Cisco Secure Services Client FIPS Module Version 1.0.0.0 Security Policy

August 8, 2008

Contents

This security policy contains these sections:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Module Overview

The Cisco Secure Services Client (Cisco SSC) FIPS Module is a software-only, multi-chip standalone cryptographic module that runs on a general purpose PC. The primary purpose of this FIPS 140-2 Level 1 validated module is to provide cryptographic services for 802.1X (Layer 2) user and device authentication for access to both wired and wireless networks. It entails providing cryptographic support for EAP protocols such as EAP-TLS, EAP-FAST and PEAP. It also provides cryptographic support for IEEE 802.11i key-exchange handshake that is based on 802.1X or WPA2 (Wi-Fi Protected Access 2) Pre-shared keys.

The physical boundary of the module is the case of the PC (Figure 1). The logical boundary of the module is the single cryptographic module dynamic link library (crypt.dll). A high level architecture of the Cisco Secure Services Client, including the cryptographic boundary, is shown in Figure 2.

The cryptographic module runs on the following operating systems:

- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows 2003 Server (not included in FIPS 140-2 Operational Testing)

Figure 1 PC Hardware Diagram that contains Cisco Secure Services Client

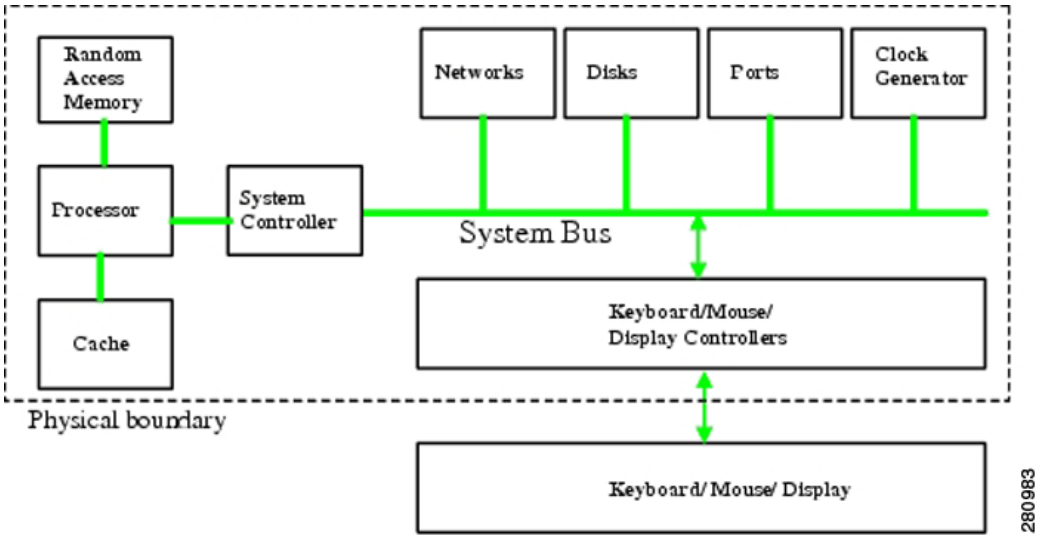
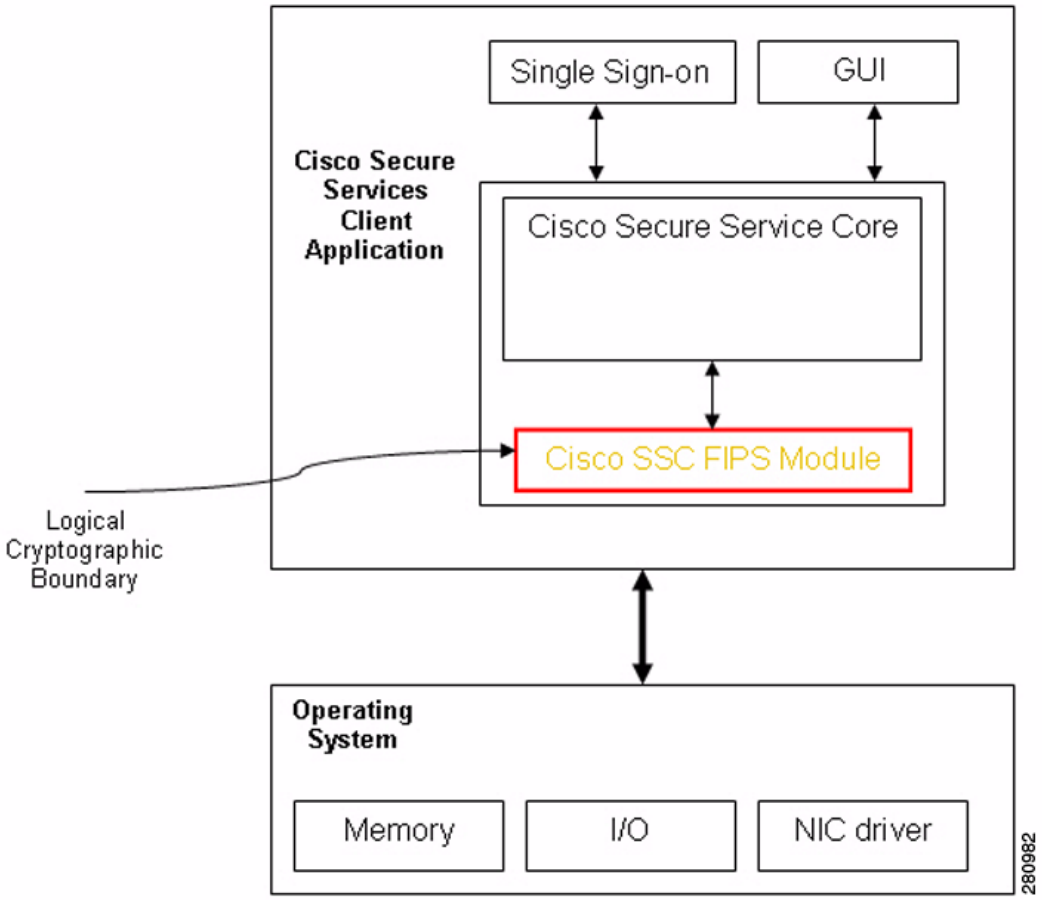


