SAIC®
From Science to Solutions

September 12, 2012

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 AnyConnect Secure Mobility Client (Version: 3.1)** (the "Product") on September 4-6, 2012; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Microsoft Windows XP Enhanced Cryptographic Provider (RSAENH) (FIPS 140-2 Cert. #989)
2. Microsoft Windows XP Enhanced Cryptographic Provider (FIPS 140-2 Cert. #989)
3. Microsoft Windows Vista Cryptographic Primitives Library (FIPS 140-2 Cert. #1001)
4. Microsoft Windows Vista Enhanced Cryptographic Provider (FIPS 140-2 Cert. #1002)
5. Microsoft Windows 7 Cryptographic Primitives Library (FIPS 140-2 Cert. #1329)
6. Microsoft Windows 7 Enhanced Cryptographic Provider (RSAENH) (FIPS 140-2 Cert. #1330)
7. Microsoft Windows 7 Kernel Mode Cryptographic Primitives Library (FIPS 140-2 Cert. #1328)
8. Apple FIPS Cryptographic Module (FIPS 140-2 Cert. #1514)
9. Cisco SSL (C3M) (FIPS 140-2 Cert. #1643)
10. Network Security Services (NSS) Cryptographic Module (FIPS 140-2 Cert. #815)
11. 3e Cryptographic Kernel Library (FIPS 140-2 Cert. #874)

The AnyConnect Secure Mobility client was tested on the following operating systems:

Operating System	Version
Windows	Windows 7 x86(32-bit) and x64(64-bit)
	Windows Vista x86(32-bit) and x64(64-bit)
	Windows XP SP3 x86(32-bit) and x64(64-bit)
Mac	Mac OS X 10.8 x86(32-bit) and x64(64-bit)
	Mac OS X 10.7 x86(32-bit) and x64(64-bit)
	Mac OS X 10.6 x86(32-bit) and x64(64-bit)
Linux	Red Hat 6 (32-bit)
	Red Hat 6 (64-bit)
	Ubuntu 11.10 (32-bit)
	Ubuntu 11.10 (64-bit)

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 services used for HTTPs connections on Windows XP, Windows Vista and Windows 7 are offloaded to Windows XP Enhanced Cryptographic Provider, Microsoft Windows Vista Cryptographic Primitives Library or Microsoft Windows 7 Cryptographic Primitives Library,

respectively.

3. All cryptographic algorithms used for HTTPs connections on Red Hat Enterprise Linux v6, Ubuntu 11.10, and Mac OS X 10.6/10.7/10.8 are offloaded to the CiscoSSL FIPS 140-2 validated FIPS canister (C3M)
4. Bulk data encryption (via TLS and IPsec/IKEv2) for the established VPN connection uses CiscoSSL FIPS Object Module (C3M) on all platforms tested
5. MACsec key agreement is accomplished using CiscoSSL FIPS Object Module (C3M) on Windows XP, Windows Vista, Windows 7
6. MACsec traffic encryption is accomplished via the Windows Cryptographic primitives library in Windows 7
7. AnyConnect Network Access Manager (NAM) 802.1x and 801.11i key derivation and handshake make use of the CiscoSSL FIPS Object Module (C3M) on Windows XP, Windows Vista, Windows 7
8. AnyConnect Network Access Manager (NAM) 802.11i Traffic Encryption is performed by the 3e Cryptographic Kernel Library on Windows XP SP3 only

Details of SAIC's review, which consisted of source code review and operational testing, can be found in the attached test plan.

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 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,

DM Sniegowski

Daun-Marie Sniegowski
Laboratory Director