



Cisco Systems, Inc.  
7025 Kit Creek Road  
P.O. Box 14987  
Research Triangle Park  
NC 27709  
Phone: 919 392-2000  
<http://www.cisco.com>

March 27, 2014

To Whom It May Concern

Cisco completed its conformance review of the Cisco Catalyst 4948E and Catalyst 4948E-F (Version: 15.2(1)E) ("the Product") on February 13, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

Cisco IC2M Rel1v1.0.2 (FIPS 140-2 Cert. #1940)

Specifically, Cisco's review confirmed that:

1. The integrated cryptographic module (mentioned above) is initialized in a manner that is compliant with the FIPS Security Policy.
2. All cryptographic algorithms used for session establishment of SSH v2, TLS, and IKE/IPsec, are offloaded to Cisco IC2M Rel1v1.0.2 (FIPS 140-2 Cert. #1940).
3. Bulk data encryption for the established SSH, TLS, and IKE/IPsec secure connections is offloaded to Cisco IC2M Rel1v1.0.2 (FIPS 140-2 Cert. #1940).

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 the Cat 4500E series, verified by SAIC during the separate FIPS validation (certificate issued 3/26/14), hold true for the Cat 4900E/E-F series 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](mailto:certteam@cisco.com)).

Thank you,

Ed Paradise  
VP Engineering  
Cisco TRIAD