



Cisco Network Convergence System 1004 Cryptographic Module

**FIPS 140-2 Non-Proprietary Security Policy
Level 2 Validation**

Version 0.4

December 10, 2020

Table of Contents

CISCO NETWORK CONVERGENCE SYSTEM 1004 CRYPTOGRAPHIC MODULE ...	1
1 INTRODUCTION.....	3
1.1 PURPOSE.....	3
1.2 MODULE VALIDATION LEVEL	3
1.3 REFERENCES.....	3
1.4 TERMINOLOGY	4
1.5 DOCUMENT ORGANIZATION	4
2 CISCO NETWORK CONVERGENCE SYSTEM 1004 MODULE.....	5
2.1 VALIDATED CONFIGURATION	5
2.2 CRYPTOGRAPHIC BOUNDARY	6
2.3 MODULE INTERFACES.....	6
2.4 1004 FRONT AND REAR PANELS	7
3. ROLES, SERVICES, AND AUTHENTICATION	9
3.1 USER SERVICES	9
3.2 CRYPTO OFFICER SERVICES.....	10
3.3 NON-FIPS MODE SERVICES	11
3.4 UNAUTHENTICATED SERVICES	11
4. CRYPTOGRAPHIC KEY/CSP MANAGEMENT.....	12
5. CRYPTOGRAPHIC ALGORITHMS.....	16
5.1 APPROVED CRYPTOGRAPHIC ALGORITHMS	16
5.2 NON-FIPS APPROVED ALGORITHMS ALLOWED IN FIPS MODE	17
5.3 NON-APPROVED CRYPTOGRAPHIC ALGORITHMS	17
6. SELF-TESTS	17
6.1 POWER ON SELF-TESTS	17
6.2 CONDITIONAL TESTS	18
7. PHYSICAL SECURITY.....	18
7.1 TAMPER EVIDENCE LABEL (TEL) PLACEMENT.....	18
8. SECURE OPERATION	21
8.1 INITIAL SETUP	21

1 Introduction

1.1 Purpose

This is the non-proprietary cryptographic module security policy for the Cisco Network Convergence System 1004 Cryptographic Module running with firmware version IOS XR 7.0.1. This security policy describes how this module meets the security requirements of FIPS 140-2 Level 2 and how to run the module in a FIPS 140-2 mode of operation. This Security Policy may be freely distributed.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <https://csrc.nist.gov/Projects/cryptographic-module-validation-program>.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	2

Table 1 Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Network Convergence System 1004 Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2 IG and additional rules imposed by Cisco Systems, Inc. More information is available on the module from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following website:

<http://www.cisco.com/c/en/us/products/index.html>

<https://www.cisco.com/c/en/us/support/optical-networking/network-convergence-system-1004/model.html>

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Network Convergence System 1004 Cryptographic Module is referred to as NCS1K, NCS 1004, Cryptographic Module, CM, Module, Appliances or Systems.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This document provides an overview of the Cisco Network Convergence System 1004 Cryptographic Module s identified above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco Network Convergence System 1004 Module

The module uses state of the art silicon along with complete automation and real-time visibility to deliver a universal transponder solution that provides best-in-class performance for metro, long-haul and submarine applications while being simple to deploy and manage.

The module is mechanically optimized to maximize capacity at minimum space and power footprint. At 2RU, the system supports up to 4.8Tbps of client and 4.8Tbps of trunk traffic. The NCS 1004 will double capacity provided to the user compared to the other device, e.g., NCS 1002.



Figure 1: Cisco NCS 1004

2.1 Validated configuration

The validated platform consists of the following components and configurations:

- Chassis:
 - NCS1004=
- Controller Card:
 - NCS1K4-CNTRLR-K9=
- Network Interface Card(s)
 - NCS1K4-1.2T-K9
 - NCS1K4-1.2T-L-K9
- FIPS Kit:
 - AIR-AP-FIPSKIT=

The switch can be configured as follows while in the FIPS mode.

Chassis	Controller Card	Network Interface Cards
NCS1004=	NCS1K4-CNTRLR-K9=	<ul style="list-style-type: none">• NCS1K4-1.2T-K9• NCS1K4-1.2T-L-K9

Figure 2: Module Configurations

2.2 Cryptographic Boundary

The module is a hardware, multi-chip standalone crypto module. The cryptographic boundary is defined as encompassing the "top," "front," "left," "right," "rear" and "bottom" surfaces of the case. All of the functionality described in this publication is provided by components within this cryptographic boundary. The module consists of a production grade enclosure as well as components. The detailed configuration can be seen in Figure 2 above.

