RAJANT

SPEC SHEET

Rajant In-line Security Module (RiSM)

In-line Network Encryption Device

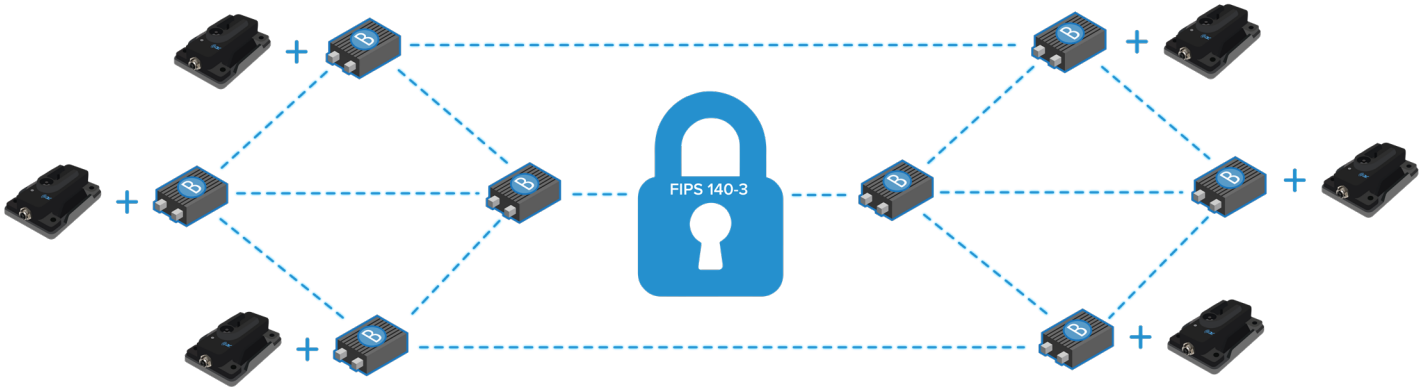
The Rajant RiSM-1SPF is a hardware security module used for in-line network encryption capable of very high data bandwidth and low latency throughput over gigabit Ethernet. **The RiSM product family is based on the Rajant Wolverine Crypto Module which has been designed and proven to pass the most stringent United States Government certification requirements.**

RiSM easily integrates into an existing Rajant Kinetic Mesh® wireless network to meet the stringent NIST FIPS 140-3 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.
- **Secure Enclaves via Rajant BC|Commander®**: A network administrator can use the Rajant BC|Commander 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.



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 Nework 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 currently under test and undergoing final NIST FIPS 140-3 Level 2 certification testing. For the current status of the RiSM certification, on the NIST FIPS 140-3 website, refer to the NIST FIPS 140-3 Implementation Under Test (IUT) reference for the Rajant Inline Security Module (RISM): //https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List

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