parameter (SSP) configuration mode allowing the CO to load keys.
Blinking Blue	⊗	The module is actively downloading a FW image.
Blinking Red	⊗	The module has encountered an error while running.
Blinking Magenta	⊗	The module has encountered a security critical error while running.

Table 5: Module Status Led

The module status may also be ascertained using the periodic module status message (UDP port 55580 multicast destination address IPv4 ‘224.0.0.224’ or IPv6 ‘fe90::’) sent every ten seconds over both PT and CT Ethernet interfaces.



Module Serial Number (4 bytes)	Message Origin Interface (1 byte)	PT Eth Link Status (3 bytes)	Module Up Time Seconds (4 bytes)	Module Status (2 bytes)

Module Status

0x0000	Unkeyed
0x0001	SSP Config (Pending Set Time)
0x0002	SSP Config (Pending CO Password)
0x0003	Reserved
0x0004	SSP Config (Pending Key Fill)
0x0005	SSP Config (Key Filled)
0x0006	FW Download
0x0007	Error (General or Security)
0x0008 – 0x000E	Reserved
0x000F	Operational

Module Status Message

Figure 4: Module Status Message

The Ethernet link and activity status are indicated by the Ethernet Status Led for each Ethernet port as show below.

Status	Color	Description
Solid Gray	⚪	Device has no Ethernet link
Solid Red	🔴	10 Link, no activity
Solid Yellow	🟡	100 Link, no activity
Solid Green	🟢	1000 Link, no activity
Blinking Red	⊗	10 activity
Blinking Yellow	⊗	100 activity
Blinking Green	⊗	1000 activity

Table 6: Ethernet Status LED

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A4095	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
AES-GCM	A4096	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
AES-KWP	A4096	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
ECDSA KeyGen (FIPS186-5)	A4096	Curve - P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4096	Curve - P-384, P-521	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4096	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
Hash DRBG	A4096	Prediction Resistance - Yes Mode - SHA2-512	SP 800-90A Rev. 1
HMAC-SHA2-384	A4096	Key Length - Key Length: 8-65536 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4096	Domain Parameter Generation Methods - P-521 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA TwoStep Sp800-56Cr1	A4096	Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2
KDF SP800-108	A4096	KDF Mode - Feedback Supported Lengths - Supported Lengths: 8-4096 Increment 8	SP 800-108 Rev. 1
SHA2-384	A4096	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-512	A4096	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 7: Approved Algorithms

The Module implements the approved cryptographic algorithms listed in the table above.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	symmetric:KDF SP800-108 asymmetric:KAS-ECC-SSC Sp800-56Ar3	Rajant RISM Crypto Library	Key Generation per 133R2 Section 4

Table 8: Vendor-Affirmed Algorithms

The Module implements the vendor affirmed cryptographic algorithms listed in the table above.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-CTR	Obfuscate stage 1 FW per IG 2.4a Scenario 1	Decryption of stage 1 FW image by boot rom
SHA2-256	Redundant stage 1 FW signature verification per IG 2.4a Scenario 2	Signature verification of stage 1 FW image by boot rom
ECDSA P-384	Redundant stage 1 FW signature verification per IG 2.4a Scenario 2	Signature verification of stage 1 FW image by boot rom

Table 9: Non-Approved, Allowed Algorithms with No Security Claimed

The Module implements the non-approved but allowed cryptographic algorithms with no security claimed listed in the table above.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES GCM	BC-Auth	Encrypt/Decrypt RISM MP message, FW download and FW storage		AES-GCM: (A4096) AES-ECB: (A4096)
AES KWP	BC-Auth	Encrypt/Decrypt CSPs		AES-KWP: (A4096) AES-ECB: (A4096)
AES GCM FPGA	BC-Auth	Encrypt/Decrypt data traffic		AES-GCM: (A4095) AES-ECB: (A4095)
DRBG	DRBG	Random bit generator for keys and other random data		Hash DRBG: (A4096) SHA2-512: (A4096)
ECDSA Sig Ver	DigSig-SigVer	Firmware signature verification		ECDSA SigVer (FIPS186-5): (A4096) SHA2-384: (A4096)
KAS-SSC	KAS-SSC	Secure session key agreement shared secret computation		ECDSA KeyVer (FIPS186-5): (A4096) ECDSA KeyGen (FIPS186-5): (A4096) KAS-ECC-SSC Sp800-56Ar3: (A4096)
KAS-KDF	KAS-56CKDF	Secure session key derivation algorithm		KDA TwoStep Sp800-56Cr1: (A4096) HMAC-SHA2-384: (A4096) KDF SP800-108: (A4096) SHA2-384: (A4096)
SHA2-384	SHA	Hash the password		SHA2-384: (A4096)
KBKDF	KBKDF	Derive traffic keys		KDF SP800-108: (A4096) HMAC-SHA2-384: (A4096)

Table 10: Security Function Implementations

The Module implements the security functions listed in the table above.

