



January 24, 2017

To Whom It May Concern:

CGI verified that the following software version faithfully embeds a FIPS 140-2 validated cryptographic module:

- 8.3

The software is known to operate on the following platforms:

- Cisco 2504, 5520, 8510 and 8540 Wireless LAN Controllers

During the course of the review, it was confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product:

- Cisco FIPS Object Module Version: 6.0, FIPS 140-2 certificate #2505

CGI confirmed that the following features leverage the embedded module to provide cryptographic services:

Encryption/Hashing/Key Derivation associated with the following services:

- 802.11
- IPsec
- RADIUS
- SSH
- SNMPv3
- TACACS+
- TLS/DTLS

Diffie-Hellman and Asymmetric Encryption associated with the following services:

- IPsec
- SSH

Additionally, CGI confirmed that the above referenced cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of CGI and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Marc Boire'.

Marc Boire
Laboratory Manager,
CGI IT Security Evaluation and Test Facility