Figure 2 High-Level Architecture of the Cisco Secure Services Client



Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2 (as shown in Table 1).

Table 1 Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1

Table 1 Module Security Level Specification (continued)

Security Requirements Section	Level
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Modes of Operation

Approved Mode of Operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- RSA with 1024, 1536, 2048, 3072, 4096 bit keys for digital signature generation and verification (Cert. #325)
- AES CBC mode with 128, 192, 256 bit keys for encryption and decryption (Cert. #699)
- HMAC-SHA1 for keyed hashing (Cert. #377)
- SHA1 for hashing (Cert. #727)
- Triple-DES TECB mode (2-key) for use in ANSI X9.31 DRNG only (Cert. #630)
- ANSI X9.31 A.2.4 Deterministic Random Number Generator (Cert. #410)

In the FIPS Approved mode of operation, the cryptographic module supports the following FIPS allowed algorithms:

- AES (Cert. #699; key wrapping; key establishment methodology provides 128 bits of encryption strength).
- Diffie-Hellman

The Cisco Secure Services Client FIPS Module provides underlying functions to support the commercially available TLS protocol. TLS is implemented outside of the logical cryptographic boundary. The module provides services that implement the Diffie-Hellman primitives required for TLS.

The cryptographic module may be configured for FIPS mode by performing the "fipsInit" configuration step. The return status of FIPS_OK by fipsInit indicates that the mode was set successfully. Based on the return status value of fipsInit, a message is logged by Cisco Secure Services Client.

