



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

18, June 2015

To Whom It May Concern

Cisco completed its conformance review of Cisco Systems Inc.'s Cisco Unified Communication Manager (CUCM) with Prime License Manager (PLM), software version 10.5 on June 11, 2015, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (version 4.1), cert #2100
2. RSA BSAFE® Crypto-J JSAFE and JCE Software Module 5.0.1, cert #1502
3. Red Hat Enterprise Linux 6.2 Openswan Cryptographic Module cert #1859
4. Red Hat Enterprise Linux 6.2 OpenSSH Server Cryptographic Module cert #1792

Specifically, Cisco's review confirmed that:

Cisco confirmed that the following features leverage the **Cisco FIPS Object Module** to provide cryptographic services used for, **Call Processing (TLS)**, **CA Services (TLS)**, and **Certificate Trust Lists (TLS)**.

Cisco confirmed that the following features leverage the **Crypto-J JSAFE and JCE Software Module** to provide cryptographic services used for, **HTTPs**, **LDAP over SSL**, **SFTP**, **PLM Agent Interaction Client**, **PLM Swift Interaction Client**, and **Certificate Management**.

Cisco confirmed that the following features leverage the **Openswan Cryptographic Module** to provide cryptographic services used for, **IKEv1**, **IKEv2**, and **IPsec**.

Cisco confirmed that the following feature leverages the **OpenSSH Server** to provide cryptographic services used for, **SSH**.

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

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

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

Moreover, the FIPS conformance claims made for Cisco Unified Communication Manager (CUCM) with Prime License Manager (PLM), version 10.5.1, verified by Leidos, hold true for Cisco Unified Communication Manager (CUCM) with Prime License Manager (PLM), version 10.5.2 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 Security & Trust Organization (STO) Engineering