2.3 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input and status output. The module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following table:

Physical Interfaces	FIPS 140-2 Logical Interfaces
Network Interface Card <ul style="list-style-type: none"> • 12 QSFP28 Ports • 8 DWDM Line/Trunk Ports Controller Card <ul style="list-style-type: none"> • 2 RJ45 Management port • 1 SFP Management port • 1 Console Port 	Data Input Interface
Network Interface Card <ul style="list-style-type: none"> • 12 QSFP28 Ports • 8 DWDM Line/Trunk Ports Controller Card <ul style="list-style-type: none"> • 2 RJ45 Management port • 1 SFP Management port • 1 Console Port 	Data Output Interface
Controller Card <ul style="list-style-type: none"> • 2 RJ45 Management port • 1 SFP Management port • 1 Console Port 	Control Input Interface
Network Interface Card <ul style="list-style-type: none"> • 12 QSFP28 Ports • 8 DWDM Line/Trunk Ports Controller Card <ul style="list-style-type: none"> • 2 RJ45 Management port • 1 SFP Management port • 1 Console Port LEDs	Status Output Interface

Table 2: NCS 1004 Interfaces

Note:

1. The USB ports (2) on the Controller Card were covered by the Tamper Evident Label (TEL) and shall not be used in FIPS mode.