2.7 Algorithm Specific Information

AES-GCM:

Data Traffic Service deterministic IV generation and restoration:

The data traffic IV consists of a 32-bit fixed field, unique to the module, and a 64-bit invocation field, incremented by 1 after each use. The invocation field wraps after 2^64 increments. However, the module is not capable of reaching this limit as the key duration is 24 hours. The module can at most process 103,846,147,200 Ethernet frames at 1 gigabit link rate in a 24-hour period. The service does not error on wrap around as the 64-bit invocation field space is sufficiently large to ensure an IV cannot wrap around.

The upper 32-bit value of the invocation field is incremented and stored in flash every time the lower 32-bit value wraps. The stored value in flash is used to initialize the upper 32-bits of the invocation field on reset, eliminating the possibility of replicating a previously used invocation field upon restoration.

Secure Session Service deterministic IV generation and restoration:

The secure session IV consists of a 72-bit fixed field, generated randomly each time a new key session key is established and a 24-bit invocation field, incremented by 1 after each use. The invocation field wraps after 2^24 increments after which the secure session is terminated.
A new secure session is established in the case of power loss or reset.

2.8 RBG and Entropy

Cert Number	Vendor Name
E46	Microchip Technology Inc

Table 11: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
ECC608 NRBG Entropy Source	Physical	ATECC608B	1	0.5071	None

Table 12: Entropy Sources

2.9 Key Generation

The module generates symmetric keys in compliance with NIST SP 800-133r2, sections 4, 6.2.1 and 6.2.2, using a NIST SP 800-90A Hash DRBG for random number generation and NIST SP 800-90B entropy source (see section 2.8 RBG and Entropy).

Asymmetric keys are generated in compliance with NIST SP 800-133r2, sections 5.1 and 5.2 and FIPS 140-3 IG D.H.

2.10 Key Establishment

Key establishment is performed in compliance with NIST SP 800-56Arev3 section 6.1.2.2 and NIST SP 800-56CRev2 section 5. No key confirmation is supported.
Key transport is performed in compliance with FIPS 140-3 IG D.G using AES GCM algorithm. See AES-GCM in section 2.7.

2.11 Industry Protocols

The section is not applicable.

2.12 Additional Information

The module implements a proprietary protocol for configuration and management secured with approved cryptographic algorithms. The Rajant In-Line Security Module Management Protocol (RiSM-MP) establishes a logical UDP based authenticated and encrypted control channel over the PT or CT network interface. It utilizes 56Ar3 Ephemeral Unified ECC CDH key agreement scheme to establish a session key to encrypt all sensitive data with AES GCM 256 encryption. The CO role is also authenticated as part of establishing the secure channel.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
OFF/ON/Zeroize Switch	Control Input	None
Zeroize Button	Control Input	None
Module Status LED	Status Output	Color coded module state
PT Eth Status LED	Status Output	Link speed and activity
CT Eth Status LED	Status Output	Link speed and activity
PT Eth/POE IN (M12)	Data Input Data Output Control Input Status Output Power	POE power, PT network traffic, module configuration and management, network control protocols, module status message
CT Eth/POE OUT (M12)	Data Input Data Output Control Input Status Output Power	POE power, CT network traffic, module configuration and management, network control protocols, module status message

Table 13: Ports and Interfaces

The Module’s ports and associated FIPS defined logical interface categories are listed in the above table.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Password	Memorized secret used to authenticate an operator.	SHA2-384	1/95^8	30/95^8

Table 14: Authentication Methods

Password:

The password authentication method is used for role based authentication for operators accessing the module over RiSM-MP secure session.

The minimum passphrase length is eight bytes. The passphrase character set consists of the 95 printable characters of **A-Z**, **a-z**, **0-9**, **space**, and the 32 special characters (**! @ # $ % ^ & * ( ) _ + - = [ ] { } ; ' : “ , . / < > ? \ | ` ~**) .

The Module will reject all operator authentication attempts after 30 consecutive failed attempts for a period of one-minute beginning with the time of first failed attempt. Thus no more than 30 failed authentication attempts are allowed per minute. The probability of a successful passphrase guess in a single attempt using the character set described above is 1/95^8, which is lower than the required 1/1,000,000. The probability of a successful guess using multiple attempts in a one-minute period using the rate limit described above is 30/95^8, which is lower than the required 1/100,000.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	Password

Table 15: Roles

The module supports a single distinct authenticated operator role, Cryptographic Officer (CO). The cryptographic module enforces separation of roles by utilizing role based access control for authenticated services.

