20, August 2014

To Whom It May Concern

Cisco completed its conformance review of Cisco Systems Inc.'s 8800 Series IP Phones, software version 10.2.2 on August 20, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

    1.   Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643)

Specifically, Cisco's review confirmed that:

1. The integrated cryptographic module (mentioned above) is initialized in a manner that is compliant with its individual security policies.

2. All cryptographic algorithms used in TLSv1 for session establishment, encryption, and authentication are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643).

3. All cryptographic algorithms used in Secure Storage for encryption and authentication are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643).

4. The cryptographic algorithm used for RSA Signature Verification for authentication using RSA verification is offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643).

5. All cryptographic algorithms used for File Authentication and Encryption for encryption and authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #1643).

6. All cryptographic algorithms used for sRTP for session establishment, traffic encryption and traffic authentication are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643).

7. All cryptographic algorithms used for Image Authentication for image authentication are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643)

8. All cryptographic algorithms used for EnergyWise for the power saving functionality are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643)

9. All cryptographic algorithms used for Secure Boot for image resilience are offloaded to Cisco Common Crypto Module (C3M) (FIPS 140-2 Cert. #1643)

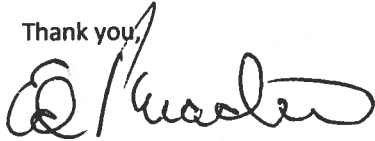10. The Product will not operate if the integrated FIPS module (mentioned above) is missing or altered

The Product will not operate if the integrated FIPS module (mentioned above) is missing or altered. Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

Moreover, the FIPS conformance claims made for 8800 series IP Phones software version 10.2.1, verified by Leidos, hold true for Cisco 8800 IP Phones, software version 10.2.2 with no additions or removal of cryptographic services or cryptographic implementations.

The intention of this letter is to provide our assessment that the Product correctly integrates and uses validated cryptographic modules within the scope of the claims indicated above. Cisco offers no warranties or guarantees with respect to the above described conformance review. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Cisco's analysis, testing or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
VP Engineering
Cisco TRIAD