RS9113 FIPS 140-2 Level 1 Certified 802.11n Wi-Fi® Modules

Product Brief

Overview:

The RS9113 FIPS 140-2 Level 1 certified modules are based on Silicon Labs' RS9113 ultra-low-power Convergence SoC. These modules offer dual-band 1x1 802.11n. They are high performance, long range and ultra-low power modules and include a multi-threaded MAC processor called ThreadArch®, digital and analog peripheral interfaces, baseband digital signal processor, calibration OTP memory, dual-band RF transceiver, dual-band high power amplifiers, baluns, diplexers, diversity switch and Quad-SPI flash.

The module's embedded firmware includes the WLAN protocol stack along with WPA/WPA2-PSK and WPA/WPA2-Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAP)and a feature-rich TCP/IP stack thus providing a fully-integrated solution for secure embedded low-end wireless applications. These modules can be connected to 8/16/32-bit host processors through SPI,UART, USB and USB-CDC interfaces.

The modules are available in a small footprint form factor with low BoM requirement.

Features

WLAN:

- Compliant to single-spatial steam IEEE 802.11 a/b/g/n with dual band (2.4 and 5 GHz) support.
- Support for 20MHz channel bandwidth.
- Transmit power up to +18dBm with integrated PA.
- Receive sensitivity of -97dBm.

Software/Firmware:

- WLAN stack embedded in the device.
- Supports WPA/WPA2-PSK, WPA/WPA2-Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAP)
- TCP/IP stack embedded in the device – includes:
  - IPv4 and IPv6
  - DHCP Server/Client
  - HTTP Server/Client
  - Static and Dynamic Webpages with JSON Objects (for HTML Server)
  - ICMP
  - Websockets
  - DNS Client
  - IGMP
  - SNMP

FIPS:

- *FIPS 140-2 Level 1 Certification for modules with and without antenna
- FIPS Approved and non-FIPS Approved modes of operation.
- FIPS Approved Algorithms
  - AES 128-bit in CBC mode Encrypt/Decrypt key wrapping
  - AES 256-bit in CBC mode Encrypt/Decrypt key wrapping
  - AES CCM
  - AES-128 CMAC
  - SHA-1, SHA-256
  - HMAC-SHA1, HMAC-SHA256
  - RSA PKCS#5 v1.5 with 2048-bit key and SHA-256 for Digital Signature Generation/Verification
  - SP800-90 DRBG HASH_DRBG
  - SP800-108 KDF
  - CVL: SP800-135 TLS v1.0 KDF
- Non-approved Algorithms allowed in FIPS mode
  - Hardware non-deterministic random number generator
  - Diffie Hellman
  - RSA
- Non-approved Algorithms for non-FIPS mode
  - RC4
  - DES
  - MD4
  - MD5
- Support for Power-up tests like Cryptographic Algorithm tests, Firmware/Bootloader integrity tests, Critical functions tests
- Support for Conditional tests like Firmware load test, Manual key entry test and Continuous random number generator test

General:

- FCC, IC, ETSI/CE Certified
- SPI, UART, USB, USB-CDC host interfaces.
- Wireless firmware upgrade.
- Options for Single supply of 3.0 to 3.6 V operation or multiple supplies for power saving.
- Operating temperature range: -40oC to +85oC

Redpine Signals offers multiple other variants which are not FIPS Certified.