The above table lists all roles supported by the module. The Module does not support a maintenance role. The Module does not support bypass capability. The Module does not support concurrent operators.

The CO role is authenticated using a password. The module has a default CO password which must be changed during initialization of the module. The CO password is transmitted to the module encrypted using approved algorithms. The CO role authentication is cleared upon reset as well as after 120 seconds of inactivity and it must be re-established by the operator. Prior authentications are cleared any time a role is authenticated.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Version Information	Retrieve version information (Show Version)	Version data including model, overall FW version, FW component versions, serial number and HW version.	Version request message	Version response message	AES GCM	CO - RISM-MP-SK: E
Status Information	Retrieve module status, HW status, LED status, key status and network statistics (Show Status)	Module status, HW status data, LED status, key status and network statistics data	Request message for module status, HW status, LED status, key status, or network statistics	Response message with module status, HW temp and voltages data, LED status, key status, or network statistics data	AES GCM AES KWP	CO - RISM-MP-SK: E - LKEK-S2: E - LKEK: G,E,Z - NK: E Unauthenticated - LKEK-S2: E - LKEK: G,E,Z - NK: E
Audit Log	Retrieve binary audit log	Binary audit data file	Audit request messages	Audit response messages with audit data	AES GCM	CO - RISM-MP-SK: E
Configuration	Retrieve and configure SSPs and other module parameters	Configuration success or failure response, Configuration value response	Request message to get time, set time, set IP, get MTU, set MTU, enable/disable anti-replay, set	Response message with current time, set time success or failure, set IP success or	AES GCM AES KWP	CO - RISM-MP-SK: E - LKEK-S2: E - LKEK: G,E,Z - NK: W - Password: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			network key, set CO password, enable/disable LEDs, or enter/exit config	failure, current MTU, current MTU, anti-replay enabled setting, set network key result, set CO password success or failure, current LEDs enabled setting or current module state		
Secure Session	Start and stop an encrypted and authenticated session	Session response message with session parameters	Start session message with session parameters, end session message	Start session response message with session parameters, end session response message	DRBG KAS-SSC KAS-KDF AES KWP SHA2-384	CO - RISM-MP-DH: G,E,Z - RISM-MP-DH-Pub: G,R,E,Z - RISM-MP-Secret: G,E,Z - RISM-MP-SK: G,Z - LKEK-S2: E - LKEK: G,E,Z - NK: E - DRBG-EI: E - Password: E - DRBG-State V: E - DRBG-State C: E - 108-KDF Feedback State: G,E,Z - 56Cr1-Two-Step KDA State: G,E,Z - Module Challenge Response: G,R,Z - CO Auth Token: G,W,E,Z - RISM-MP-DH-Pub Peer: W,E,Z
Firmware Update	Download firmware image and verify signature, reset to apply update	Module status FW Download, automatic module reset and zeroize on success	FW update request messages, FW update data message	FW update response message with result	AES GCM ECDSA Sig Ver	CO - RISM-MP-SK: E - FW-2-Update-Pub: E - FW-1-Update-Pub: E
Module reset/Self-test	Module reset, self-test and initialization.	Self-test initiated response, automatic reset of module	Self-test request message	Self-test response message	AES GCM	CO - RISM-MP-SK: E - FW-1-Load-Pub: E
Data traffic	Encrypt/Decrypt network packets between other modules in the enclave. This service is enabled as a result of self-initiated cryptographic	Module status OPERATIONAL	Plaintext, Ciphertext data	Ciphertext, plaintext data	AES GCM FPGA KBKDF	Unauthenticated - TEK: G,E,Z - TKPK: G,E,Z - TKPK-L2: G,E,Z - NK: E - LKEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	output capability configured by the CO using the Configuration service.					
Zeroize	Zeroize the specified SSPs.	Zeroize initiated response, module status STANDBY after automatic reset	Zeroize request message, Manual zeroize with toggle switch and zeroize button	Zeroize response message	AES GCM	CO - RISM-MP-SK: E,Z - DRBG-EI: Z - Password: Z - LKEK: Z - LKEK-S2: Z - NK: Z - TKPK: Z - TKPK-L2: Z - TEK: Z - RISM-MP-DH: Z - RISM-MP-Secret: Z - DRBG-State V: Z - DRBG-State C: Z

Table 16: Approved Services

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

A module running in Approved mode of operation is capable of receiving a firmware update. The firmware update is a partial image replacement, either stage 1 or the stage 2 FW. The firmware update is performed by the CO as follows. See section 6.2 for additional FW loading requirements.