2.4 1004 Front and Rear Panels

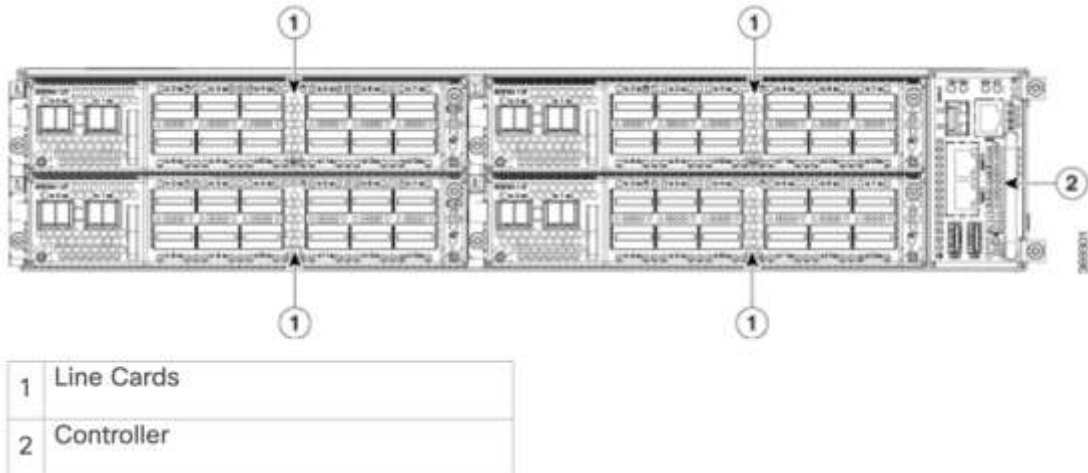


Figure 3: NCS 1004 Front View

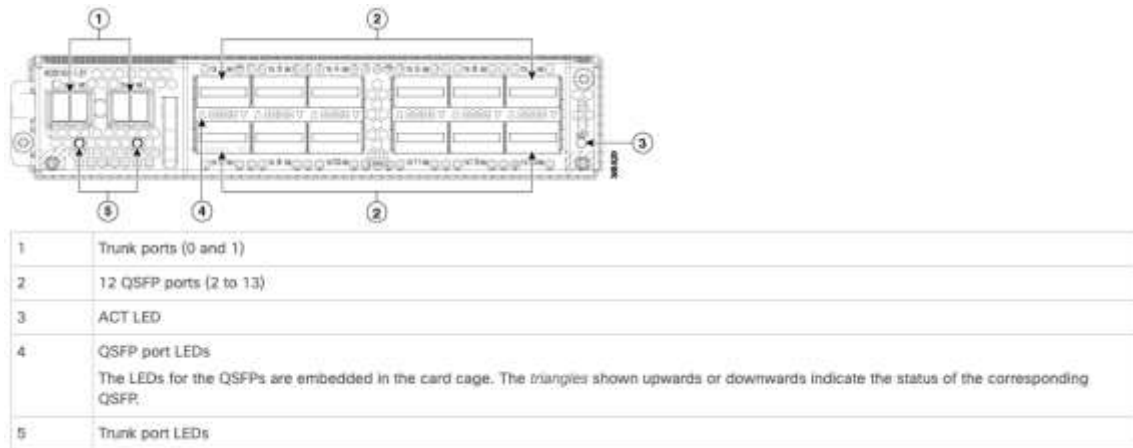
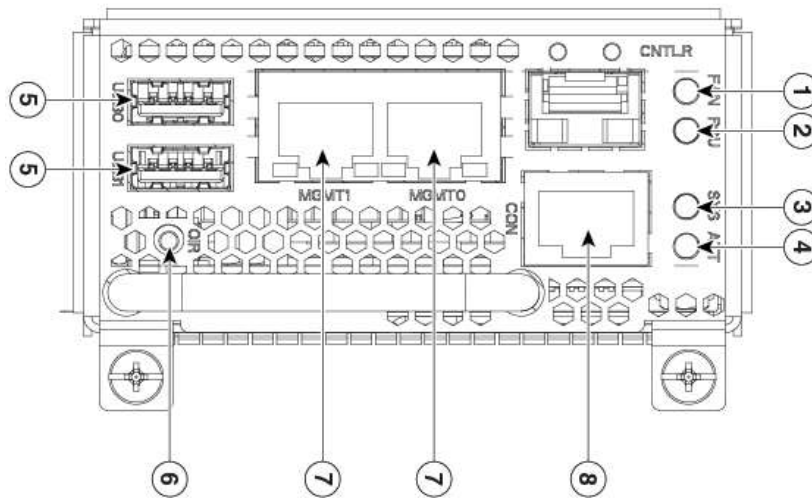
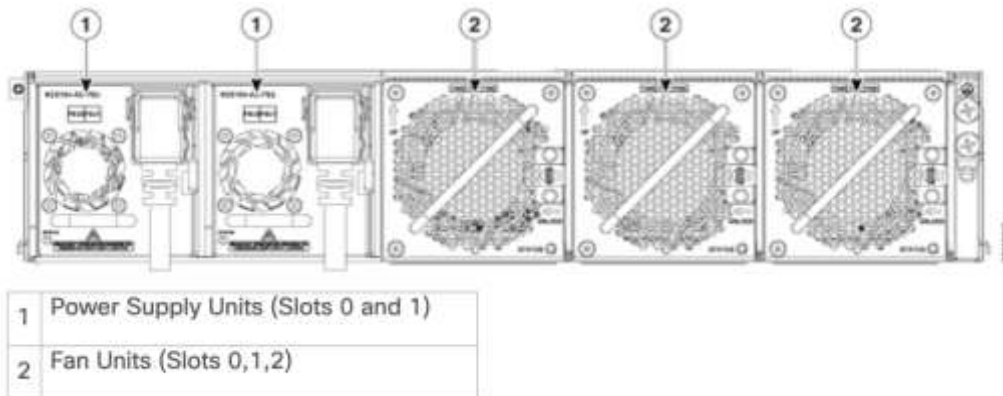


Figure 4: NCS 1004 Line Card



1	Fan Unit Status
2	Power Supply Unit Status
3	System Status
4	Attention LED
5	USB Ports (0 and 1)
6	OIR Button
7	Management Ports (0 and 1)
8	Console Port

Figure 5: NCS 1004 Controller Card



1	Power Supply Units (Slots 0 and 1)
2	Fan Units (Slots 0,1,2)

Figure 6: NCS 1004 Rear View

3. Roles, Services, and Authentication

The module can be accessed in one of the following ways:

- Console port
- SSHv2
- SNMPv3
- TLS v1.2
- OTNSec (using IKEv2 for key establishment)

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two main roles in the router that operators may assume: The Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services.

