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

July 2, 2014

To Whom It May Concern

Cisco completed its conformance review of Cisco Tandberg TC software (Version:7.2)("the Product") on July 2, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

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

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 policy.
2. All cryptographic algorithms used for TLS used in HTTPs and SIP for session establishment, traffic encryption, and traffic authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2100). The product is able to load certificates that have a key size less than 2048 bits, however this is not allowed while in FIPS mode.
3. All cryptographic algorithms used for SSHv2 for session establishment, traffic encryption, and traffic authentication are offloaded to Cisco FIPS Object Module (FOM) (FIPS 140-2 Cert. #2100)
4. All cryptographic algorithms used for H.235 Media stream security for traffic encryption are offloaded to Cisco FIPS object module (FOM) (FIPS 140-2 Cert. #2100). The product also supports the use of 1024 bit Diffie-Hellman, however any key sizes less that 2048 bits shall not be used with the product in a FIPS conformant manner
5. All cryptographic algorithms used for sRTP for session establishment, traffic encryption, and traffic authentication are offloaded to Cisco FIPS object module (FOM) (FIPS 140-2 Cert. #2100)
6. The product will not operate if the integrated module (listed above) is missing or altered.

The FIPS conformance claims made for Cisco Tandberg TC 7.1.3, verified by Leidos (19 May, 2014), continue to hold true for Cisco Tandberg TC 7.2 with the addition of a new web server and support for remote pairing touch 10 using TLS made in version 7.2.

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

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