Redpine Signals Announces Availability of FIPS 140-2 Certified Wi-Fi Modules for Government and Healthcare Markets

NEWS HIGHLIGHTS

- Industry's only FIPS certified Wi-Fi module with hardware loopback for encryption, offering high data throughput and no requirements on the host
- Cryptographic boundary contained within module
- Support for WPA2 Enterprise security with wide choice of FIPS certified cryptographic algorithms
- Enables systems with full range of processors - including lightweight MCUs - to be FIPS certified

San Jose, CA, March 9, 2016 – Redpine Signals today announced the availability of its Federal Information Processing Standard (FIPS) 140-2 certified Wi-Fi module – the RS9113-N00-D0F device based on the company's M2MCombo™ chipset. Redpine's FIPS 140-2 certified Wi-Fi modules enable system designers and device makers to easily develop products for applications that handle sensitive data in systems employed by Federal Agencies as well as in healthcare, financial services, education and manufacturing areas.

The module is the first in the industry with a completely in-hardware implementation of the AES-CCMP security function used in WPA2, that includes the required loopback features that enable it to be certified FIPS 140-2 compliant and validated by the Cryptographic Module Validation Program (CMVP), a joint effort of the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC).

"FIPS 140-2 validation, apart from being a mandatory requirement of secure systems deployed by Federal agencies, should be viewed as an important benchmark for securing sensitive data throughout the healthcare industry. That is why we have chosen to incorporate Redpine's FIPS certified module in our Wi-Fi-based Infinity M300 patient-worn telemetry monitor," said Lloyd Stern, Vice President of Patient Monitoring Systems Product Management at Draeger Medical Systems.

The RS9113-N00-D0F module is a fully self-contained device with the ability to provide a dual-band 2.4/5 GHz 802.11n Wi-Fi interface in systems with minimal host processing power – including 8-bit microcontrollers. It offers both WPA2-PSK and WPA2-Enterprise security methods, with a host of FIPS certified cryptographic algorithms in the authentication process of the Enterprise Security modes, with its embedded TCP/IP stack supporting IPv4 and IPv6, and SSL connections.

"With our FIPS certified Wi-Fi module, for the first time, developers have the freedom to build a FIPS compliant system without needing to integrate an external supplicant or be restricted to a limited choice of platforms and operating systems," said Venkat Mattela, CEO of Redpine Signals. "We have designed this from the ground-up to address the needs of systems manufacturers in specialized and sensitive areas of the Internet of Things market, taking out the complexity of adding FIPS compliance to embedded systems."

"The NIST Risk Management Framework is one more step in the recognition that cybersecurity has become a huge issue in U.S. federal IT, and that current approaches are no longer adequate to address the complexity and evolution of threats," said Katell Thielemann and Paul E. Proctor, analysts from Gartner, in their report on Best Practices to support the U.S. Federal Government Transition to the Risk Management Framework. FIPS-140-2 is one such standard that helps in protecting sensitive information of Government agencies, Healthcare Companies, or any such companies that needs to protect sensitive information.

By retaining hardware based AES-CCMP encryption for WPA2 modes with the loopback enabled in hardware, the RS9113-N00-D0F module offers high data throughputs equivalent to non-FIPS modes. The module's WPA2 Enterprise Security modes include EAP-TLS, EAP-TTLS, EAP-PEAP with a comprehensive choice of FIPS approved cryptographic algorithms.

The RS9113-N00-D0F module is available in production volumes now. For more information, please visit www.redpinesignals.com.

About Redpine Signals

Headquartered in San Jose, California, Redpine Signals, Inc., is a fabless semiconductor, M2M devices and wireless system solutions company focusing on innovative, ultra-low power and high-performance products for next-generation wireless applications. Redpine was founded in 2001 and was the first in the industry to launch an ultra low power and low-cost single-stream 802.11n chipset in late 2007. Again, in 2009 Redpine pioneered the adoption of self-contained 802.11abgn modules into the then emerging M2M market. In 2013, Redpine introduced the world's first multiprotocol wireless chipset for the Internet of Things market – featuring Wi-Fi, dual-mode BT 4.0, and ZigBee. Redpine has created multiple products based on this chipset including n-Link (hosted), Connect-io-n (embedded) and WiSeConnect (advanced embedded) modules. Redpine offers technology and products covering multiple market segments in the IoT (industrial, medical, automotive, connected home, smart energy, building automation and real-time locationing), mobile and networking markets. Redpine's technology and product portfolio includes chipsets, modules and devices. The company has 220 employees worldwide.

For more information on Redpine products, visit http://www.redpinesignals.com

Press Contact:
PR@redpinesignals.com
+1-408-748-3385