The User and Crypto Officer passwords and all other shared secrets must each be at least eight (8) characters long, including at least one six (6) alphabetic characters, (1) integer number and one (1) special character in length (enforced procedurally). See the Secure Operation section for more information. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 6,326,595,092,480 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total). The calculation should be $52 \times 52 \times 52 \times 52 \times 52 \times 52 \times 32 \times 10 = 6,326,595,092,480$. Therefore, the associated probability of a successful random attempt is approximately 1 in 6,326,595,092,480, which is less than the 1 in 1,000,000 required by FIPS 140-2.

In addition, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, if an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is $60,000 / 6,326,595,092,480 = 1/105,443,251$, which is less than 1 in 100,000 required by FIPS 140-2.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chances required by FIPS 140-2. Similarly, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, an attacker would probably get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is $60,000 / 2^{112} = 1/8.67 \times 10^{28}$, which is less than 1 in 100,000 required by FIPS 140-2.

3.1 User Services

A User enters the system by accessing the Console port, SSHv2, TLSv1.2, SNMPv3 and OTNSec. The User role can be authenticated via either User Name/Password or RSA based authentication method. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The services available to the User role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below.

The services available to the User role consist of the following:

Services	Description	Keys and CSPs Access
Status Functions	View the module configuration, routing tables, active sessions health, and view physical interface status.	User password (r, w, d)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	User password (r, w, d)
Network Functions	Connect to other nodes and initiate diagnostic network services (i.e., ping, mtrace).	User password (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2.	User password, SSHv2 private key, SSHv2 public key, SSHv2 integrity key and SSHv2 session key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
TLSv1.2 Functions	Negotiation and encrypted data transport via TLSv1.2.	User password, DRBG entropy input, DRBG seed, DRBG V, DRBG Key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key and TLS integrity key (r, w, d)
SNMPv3 Functions	Monitor device using SNMPv3	SNMPv3 engineID, SNMPv3 password and SNMPv3 session key (r, w, d)
OTNSec Functions	Negotiation and encrypted data transport via OTNSec	IKEv2 skeyid, IKEv2 skeyid_d, SKEYSEED, ISAKMP preshared, IKE session encryption key, IKE session authentication key, OTNSec session key (r, w, d)

Table 3: User Services (r = read, w = write, d = delete)

3.2 Crypto Officer Services

During initial configuration of the module, the Crypto Officer password is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration of the module. A CO role enters the system by accessing the Console port, SSHv2, TLSv1.2, SNMPv3 or OTNSec. The User role can be authenticated via either User Name/Password or RSA based authentication method. The services available to the Crypto Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below. The Crypto Officer services consist of the following:

Services	Description	Keys and CSPs Access
Configure the module	Define network interfaces and settings, enable interfaces and network services, set system date and time, and load authentication information.	DRBG seed, DRBG entropy input, DRBG V and DRBG key, DH private DH public key, DH shared secret, ECDH private ECDH public key, ECDH shared secret, User password, Crypto Officer (CO) password, SSHv2 private key, SSHv2 public key, SSHv2 session integrity key, SSHv2 session key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, SNMPv3 engineID, SNMPv3 password, SNMPv3 session key, IKEv2 skeyid, IKEv2 skeyid_d, SKEYSEED, ISAKMP preshared, IKE session encryption key, IKE session authentication key, OTNSec session key (r, w, d)
Define Rules and Filters	Create packet Filters that are applied to User data streams for each node.	User password (r, w, d)
View Status Functions	View the appliance configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	User password, Crypto Officer (CO) password (r, w, d)
Manage the Module	Log off users, shutdown or reload the module, erase the memory, view complete configurations, manager user rights, perform firmware updates, and restore configurations.	Crypto Officer (CO) password (r, w, d)

TLsv1.2 Functions	Configure TLsv1.2 parameters, provide entry and output of CSPs.	DRBG entropy input, DRBG Seed, DRBG V, DRBG Key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key and TLS integrity key (r, w, d)
SSHv2 Functions	Configure SSHv2 parameter, provide entry and output of CSPs.	Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, EC Diffie-Hellman private key, EC Diffie-Hellman public key, EC Diffie-Hellman Shared Secret, SSHv2 private key, SSHv2 public key, SSHv2 session integrity key and SSHv2 session key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
SNMPv3 Functions	Device configuration of monitoring services and monitoring by the CO using SNMPv3	SNMPv3 engineID, SNMPv3 password and SNMPv3 session key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)
OTNSec Functions	Configure OTNSec parameters, provide entry and output of CSPs.	IKEv2 skeyid, IKEv2 skeyid_d, SKEYSEED, ISAKMP preshared, IKE session encryption key, IKE session authentication key, OTNSec session key (r, w, d)