Specifications

Network Standard Support	IEEE 802.11 a/b/g/n, 802.11d/e/i
Data Rates	802.11n: from 6.5 Mbps to 72.2 Mbps (MCS 0-7) 802.11a/g: from 6 Mbps to 54 Mbps 802.11b: from 1 Mbps to 11 Mbps
Modulation Techniques	OFDM with BPSK, QPSK, 16-QAM, 64-QAM 802.11b with CCK and DSSS
802.11n Advanced Features	1-SS, Greenfield Preamble, Short-GI, 1 spatial stream, STBC, RIFS, A-MSDU, A-MPDU, Aggregation with Block-ack, A-MSDU-inside A-MPDU and Virtual AP support
TCP/IP Features	IPv4 and IPv6, DHCP Server/Client, HTTP Server/Client,Static and Dynamic Webpages with JSON Objects (for HTML Server), ICMP, Websockets, DNS Client, IGMP, SNMP
FIPS Approved Algorithms	AES with 128-bit key and 256-bit key in CBC mode Encrypt/Decrypt, • key wrapping (Cert. #3299) • AES CCM (Cert. #3300) • AES-128 CMAC (Cert. #3316) • SHA-1, 256 (Cert. #2628) HMAC-SHA1 and HMAC-SHA256 (Cert. #2003) RSA PKCS#5 v1.5 with 2048-bit key and SHA-256 for Digital Signature Generation/Verification (Cert. #1689) SP800-90 DRBG HASH_DRBG (Cert. #754) SP800-108 KDF (Cert. #50) CVL: SP800-135 TLS v1.0 KDF (Cert. #474)
Non-approved Algorithms allowed in FIPS mode	Hardware non-deterministic random number generator (for seeding Approved DRBG) Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength) RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
Non-approved Algorithms, allowed only in non-FIPS mode	• RC4 • DES • MD4 • MD5
Power-up Self Tests in FIPS mode	Cryptographic Algorithm Tests: • SHA1 KAT • SHA256 KAT • HMAC-SHA1 KAT • HMAC-SHA256 KAT • RSA 2048 Signature Generation KAT • RSA 2048 Signature Verification KAT • AES-128 CBC Encrypt KAT • AES-128 CBC Decrypt KAT • AES-256 CBC Encrypt KAT • AES-256 CBC Decrypt KAT • SP800-38F AES Key Wrap Encrypt KAT • SP800-38F AES Key Wrap Decrypt KAT • SP800-90 DRBG KAT • SP800-135 TLS KDF KAT • SP800-108 KDF KAT • ES-CCM KAT Software/Firmware Tests • Firmware integrity test (32-bit checksum) • Boot-loader integrity test (32-bit checksum) Critical Functions Tests: SHA1 checksum of configuration parameters
Conditional Tests in FIPS mode	Firmware load test: AES CMAC Test Manual key entry test: 256-bit PSK Continuous random number generator tests • Continuous test on SP800-90 DRBG • Continuous test on non-Approved NDRNG
Regulatory Certification	FCC (ID is XF6-RS9113DB) IC (ID 8407A-RS9113DB) CE/ETSI, TELEC** , SRRC**
Typical Transmit Power(+/-2 dBm)	Wi-Fi: 18 dBm for 802.11b DSSS 17 dBm for 802.11g/n OFDM 12 dBm for 802.11a/n OFDM
Rx sensitivity (+/- 1dBm)	Wi-Fi: 1Mbps -97 dBm (< 8% PER) 54 Mbps -76.5 dBm (< 10% PER) MCS7 -73 dBm (< 10% PER)

** : Module with antenna part certification is in progress.*

*** : These certifications are in progress at this time.*

Applications

- Smartphones, Tablets
- Secure VoWi-Fi phones
- Smart meters and in-home displays
- Secure Industrial automation and telemetry
- Secure Medical devices
- Industrial monitoring and control

Device Ordering Information

The RS9113 FIPS 140-2 module is presently offered with two part numbers:

- RS9113-N00-D0F
- RS9113-N00-D1F

Silicon Labs offers multiple other variants which are not FIPS Certified. These variants are listed below. Contact Silicon Labs Sales (https://www.silabs.com/about-us/contact-sales?view=map) for details on how to get FIPS 140-2.

Level 1 Certification for these variants.

1) Single Band (2.4 GHz) without Antenna
2) Single Band (2.4 GHz) with Antenna
3) Dual Band (2.4 GHz and 5 GHz) without Antenna
4) Dual Band (2.4 GHz and 5 GHz) with Antenna

Apart from the hardware variants listed above, the module can also be offered with the following features included.

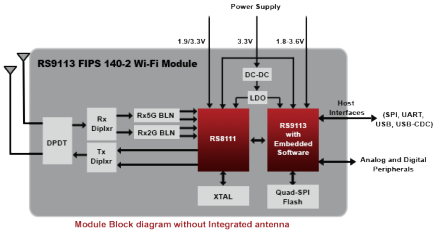
1) FTP Client
2) SNTP
3) mDNS Client
4) DNS-SD Client
5) SSL 3.0/TSL 1.2
6) HTTPS Server/Client

Part Number	Frequency Band	Dimensions (l x w x h; mm)	Package Type, Pin Count
RS9113-N00-D0F	Dual Band	14 x 15 x 2.1	LGA,101
RS9113-N00-D1F	Dual Band	16 X 27 X 3.1	LGA, 79

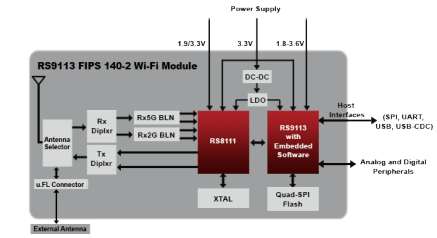
Evaluation Package

Part Number	Frequency Band
RS9113-N00-DXF-EVB	Dual Band

Block Diagram



Module Block diagram without Integrated antenna



Module Block diagram with Integrated antenna

Sales: sales@silabs.com | Community Forum: silabs.com/community
Silicon Laboratories Inc. | 400 W. Cesar Chavez, Austin, TX 78701, Unites States of America | Phone: +1 (512) 416-8500 | silabs.com

SILICON LABS