

October 29, 2015

To Whom It May Concern:

Acumen Security verified that the following product faithfully embeds a FIPS 140-2 validated cryptographic module,

- Cisco Secure Access Control Server, version 5.8.

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product,

- Cisco FIPS Object Module (version 4.1), cert #2100,

Acumen Security confirmed that the following features leverage the **Cisco FIPS Object Module** to provide cryptographic services, **SSH, TLS, Radius Key Wrap, 802.1X Authentication with PEAP and EAP_TLS**, and **Online Certificate Status Protocol (OCSP)**.

The above referenced modules provide all of the cryptographic functionality for each of the services listed above, including:

1. Session establishment supporting each service,
2. All underlying cryptographic algorithms supporting each services' key derivation functions,
3. Hashing for each service,
4. Symmetric encryption for each service.

Additionally, Acumen Security 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 Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,



Ashit Vora
Laboratory Director