Table 4: Crypto Officer Services (r = read, w = write, d = delete)

3.3 Non-FIPS mode Services

The cryptographic module in addition to the above listed FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the Non-Approved services in Section 3.3, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Services ¹	Non-Approved Algorithms
SSH	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

Table 5: Non-approved algorithms in the Non-FIPS mode services

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

3.4 Unauthenticated Services

The services for someone without an authorized role are to view the status output from the module's LED pins and cycle power.

¹ These approved services become non-approved when using any non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

4. Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role login, and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual distribution are used for pre-shared keys whereas protocols such as TLS and SSH are used for electronic distribution.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. Only an authenticated Crypto Officer can view the keys. All other keys are associated with the user/role that entered them. The entropy source (NDRNG) within the module provides at least 256 bits of entropy to seed SP800-90a DRBG for use in key generation.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256)	384-bits	This is the entropy for SP800-90A CTR_DRBG. Used to construct the seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256)	384-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR_DRBG (AES-256)	128-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG key	SP800-90A CTR_DRBG (AES-256)	256-bits	Internal critical value used as part of SP800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman shared secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-379 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by using FIPS186-4 key generation method, and the seed used to generate asymmetric key-pairs is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
Diffie-Hellman public key	DH	2048 – 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman shared Secret	ECDH	P-256, P-384, P-521 Curves	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman private key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPsec session. The private key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is generated by using FIPS186-4 key generation method, and the seed used to generate asymmetric key-pairs is generated by calling SP800-90A DRBG..	DRAM (plaintext)	Power cycle the device
EC Diffie-Hellman public key	ECDH	P-256, P-384, P-521 Curves	Used in establishing the session key for an IPsec session. The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Power cycle the device
User password	Password	8-25 characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Overwrite with new password
Crypto Officer (CO) password	Password	8-25 characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
SSHv2 private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by using FIPS186-4 RSA key generation method, and the seed used to generate asymmetric key-pairs is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SSHv2 integrity key	HMAC-SHA-1/256	160-256 bits	Used for SSHv2 connections integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 session key	AES	AES 128/192/256 bits	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSHv2).	DRAM (plaintext)	Automatically when SSH session is terminated
TLS RSA private key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. This key is generated by using FIPS186-4 RSA key generation method, and the seed used to generate asymmetric key-pairs is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public key	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiations. This key is derived in compliance with FIPS186-4 RSA key pair generation method in the module. Generated by the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	Keying material	48 Bytes	Keying material used to derive TLS master secret during the TLSv1.2 session. This secret is internally generated by calling SP800-90A DRBG.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS master secret	Keying material	48 Bytes	Keying material used to generate other TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS encryption key	AES	AES 128/192/256 bits	Used in TLS connections to protect the session traffic. This key is derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA 256/384/512	256-512 bits	Used for TLS integrity to assure the traffic integrity. This key is derived via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SNMP v3 password	Shared Secret	32 bytes	The password use for SNMPv3 authentication. It is entered by Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
SNMPv3 engineID	Shared Secret	32 bits	Unique string to identify the SNMP engine	NVRAM (plaintext)	Overwrite with new engine ID
SNMPv3 session key	AES	128 bits	Used to protect SNMPv3 traffic. It was derived using key derivation function defined in SP800-135 KDF (SNMPv3).	DRAM (plaintext)	Automatically when SNMP session is terminated
IKEv2 skeyid	Keying material	160 – 512 bits	It was derived using key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
IKEv2 skeyid_d	Keying material	160 – 512 bits	It was derived using key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
SKEYSEED	Keying material	160 bits	Keying material known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Power cycle the device
ISAKMP preshared	Pre-shared secret	Variable 8 plus characters	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new shared secret
IKE session encryption key	AES	256 bits	The IKE session encrypt key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	DRAM (plaintext)	Power cycle the device
IKE session authentication key	HMAC-SHA256	256 bits	The IKE session authentication key is derived by using skeyid_d, Diffie-Hellman shared secret and other non-secret values through the key derivation functions defined in SP800-135 KDF (IKEv2). Used for payload integrity verification.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
OTNSec session Key	AES-GCM	256 bits	The OTNSec uses IKEv2 to establish the cryptographic keys, where SP800-135 KDF (IKEv2) was used to derive the session keys to protect the OTNSec traffic.	DRAM (plaintext)	Power cycle the device

