RAJANT

RAJANT CRYPTOGRAPHY

RiSM – Rajant's In-line Security Module

The RiSM-1SPF is an in-line network encryption appliance capable of very high data bandwidth and low latency throughput over gigabit Ethernet. **The RiSM product family is based on Rajant's Wolverine Crypto Module which has been designed and proven to pass the most stringent US Government certification requirements.** RiSM is a low-power device with POE pass-through capabilities, making it simple to add to and upgrade an existing Rajant Kinetic Mesh® wireless network to meet NIST FIPS 140-3 requirements. RiSM is ruggedized and may be used in extreme environments to secure traffic between secure enclaves (a group of similarly configured RiSMs).

Key Technology Features

Certifications

- NIST FIPS 140-3 Level 2 (IUT)

Performance

- >500 Mbps Full-Duplex 256 AES-GCM Traffic throughput
- 12 uS end-to-end latency (typical)

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 roll over support
- Anti-Replay flexibility support
- Security monitoring features via BCICommander

Ethernet Interfaces

- Plain Text (POE in) side: M12 10/100/1000 auto MDIX with support for 2 or 4-pair Passive PoE pass-through (up to 90W)
- Cipher Text (POE out) side: M12 10/100/1000 auto MIDX with support 2 or 4-pair Passive PoE pass-through (up to 90W)

Field Support

- Configuration/Support is integrated within Rajant's BCICommander network monitoring and management application.
- Field Debug Logging and Software Upgrade support capable

Algorithms Currently Implemented

- AES 256 GCM/CTR/ECB
- SHA 256/384
- HMAC-SHA384
- ECDSA 256/384
- AES KEYWRAP/KEYUNWRAP
- DRBG [90A]
- KAS-ECC [56Ar3]
- KDA [56Cr1]
- KDF [108]

Size

- 152.4mm x 95.3mm x 51mm (6" x 3.75" x 2")

Temperature

- Ambient (operating) -40°C to 70°C and storage -40°C to 80°C

Power

- 7.5W @ 25C average and 10.5W @ 70C peak

Enclosure Rating

- Fan-less design with metal IP67 rated case

RiSM Technology Advantages

- **FIPS 140-3 Certification:** RiSM is currently under test and undergoing final FIPS 140-3 Level 2 certification testing. Status of RiSM's certification is listed on NIST's FIPS 140-3 website.

  NIST FIPS 140-3 Implementation Under Test reference:

  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/iut-list

- **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 very low latency throughput.
- **Power Over Ethernet (POE):** RiSM is a low-power device and can be powered via either Ethernet interfaces, making it easy to be integrated into an existing POE enabled network configuration. In addition, RiSM provides POE pass-through feature that allows downstream devices that are connected to RiSM, such as a Rajant BreadCrumb® Wireless Node, to be powered from the same POE source.
- **Secure Enclaves via BCICommander:** RISM management support has been integrated into Rajant's easy-to-use BCICommander network monitoring and management application. BCIC allows for Secure Enclave configurations to be defined and then remotely applied to RiSM devices for initialization and keying. With RiSM's BCIC support and POE capable interfaces it is simple to add RISM devices to and upgrade an existing BreadCrumb Kinetic Mesh network to meet NIST's stringent FIPS 140-3 requirements.
- **Ruggedized Design:** RiSM is designed and tested to meet the same industrial grade environmental requirements as many of Rajant's BreadCrumb Wireless Nodes. Thus, making RiSM suitable for nearly any installation location.

Technology Team

RiSM is made possible by Rajant's Information Assurance (IA) team that is comprised of Embedded Security Engineers who have extensive experience in designing secure network devices. The team includes Hardware and Software Engineers, as well as FPGA and System Engineers. Together, they developed cryptographic solutions primarily for US Government and DoD applications. Their custom embedded solutions have been proven to satisfy the most challenging certification requirements.

Tel: 484.595.0233 | www.rajant.com

Updated 3/23/2023

20+ Years OF GAME-CHANGING WIRELESS

RAJANT

*If it's **moving**, it's Rajant.*
*Industrial Wireless Networks **Unleashed.***