FIPS module initialization failure string format in the log is:

```
"FIPS module error code: "
```

FIPS module initialization success string format in the log is:

```
"Successfully initialized FIPS module"
```

Non-FIPS Mode of Operation

In non-FIPS mode, the cryptographic module provides non-FIPS Approved algorithms as follows:

- RC4 for encryption and decryption
- DES for encryption and decryption
- MD4 for hashing
- MD5 for hashing
- HMAC-MD5
- DSA implementation for legacy use; algorithm not tested (non-compliant)

Ports and Interfaces

The physical ports of the module are provided by the general purpose computer on which the module is installed. All FIPS ports and interfaces are defined as the API of the cryptographic module. The API contains all data input, data output, control input, and status output interfaces to and from the module.

Identification and Authentication Policy

Assumption of roles

The Cisco Secure Services Client FIPS Module supports two distinct operator roles (User and Cryptographic Officer). The module does not provide any identification or authentication means of its own. The Cryptographic Officer and the User roles are implicitly assumed based on the service requested.

Table 2 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
Cryptographic Officer	N/A	N/A

Table 3 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

Access Control Policy

Roles and Services

The Cisco Secure Services Client FIPS Module supports the authorized services described in Table 4.

Table 4 Services Authorized for Roles

Role	Authorized Services
User:	• AES Encryption: Encrypt data passed into the module • AES Decryption: Decrypt data passed into the module • AES Key Unwrap: Unwrap an AES key • Generate Random Number: Generates a random number using ANSI X9.31 A.2.4 DRNG • DH Key Generation: Generate DH Components using ANSI X9.31 A.2.4 DRNG • DH Compute Key: Perform the DH modular exponentiation to compute the Shared Secret. • RSA Sign: Digitally sign data with RSA. • RSA Verify: Verify digitally signed data with RSA. • HMAC-SHA1: Provide keyed hashing function • SHA1: Provide hashing function • Helper Services: Provide help information for the various services • Show Status: API function call response
Cryptographic Officer:	• Zeroize: Actively destroy all plaintext Critical Security Parameters (CSPs) • Show Status: API function call response

Other Services

The Cisco Secure Services Client FIPS Module supports the following services that do not require an operator to assume an authorized role:

- Self-tests: This service executes the suite of power-up self-tests required by FIPS 140-2 and is invoked by reloading the library.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services.

Table 5 CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation		
C.O.	User				
	x	AES Encryption	AES Key	Use	Destroy
	x	AES Decryption	AES Key	Use	Destroy
	x	AES Key Unwrap	AES KEK	Use	Destroy
			AES Key	Write	
	x	Generate random number	DRNG Seed Key	Use	Destroy
			DRNG Seed	Use	Destroy
	x	DH Key Generation	DH Private Component	Generate	Destroy
			DH Public Component	Generate	
	x	DH Compute Key	DH Private Component	Use	Destroy
			DH Public Component	Use	
			Shared Secret	Compute	
	x	RSA Sign	RSA Private Key	Use	Destroy
	x	RSA Verify	RSA Public Key	Use	
	x	HMAC-SHA1	HMAC Key	Use	Destroy
	x	SHA1	No access to CSPs		
	x	Helper Services	No access to CSPs		
x		Zeroize	Destroy all plaintext CSPs		
x	x	Show Status	No access to CSPs		

Cryptographic Key Management

Key Generation

The Cisco Secure Services Client FIPS module generates keys using the ANSI X9.31 FIPS Approved random number generator.

Key Transport

The AES key may enter the module AES wrapped with the AES KEK.

Key Storage

All keys and CSPs used by the module are stored as plaintext in volatile RAM only. No keys or CSPs are persistently stored within the module.

Key Destruction

All keys (except public keys) and CSPs are zeroized and freed once no longer needed. Keys and CSPs may also be destroyed by the zeroize service.

