



June 13, 2013

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

To Whom It May Concern:

SAIC completed its conformance review of the Cisco Systems, Inc.'s **Cisco Unity Connection v 8.6.1** (the "Product") on June 6, 2013; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Red Hat Enterprise Linux 5 OpenSSL Cryptographic Module version 1.1 (FIPS 140-2 Cert. #1320)
2. RSA BSAFE Crypto-J Software Module version 4.1 (FIPS 140-2 Cert. #1291)
3. Red Hat Enterprise Linux 5 Libgcrypt Cryptographic Module version 1.0 (FIPS 140-2 Cert. #1305)

Specifically, SAIC's review confirmed that:

1. Each of the integrated cryptographic modules (mentioned above) are initialized in a manner that is compliant with their individual security policies.
2. All cryptographic algorithms used in TLSv1/HTTPS used for session establishment and bulk data encryption, are offloaded to Red Hat Enterprise Linux 5 OpenSSL Cryptographic Module version 1.1 (FIPS 140-2 Cert. #1320).
3. All cryptographic algorithms used in TLSv1 for session establishment of voice calls, are offloaded to RSA BSAFE Crypto-J Software Module version 4.1 (FIPS 140-2 Cert. #1291).
4. All cryptographic algorithms used in sRTP for SIP packet authentication, are offloaded to the Red Hat Enterprise Linux 5 OpenSSL Cryptographic Module version 1.1 (FIPS 140-2 Cert. #1320).
5. All cryptographic algorithms used in sRTP for SIP packet encryption, are offloaded to the Red Hat Enterprise Linux 5 Libgcrypt Cryptographic Module version 1.0 (FIPS 140-2 Cert. #1305).
6. The FIPS module Red Hat Enterprise Linux 5 OpenSSL Cryptographic Module version 1.1 (FIPS 140-2 Cert. #1320) was verified by checking Call Manager version 8.6.1a, which is a previously reviewed Product for compliance. However, in this release of the Unity Connection product, SAIC has determined that the Call Manager version used was 8.6.1.1.20009-3. SAIC reviewed the source code this version of Call Manager and successfully verified that there are no cryptographic differences between this version and the compliant 8.6.1a version.
7. The Product's services listed above will not operate if any of the integrated FIPS validated modules (mentioned above) are missing or altered.

Details of SAIC's review, which consisted of source code review and operational testing, are obtainable by special request.

Please note that for this review, SAIC only examined the Product features referenced above and while the Product may contain other features or functionality, SAIC did not examine these during its review and makes no claims or representations regarding them. Furthermore, the Cryptographic Module Validation

Science Applications International Corporation

Franklin Center | 6841 Benjamin Franklin Drive | Columbia, MD 21046 | tel: 443.367.7322 | fax: 443.367.7948 | saic.com



Program (CMVP) has not independently reviewed SAIC's analysis, testing, or results.

The intention of this letter is to provide independent opinion that the Product correctly integrates and uses validated cryptographic modules within the scope of claims indicated above. SAIC offers no warranties or guarantees with respect to the above described compliance review. This letter does not imply an SAIC certification or product endorsement.

Please let us know if you have any questions.

Sincerely,

A handwritten signature in black ink that reads "DMSniegowski". The signature is written in a cursive, somewhat stylized script.

Daun-Marie Sniegowski
Laboratory Director