1. Ensure the FW update file is received directly from Rajant. A FW update file from Rajant is signed and encrypted by Rajant. Any other file will fail integrity validation and the FW will not be updated.
2. Perform the FW update using the management tool. Note that the module will be in SSP config state and not encrypt or decrypt data traffic during FW update.
3. The module will perform a ECDSA signature verification FW load test on the downloaded FW.
4. The module will reset automatically after downloading the FW and passing the FW load test to apply the new FW and perform self-tests.
5. Read the module FW version using the management tool and ensure it is matches the new FW version.

4.6 Cryptographic Output Actions and Status

The module supports SICOC initiated by the CO using the module’s Configuration service. The initiation process is described in the section 11.1, under Module Initialization. The module will automatically enter the operational state after boot and show status output of OPERATIONAL, indicating SICOC is active, enabling the Data Traffic service.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware component(s):

- Stage 1 firmware: executable binary stored encrypted in flash
- Stage 2 firmware: executable binary and FPGA image stored encrypted in flash

Stage 1 firmware authenticates its stored flash image using ECDSA P-384. Stage 2 firmware stored flash image integrity is verified using 128-bit EDC.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by performing a module reset or power cycle.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

6.2 Additional Information

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

The Module includes a firmware update service to support necessary updates. Firmware versions validated by CMVP for FIPS 140-3 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

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evident Seal	90 days	Verify there are no cracks in or crumbling of the applied Cyanoacrylate material

Table 17: Mechanisms and Actions Required

The Module is a monolithic mechanical enclosure secured with four screws on the bottom. There are no openings to give visual or physical access to the internal components. The Module must be located in a controlled access area.

The tamper evidence is provided by the use of a cyanoacrylate material (Loctite® 425, mfg. Part no. 42540, available from Rajant) covering selected chassis access screws. Screws requiring application are indicated in figure below.

It is recommended that the CO perform regular inspections of the Module while in operation. The recommended tamper inspection period for the Module is once every 90 days. Any attempt to open the Module will be visible as cracks in the Cyanoacrylate material or crumbling of the material. Zeroize and remove module from service upon tamper detection and contact manufacturer.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seal	90 days	Verify there are no cracks in or crumbling of the applied Cyanoacrylate material.

Table 18: Physical Security Inspection Guidelines

The Module will be shipped from the manufacturer with tamper-evident coatings pre-applied, as shown below.

