RAJANT

FIPS 140-3™

SPEC SHEET

Rajant In-line Security Module (RiSM)

Rugged In-line Network Encryption

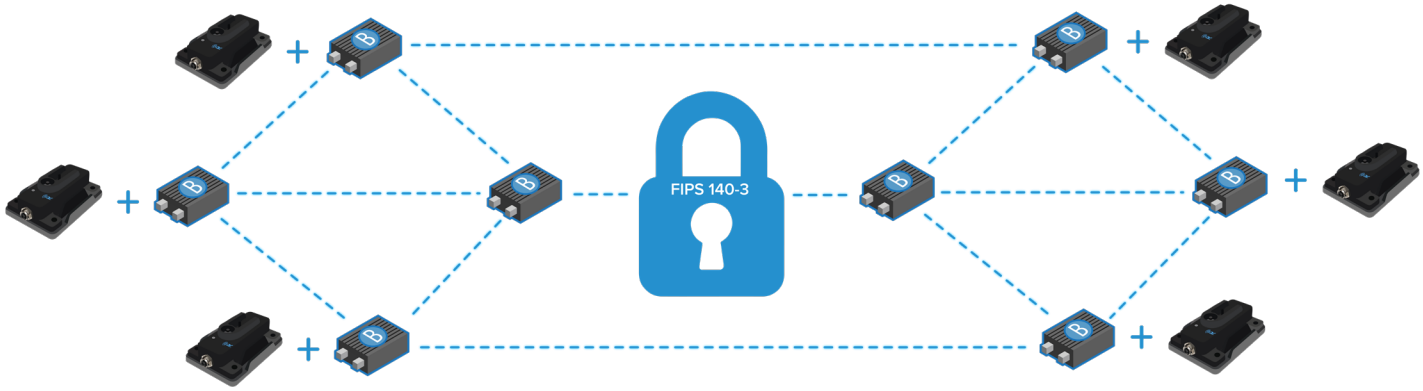
The Rajant RiSM-1SPF is a hardware security module used for in-line network encryption capable of very high data bandwidth and low latency throughput over gigabit Ethernet. **The RiSM product family is based on the Rajant Wolverine Crypto Module, and is FIPS 140-3 Level 2 Validated, Certificate #5110.**

RiSM easily integrates into an existing Rajant Kinetic Mesh® wireless network to meet the stringent NIST FIPS140-3 Level 2 requirements. RiSM also meets the requirements for protecting Sensitive But Unclassified (SBU) and Controlled Unclassified Information (CUI) data.

RiSM is ruggedized for use in extreme environments to secure traffic between a group of similarly-configured RiSMs (secure enclaves). RiSM is a low-power device with Power-over-Ethernet (PoE) passthrough capabilities.

RiSM Key Features

- **High Throughput and Low Latency Traffic Cryptographic Processing:** RiSM uses a programmable data-path processing core that is optimized for 256 AES-GCM encryption/decryption Layer 2 packet processing with low-latency throughput.
- **Power Over Ethernet (PoE) capability:** RiSM is a low-power device with Power-over-Ethernet (PoE) pass-through capabilities. RiSM can be powered via Ethernet interfaces, making RiSM easy to integrate into an existing PoE-enabled network configuration. The PoE pass-through feature allows upstream devices, such as a connected Rajant BreadCrumb® Wireless Node, to be powered from the same PoE source. A PoE splitter device can also be used with RiSM to split power and data for connected devices.
- **Secure Enclaves via Rajant BCⅠCommander®**: A network administrator can use the Rajant BCⅠCommander software to define and remotely apply secure enclave configurations to RiSM devices for initialization and keying.
- **Ruggedized Design**: RiSM has been designed and tested to meet the same extreme industrial-grade environmental requirements as many Rajant BreadCrumb Wireless Nodes, making RiSM devices suitable for installation in nearly any location.
- **Installation and Use**: RiSM only needs to be used at device ingress endpoints where sensitive data encryption is needed, and at network egress points where decryption is needed. All of the mesh nodes between do not require RiSM to pass encrypted traffic.



InstaMesh®

InstaMesh is the advanced, patented[1] protocol developed by Rajant that directs the continuous and instantaneous forwarding of packets from wireless and wired connections. InstaMesh enables complete network mobility, high throughput, and low latency with very low maintenance and administrative requirements. Operating at Layer 2, and not requiring a root node or LAN Controller, InstaMesh provides robust fault tolerance even when there is a connection or node outage. In any network configuration, InstaMesh networking software always determines the most efficient path between any two points, even when those points are in motion.

[1] U.S. Patent 9,001,645

Network & Security	
Secure Design	• Plain Text/Cipher Text traffic processing separation • Tamper evident protections • Passive and Active Zeroize protections • Remote Network Zeroize • Remote Secure Keying • Perfect Forward Secrecy via autonomous key rollover support • Anti-replay flexibility support • Security monitoring features via Rajant BCICommander application
Security Algorithms	• AES 256 GCM/CTR/ECB • KDA [56Cr1] • HMAC-SHA384 • ECDSA 256/384 • AES KEYWRAP/KEYUNWRAP • DRBG [90A] • KAS-ECC [56Ar3] • KDA [56Cr1] • KDF [108]
Security Certifications	RiSM is FIPS 140-3 Level 2 Validated, Certificate #5110. Refer to the following CMVP link for verification and status: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5110.

Input/Output	
Ethernet Interfaces	Rugged (2) M12, X-Code female connector, 10/100/1000 Mbps, IEEE 802.3, auto MDI/MDIX management and monitoring, passive PoE
Max Data Rate	Up to 500Mbps data throughput, 256 AES-GCM encryption/decryption

Field Support	
Device Configuration	The Rajant BC|Commander application provides functions to remotely configure or upgrade RiSM devices in an existing Rajant Kinetic Mesh® wireless network.
Secure Enclave Configuration	The Rajant BC|Commander application provides functions to remotely define and apply Secure Enclave configurations to RiSM devices for initialization and keying.
PoE-enabled Network Configuration	RiSM device configuration functions in the BC|Commander application and PoE-capable interfaces on RiSM devices make it easy to add or upgrade RiSM devices in an existing Rajant Kinetic Mesh® wireless network.

Physical	
Dimensions	152.4mm x 95.3mm x 51mm (6 in x 3.75 in x 2 in)
Weight	624g (22oz)
Temperature	Ambient (operating): -40 °C to +60 °C (-40 °F to 140 °F) Storage: -40 °C to +80 °C (-40 °F to 176 °F)
Enclosure	Fan-less metal enclosure, IP67
Warranty	1 year

Power	
Power Consumption	Average: 8W @ 25C Peak: 11W @ 60C
PoE Input	38 - 60VDC Passive PoE
PoE Pass Through	POE pass through device. See User Guide for system use guidelines.

Tel: 484.595.0233 | **www.rajant.com** |

Updated 02/04/2026

BreadCrumb, InstaMesh, Kinetic Mesh, Living Network, and BC|Commander and their stylized logos are registered trademarks of Rajant Corporation. All other trademarks are the property of their respective owners.
© Copyright 2023 - 2026 Rajant Corporation. All rights reserved.

20+ Years OF GAME-CHANGING WIRELESS

RAJANT
INTELLIGENT EDGE
Enabling Industrial AI