Table 6: Cryptographic Keys and CSPs

5. Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

5.1 Approved Cryptographic Algorithms

	Cisco FIPS Object Module Implementation	HW On-board Algorithm Implementation
AES (AES-CBC); Key Length: 128, 192, 256	Cert. #C910	
AES (AES-ECB, AES-GCM); Key Length: 256	N/A	Certs. #4707 and #4770
SHS (SHA-1, SHA-256, SHA-384, SHA-512)	Cert. #C910	N/A
HMAC (HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512)	Cert. #C910	N/A
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	Cert. #C910	N/A
DRBG (AES-256, CTR_DRBG)	Cert. #C910	N/A
CVL Components (TLSv1.2, SSHv2, IKEv2 and SNMPv3)	Cert. #C910	N/A
CKG (Vendor affirmed)	N/A	N/A

Table 7: Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- No parts of the SSH, TLS, IKE and SNMP protocols, other than the KDF, have been tested by the CAVP and CMVP.
- The module's AES-GCM implementation conforms to the requirements from scenario #i under IG A.5 (scenario #1), following RFC 7296 for IKEv2. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90A DRBG.

5.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (CVL Cert. #C910, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (CVL Cert. #C910, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (non-deterministic random number generator)

5.3 Non-Approved Cryptographic Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- DES
- HMAC MD5
- MD5
- RC4
- HMAC-SHA1 is not allowed with key size under 112-bits

6. Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

6.1 Power On Self-Tests

- Cisco FIPS Object Module Algorithm Implementation POSTs
 - AES-CBC (encrypt/decrypt) KATs
 - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
 - SHA-1 KAT
 - HMAC KATs (HMAC-SHA-1/256/384/512)
 - RSA KATs (separate KAT for signing; separate KAT for verification)
- Firmware Integrity Test (HMAC-SHA-1)
- Hardware On-board Algorithm Implementation POSTs
 - AES-ECB (encrypt/decrypt) KATs
 - AES GCM (encrypt/decrypt) KATs

6.2 Conditional Tests

- Cisco FIPS Object Module Algorithm Implementation Conditional Tests
 - CRNGT to DRBG
 - CRNGT to NDRNG
 - PWCT to RSA

The module performs all power-on self-tests automatically when the power is applied. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the module's interfaces; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a security appliance reboot.

7. Physical Security

The module natively meets the FIPS 140-2 opacity requirements. However, tamper evident labels are required to meeting the FIPS 140-2 tamper evidence requirements.