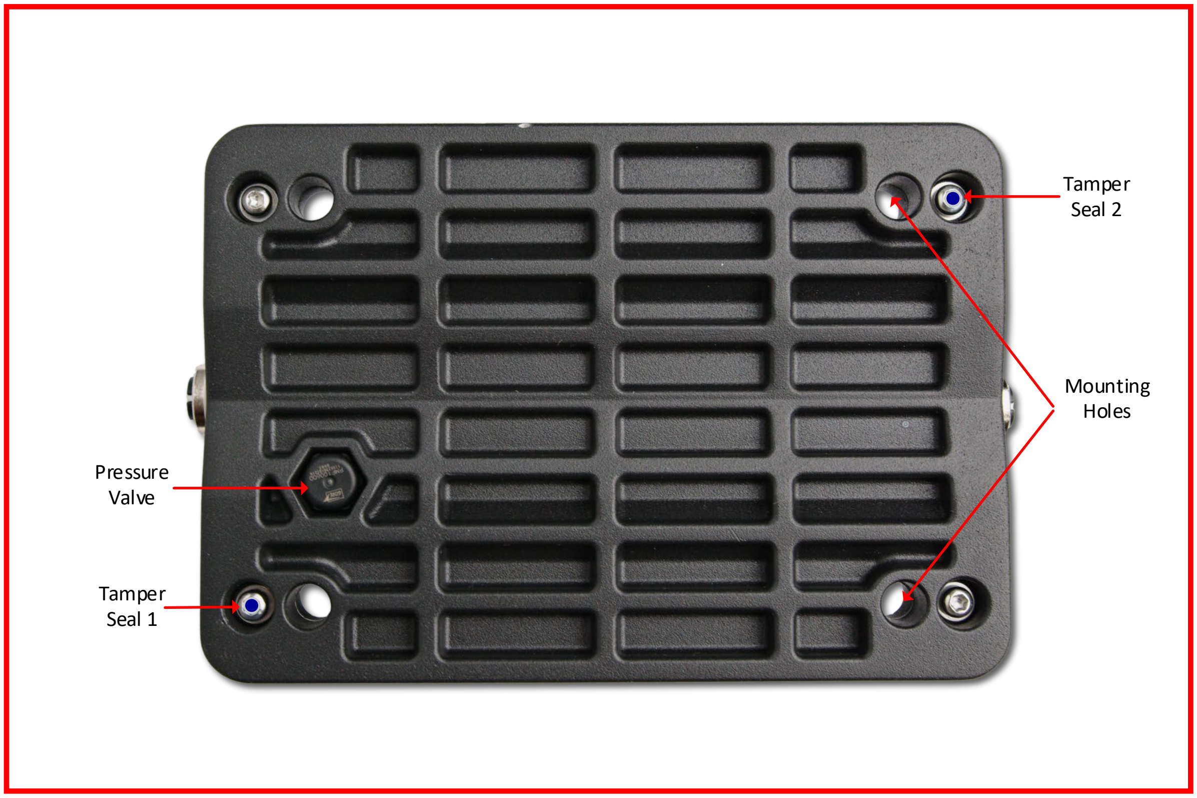


Figure 5: Module Seal Application Locations (Bottom)

Label ID	Placement
Tamper Seal 1	The drive of the screw near pressure relief valve
Tamper Seal 2	The drive of the screw diagonal from pressure relief valve and Tamper Seal 1

Table 19: Tamper-Evident Seal Locations Guidance

7.2 EFP/EFT Information

N/A for this module.

7.3 Hardness Testing Temperature Ranges

N/A for this module.

8 Non-Invasive Security

8.1 Mitigation Techniques

The Module does not implement any mitigation method against non-invasive attacks.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Flash	Flash memory	Static
HPS RAM	RAM incorporated in the HPS and FPGA	Dynamic
Key Storage	Battery backed RAM of security chip	Dynamic

Table 20: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
CO Authentication	Management Tool	Module	Plaintext	Automated	Electronic	SHA2-384
Module Authentication	Module	Management Tool	Plaintext	Automated	Electronic	SHA2-384
Config	Management Tool	Module	Encrypted	Automated	Electronic	AES GCM
FW Update	Manufacturer	Module	Encrypted	Automated	Electronic	AES GCM
Pre-loaded	Manufacturer	Module	Encrypted	N/A	N/A	AES GCM

Table 21: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Overwrite	Overwrite SSP with all zeros or perform an erase operation in flash, and then write new value.	An overwritten or erased memory location in RAM or flash is unrecoverable by hardware design.	Zeroize command issued remotely, manual zeroize using physical switch and button or a FW update operation.

Table 22: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI	Entropy input	888 - 256	Entropy - CSP	ECC608 NRBG Entropy Source		DRBG
DRBG-State V	DRBG Internal state	888 - 256	Entropy - CSP	DRBG		DRBG
DRBG-State C	DRBG Internal state	888 - 256	Entropy - CSP	DRBG		DRBG
108-KDF Feedback State	108 KDF Feedback internal state	384 - 192	Derivation material - CSP	HMAC-SHA2-384 (A4096)		KBKDF
56Cr1-Two-Step KDA State	56Cr1 Two-Step KDA internal state	384 - 192	Derivation material - CSP	HMAC-SHA2-384 (A4096)		KAS-KDF
Password	CO authentication password	64 - 1/95^8	Authentication - CSP			SHA2-384
CO Auth Token	CO password hash	384 - 192	Authentication - CSP	SHA2-384		
Module Challenge Response	Module authentication hash	384 - 192	Authentication - CSP	SHA2-384		
LKEK	SSP encryption key	256 - 256	Symmetric - CSP	KBKDF		AES KWP
LKEK-S2	LKEK derivation key	256 - 256	Symmetric - CSP	DRBG		KBKDF
NK	TKPK derivation key	256 - 256	Symmetric - CSP			KBKDF
TKPK	TKPK-L2 derivation key	256 - 256	Symmetric - CSP	KBKDF		KBKDF
TKPK-L2	TEK derivation key	256 - 256	Symmetric - CSP	KBKDF		KBKDF
TEK	Traffic encryption key	256 - 256	Symmetric - CSP	KBKDF		AES GCM FPGA
RISM-MP-SK	CO session encryption key	256 - 256	Symmetric - CSP		KAS-KDF	AES GCM
RISM-MP-DH	CO session private key	P-521 - 256	Private - CSP	DRBG		KAS-SSC
RISM-MP-Secret	CO session 56Ar3 generated secret	P-521 - 256	Derivation material - CSP	KAS-SSC		KAS-KDF
RISM-MP-DH-Pub	CO session module public key	P-521 - 256	Public - PSP	ECDSA KeyGen (FIPS186-5) (A4096)		KAS-SSC
RISM-MP-DH-Pub Peer	CO session peer public key	P-521 - 256	Public - PSP			KAS-SSC
FW-2-Update-Pub	Stage 2 FW integrity public key used to verify new image	384 - 192	Not an SSP - Neither			ECDSA Sig Ver
FW-1-Update-Pub	Stage 1 FW integrity public key used to verify new image	384 - 192	Not an SSP - Neither			ECDSA Sig Ver
FW-1-Load-Pub	Stage 1 FW integrity public key used on boot	384 - 192	Not an SSP - Neither			ECDSA Sig Ver