Table 6 Cryptographic Keys and Critical Security Parameters

Name	Description/Usage	Generation	Entry/Output
AES Key	128-256 bit key used during AES encryption and decryption	Generated externally	Entry: Plaintext entry from within the physical boundary; may also enter AES wrapped with AES KEK Output: Never output
AES Key Encryption Key (KEK)	128-bit key used to unwrap the AES Key	Generated externally	Entry: Plaintext entry from within the physical boundary Output: Never output
RSA private key	1024-4096 bit RSA key for signature generation	Generated externally	Entry: Plaintext entry from within the physical boundary Output: Never output
HMAC Key	Used during HMAC-SHA1 service	Generated externally	Entry: Plaintext entry from within the physical boundary Output: Never output
DRNG Seed Key	Used to seed the ANSI X9.31 DRNG	Generated externally	Entry: Plaintext entry from within the physical boundary Output: Never output

Table 6 Cryptographic Keys and Critical Security Parameters (continued)

Name	Description/Usage	Generation	Entry/Output
DRNG Seed	Used to seed the ANSI X9.31 DRNG	Generated externally	Entry: Plaintext entry from within the physical boundary Output: Never output
Diffie-Hellman Private Component	Used only to support external DH-based protocols	Generated internally using the ANSI X9.31 DRNG	Entry: Never entered Output: Never output from the physical boundary
Shared Secret	Used only to support external DH-based protocols	Computed internally via DH scheme	Entry: Never entered Output: Never output from the physical boundary

Table 7 Public Keys

Name	Description/Usage	Generation	Entry/Output
RSA public key	1024-4096 bit RSA key for signature verification	Generated externally	Entry: Plaintext entry within the physical boundary Output: Never output
Diffie-Hellman Public Component	Used only to support external DH-based protocols	Generated internally using the ANSI X9.31 DRNG	Entry: Plaintext entry; receive Host Public Component during DH exchange Output: Plaintext output; transmit Client Public Component during DH exchange

Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are applicable because the example device operates in a modifiable operational environment. The following Operational Environments are supported:

- Microsoft Windows XP (single-user mode)
- Microsoft Windows 2000 (single-user mode)
- Microsoft Windows 2003 Server (not included in FIPS 140-2 Operational Testing)

Security Rules

The Cisco Secure Services Client FIPS Module's design corresponds to the module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic Officer role.

2. The cryptographic module does not provide any operator authentication.

3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

4. The cryptographic module shall encrypt/decrypt message traffic using the AES algorithm.

5. In the FIPS Approved mode of operations, the operator may not use any of the following algorithms: RC4, DES, MD4, MD5, HMAC-MD5, and DSA (DSA has not been tested for FIPS use; non-compliant).

6. The cryptographic module shall perform the following tests:

Power up Self-Tests:

1. Cryptographic algorithm tests:
   a. RSA Sign/Verify Known Answer Test
   b. AES Encrypt/Decrypt Known Answer Test
   c. HMAC-SHA1 Known Answer Test
   d. SHA1 Known Answer Test
   e. Triple-DES Encrypt Known Answer Test
   f. ANSI X9.31 A.2.4 DRNG Known Answer Test
2. Software Integrity Test: HMAC-SHA1
3. Critical Functions Tests: None

Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test - performed on ANSI X9.31 A.2.4 DRNG

7. At any time, the operator shall be capable of commanding the module to perform the power-up self-test by reloading the cryptographic module into memory.

8. The cryptographic module is available to perform services only after successfully completing the power-up self-tests.

9. Prior to each use, the internal RNGs shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.

10. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.

11. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

12. The module shall not support concurrent operators.

13. The module shall not support a bypass capability.

14. The module shall not support a maintenance mode.

15. The module shall be run on a supported operating system configured in "single user" mode.

Physical Security

The FIPS 140-2 Area 5 Physical Security requirements are not applicable because the Cisco Secure Services Client FIPS Module is a software-only module.

Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Definitions and Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Program Interface
CBC	Cipher-block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DLL	Dynamic Link Library
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code

IEEE	Institute of Electrical and Electronics Engineers
KAT	Known Answer Test
MD4	Message Digest Algorithm 4
MD5	Message Digest Algorithm 5
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
PC	Personal Computer
PEAP	Protected Extensible Authentication Protocol
RAM	Random Access Memory
RC4	Rivest Cipher 4
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Secure Hash Algorithm
SSC	Secure Services Client
TDES	Triple-DES
TECB	Triple-DES Electronic Codebook
TLS	Transport Layer Security
WPA2	Wi-Fi Protected Access 2

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.