CISCO

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

December 15, 2015

To Whom It May Concern

Cisco completed its conformance review of Mobility Services Engine (MSE) (Version: 8.0.130.0)("the Product") on December 4, 2015, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules per its posted Security Policy:

1.   CiscoSSL FIPS Object Module (FOM) (FIPS 140-2 Cert. #2100)

Specifically, Cisco's review confirmed that:

1.   The CiscoSSL FIPS Object Module (FOM) is initialized in a manner that is compliant with the FOM FIPS security policy.
2.   All algorithms used for TLS and session establishment are offloaded to CiscoSSL FOM - Cert. #2100
3.   All cryptographic algorithms used for SNMPv3 secure connection are offloaded to CiscoSSL FOM

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 MSE 8.0, verified by Leidos Accredited Testing & Evaluation (AT&E) Labs NVLAP Lab code 200427-0, holds true for MSE 8.0.130.0 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 STO