Table 23: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI		HPS RAM:Plaintext	While in use	Overwrite	
DRBG-State V		HPS RAM:Plaintext	Until zeroized	Overwrite	
DRBG-State C		HPS RAM:Plaintext	Until zeroized	Overwrite	
108-KDF Feedback State		HPS RAM:Plaintext	While in use	Overwrite	
56Cr1-Two-Step KDA State		HPS RAM:Plaintext	While in use	Overwrite	
Password	Config	HPS RAM:Plaintext Flash:Encrypted	While in use	Overwrite	LKEK:Wrapped by CO Auth Token:Hash input for
CO Auth Token	CO Authentication	HPS RAM:Plaintext	While in use	Overwrite	Password:Hash digest of NK:Hash digest of
Module Challenge Response	Module Authentication	HPS RAM:Plaintext	While in use	Overwrite	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
LKEK		HPS RAM:Plaintext	While in use	Overwrite	Password:Wraps NK:Wraps LKEK-S2:Derived from
LKEK-S2		Key Storage:Plaintext	Until zeroized	Overwrite	LKEK:Derives
NK	Config	HPS RAM:Plaintext HPS RAM:Encrypted Flash:Encrypted	While in use	Overwrite	LKEK:Wrapped by TKPK:Derives CO Auth Token:Hash input for
TKPK		HPS RAM:Plaintext HPS RAM:Encrypted	While in use	Overwrite	NK:Derived from TKPK-L2:Derives LKEK:Wrapped by
TKPK-L2		HPS RAM:Plaintext HPS RAM:Encrypted	While in use	Overwrite	TKPK:Derived from TEK:Derives LKEK:Wrapped by
TEK		HPS RAM:Plaintext HPS RAM:Encrypted	While in use	Overwrite	TKPK-L2:Derived from LKEK:Wrapped by
RISM-MP-SK		HPS RAM:Plaintext	While in use	Overwrite	RISM-MP-Secret:Derived from
RISM-MP-DH		HPS RAM:Plaintext	While in use	Overwrite	RISM-MP-Secret:Derives RISM-MP-DH-Pub:Paired With
RISM-MP-Secret		HPS RAM:Plaintext	While in use	Overwrite	RISM-MP-DH:Derived from RISM-MP-DH-Pub Peer:Derived from RISM-MP-SK:Derives
RISM-MP-DH-Pub	CO Authentication	HPS RAM:Plaintext	While in use	Overwrite	RISM-MP-DH:Paired With
RISM-MP-DH-Pub Peer	CO Authentication	HPS RAM:Plaintext	While in use	Overwrite	RISM-MP-Secret:Derives
FW-2-Update-Pub	Pre-loaded FW Update	HPS RAM:Plaintext Flash:Encrypted	Until zeroized	Overwrite	
FW-1-Update-Pub	Pre-loaded FW Update	HPS RAM:Plaintext Flash:Encrypted	Until zeroized	Overwrite	
FW-1-Load-Pub	Pre-loaded FW Update	HPS RAM:Plaintext Flash:Plaintext	Until zeroized	Overwrite	

Table 24: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RAM Test	N/A		Critical Function	status OPERATIONAL or STANDBY	Write and verify data pattern in RAM
FW-1 Integrity	P-384 curve		SW/FW Integrity	status OPERATIONAL or STANDBY	Verify stage 1 FW signature
FW-2 Integrity	128-bit EDC		SW/FW Integrity	status OPERATIONAL or STANDBY	Verify stage 2 FW using EDC method
Control Path	N/A		Critical Function	status OPERATIONAL or STANDBY	Performs a control path packet injection test from PT to CT and CT to PT interfaces

Table 25: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2 384	N/A	KAT	CAST	status OPERATIONAL or STANDBY	Digest	Boot, FW Download
SHA2 512	n/A	KAT	CAST	status OPERATIONAL or STANDBY	Digest	Boot
ECDSA Key Gen	P-521 curve	KAT	CAST	status OPERATIONAL or STANDBY	Generate public key	Boot
ECDSA Key Ver	P-521 curve	KAT	CAST	status OPERATIONAL or STANDBY	Verify public key	Boot
ECDSA Sig Ver	P-384 curve	KAT	CAST	status OPERATIONAL or STANDBY	Verify signature	Boot, FW Download
AES GCM Encrypt	256 bit key, 96 bit IV, 128 bit tag	KAT	CAST	status OPERATIONAL or STANDBY	Encrypt	Boot
AES GCM Decrypt	256 bit key, 96 bit IV, 128 bit tag	KAT	CAST	status OPERATIONAL or STANDBY	Decrypt	Boot
AES KWP Wrap	256 bit key	KAT	CAST	status OPERATIONAL or STANDBY	Wrap	Boot
AES KWP Unwrap	256 bit key	KAT	CAST	status OPERATIONAL or STANDBY	Unwrap	Boot
KAS SSC	P-521 curve	KAT	CAST	status OPERATIONAL or STANDBY	Generate shared secret	Boot
KDA Two-Step	256 bit key, SHA-384, 68 bytes fixed data	KAT	CAST	status OPERATIONAL or STANDBY	Derive key	Boot
DRBG Instantiate	888 bits entropy, 128 bit nonce	KAT	CAST	status OPERATIONAL or STANDBY	Generate C and V	Boot
DRBG Generate	128 bytes of random data	KAT	CAST	status OPERATIONAL or STANDBY	Generate random data	Boot
DRBG Reseed	888 bits reseed entropy	KAT	CAST	status OPERATIONAL or STANDB	Update C and V	Boot
KDF Feedback	384 bit key, 384 bit IV, 2400 bit output key, 51 bytes fixed data	KAT	CAST	status OPERATIONAL or STANDBY	Derive key	Boot
HMAC	SHA2-384	KAT	CAST	status OPERATIONAL or STANDBY	Generate MAC	Boot
Entropy Health Test	N/A	RCT, APT	CAST	status OPERATIONAL or STANDBY	Perform entropy source health tests	DRBG request
AES GCM FPGA Encrypt	256 bit key, 96 bit IV, 128 bit tag	KAT	CAST	status OPERATIONAL or STANDBY	Encrypt	Boot
AES GCM FPGA Decrypt	256 bit key, 96 bit IV, 128 bit tag	KAT	CAST	status OPERATIONAL or STANDBY	Decrypt	Boot
KAS Ephemeral Key PCT	P-521 Curve	PCT	PCT	CO Authenticated	Verify ephemeral key pair per 56Ar3	CO Authentication
FW-1 Update	ECDSA P-384	Sig Ver	SW/FW Load	module reboot	Verify signature of downloaded image	FW Download
FW-2 Update	ECDSA P-384	Sig Ver	SW/FW Load	module reboot	Verify signature of downloaded image	FW Download

Table 26: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RAM Test		Critical Function		
FW-1 Integrity		SW/FW Integrity		
FW-2 Integrity		SW/FW Integrity		
Control Path		Critical Function		

Table 27: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2 384	KAT	CAST		
SHA2 512	KAT	CAST		
ECDSA Key Gen	KAT	CAST		
ECDSA Key Ver	KAT	CAST		
ECDSA Sig Ver	KAT	CAST		
AES GCM Encrypt	KAT	CAST		
AES GCM Decrypt	KAT	CAST		
AES KWP Wrap	KAT	CAST		
AES KWP Unwrap	KAT	CAST		
KAS SSC	KAT	CAST		
KDA Two-Step	KAT	CAST		
DRBG Instantiate	KAT	CAST		
DRBG Generate	KAT	CAST		
DRBG Reseed	KAT	CAST		
KDF Feedback	KAT	CAST		
HMAC	KAT	CAST		
Entropy Health Test	RCT, APT	CAST		
AES GCM FPGA Encrypt	KAT	CAST		
AES GCM FPGA Decrypt	KAT	CAST		
KAS Ephemeral Key PCT	PCT	PCT		
FW-1 Update	Sig Ver	SW/FW Load		
FW-2 Update	Sig Ver	SW/FW Load		

Table 28: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	Boot Error	Bootrom fails to load stage 1 FW	Power cycle, contact manufacturer	The module status LED will be off
ES2	Stage 1 FW Error	Any self-test failure in stage 1 FW Processor exception in stage 1 FW Unrecoverable error in stage 1 FW	Power cycle, contact manufacturer	The module status LED will be solid red for general error, solid magenta for security error
ES3	Stage 2 FW Error	Any self-test failure in stage 2 FW Processor exception in stage 2 FW Unrecoverable error in stage 2 FW	Power cycle, contact manufacturer	The module status LED will be flashing red for general error, flashing magenta for security error

Table 29: Error States

10.5 Operator Initiation of Self-Tests

The Module allows the operator to initiate power-up self-tests by manually power cycling the power or remotely resetting the Module using the self-test service.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The CO must perform the following steps to securely deploy modules in Approved mode of operation.

Deployment:

1. Verify module is ready for Approved mode of operation by following steps in section 2.4.
2. Establish a connection between the module and a general purpose PC running management tool. The module may be installed in the network prior to initialization. However, a direct network connection is recommended for module initialization and then subsequently deploy the initialized module to the network.

Module Initialization:

A module running in Approved mode of operation is ready to be initialized by the CO to provide the data encryption and decryption service between modules in the enclave. It supports self-initiated cryptographic output capability after being initialized by the crypto officer. Use the management tool to initialize the module.

1. Generate an enclave configuration file, if one is not available. CO is responsible for protecting the enclave configuration file.

   ‘rismtool addkey <enclave file name>’

2. Initialize module using the enclave configuration file and default CO password.

   ‘rismtool init <default IP address> <enclave file name>

   This step will configure the current date and time, update the default CO password and load network key for the enclave.

3. Verify module status led is green indicating module is operational.

An initialized module will automatically enter operational state on subsequent boot based on a valid network key being present and non-default CO password.

11.2 Administrator Guidance

This section is not applicable.

11.3 Non-Administrator Guidance

This section is not applicable.

11.4 Design and Rules

Overall security design:

1. The Module provides role-based authentication with a single distinct operator role: Cryptographic Officer.
2. The Module also has self-initiated cryptographic output capability in order to participate in a secure network enclave with other Modules. Enclave packets are authenticated using AES GCM encryption with pre-shared key on a per packet basis.
3. The Module clears previous role authentications on power cycle, upon a new authentication and after a two-minute timeout.
4. The Module does not support concurrent authenticated operators.
5. An operator does not have access to any cryptographic services prior to assuming an authorized role.
6. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module. Power up self-tests do not require any operator action.
7. Data output are inhibited during key establishment, boot up and self-tests, FW update, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. All SSPs, except as noted in the security policy, are zeroized and the module is restored to factory default state after zeroization. The CO will need to re-initialize the module per section 11.1 and 2.4.
10. The Module does not support a maintenance interface or role.
11. The Module does not support manual SSP establishment methods.
12. The Module does support entering plaintext CSPs. These CSPs and SSPs are initially entered by the CO over an AES-GCM encrypted network link using management tool running on a general purpose computer. This is covered under the “CO Authentication” method in table 21.
13. The Module does not store any plaintext CSPs outside of RAM.
14. The Module does not output intermediate key values.
15. The Module does not provide bypass services or ports/interfaces.

Rules of operation:

The module must be operated in accordance with the following rules.

1. The Module must be initialized and operated in accordance with Verification of Approved Mode of operation and Life-Cycle Assurance sections.
2. Regularly inspect Module for damage and tampering (see Physical Security section).
3. Regularly verify the installed firmware version is approved using the management tool.
4. Only update module firmware with approved versions.
5. Regularly verify the operational status of the module using the management tool and promptly address any error status. Remove module from service if error status is not resolved by a reboot.
6. The module enforces an 8-byte minimum length for CO password. It is recommended to establish a strong CO passphrase policy and change passphrases on a regular basis.
7. The module supports configuration two network keys at a time for seamless key rollover for the data service. It enforces a maximum network key period of one year and will

inhibit data service when no network keys are configured. It is recommended to check and configure a new network key as the active key expires.

8. Use a trusted general purpose PC to run the management tool.
9. Ensure the protection of network key is only entrusted to COs.
10. Zeroize modules when not in operation or returning to manufacturer.

11.5 Maintenance Requirements

Operation:

1. The network key period must not exceed one year. CO must update network key prior to expiration for seamless operation.
2. CO must periodically verify and update module time to compensate for clock drift so that data encryption keys remain synchronized across the secure network enclave.

Firmware Update:

A module running in Approved mode of operation is capable of receiving a firmware update. The CO performs a firmware update when Rajant releases new firmware using the process described in external software/firmware loaded section. See section 6.2 for additional FW loading requirements.

11.6 End of Life

Decommission:

The module must be zeroized prior to decommissioning or re-deployment.

12 Mitigation of Other Attacks

12.1 Attack List

Anti-Replay:

The Module is designed to reject replayed encrypted packets received on the ciphertext interface. Any encrypted packet received on the ciphertext interface that is determined to be replayed is dropped and not forwarded to the plaintext interface. The anti-replay mechanism only applies to encrypted packets on the ciphertext interface.