7.1 Tamper Evidence Label (TEL) placement

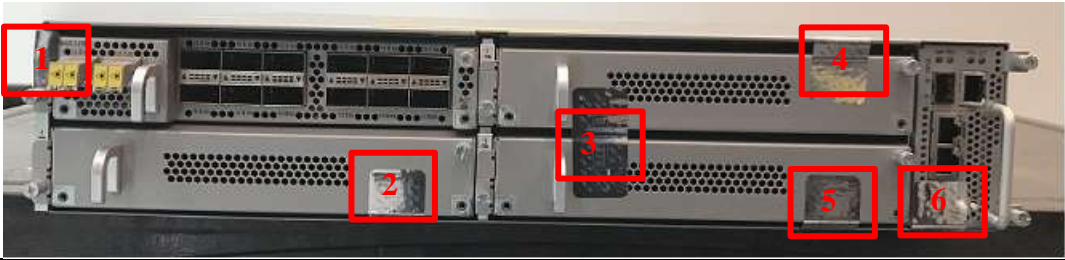
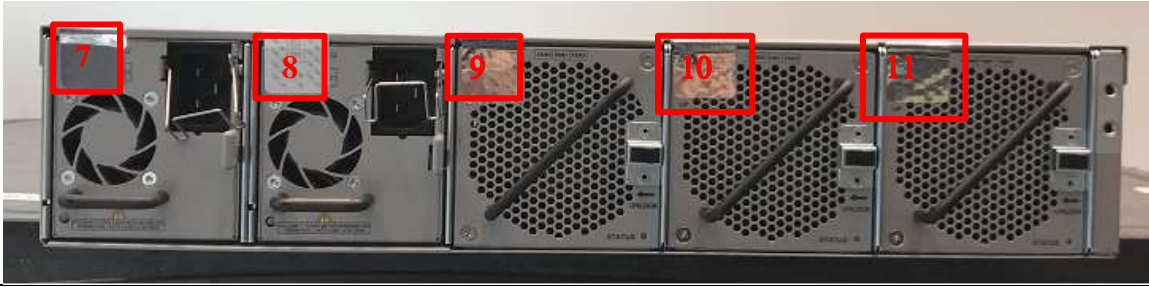
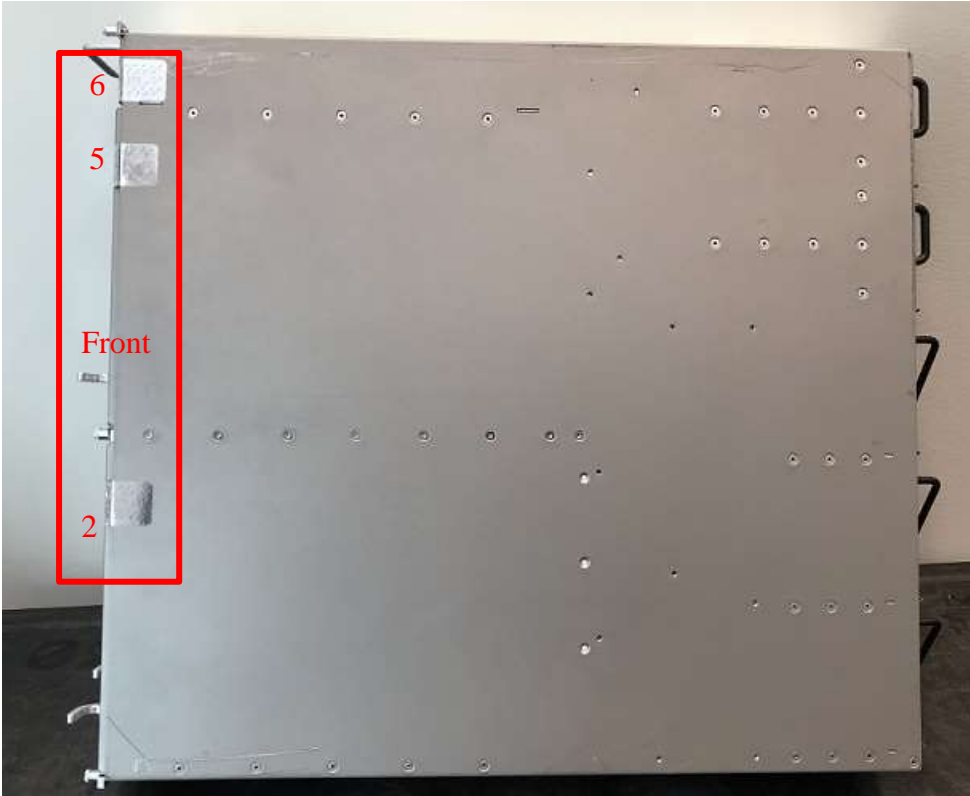
The tamper evident labels (TELs) shall be installed on the module prior to operating in FIPS mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location. Once the module has been configured to meet FIPS 140-2 Level 2 requirements, the module cannot be physically accessed without signs of tampering. Any attempt to open the module units will damage the tamper evidence seals or the material of the module cover. Tamper evidence seals can be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices.

Should the CO have to remove, change or replace TELs for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth. Any deviation of the TELs placement by unauthorized operators such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below shall mean the module is no longer in FIPS mode of operation. Returning the system back to FIPS mode of operation requires the replacement of the TELs as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy. To seal the system, apply tamper-evidence labels as depicted in the figures below.

Chassis Models	Number Tamper labels	Tamper Evident Labels
NCS1004=	15	AIR-AP-FIPSKIT=

Table 8: NCS1004 TELs

The module has a total of 15 TELs places in different locations.

View	NCS1004 – TEL Placement and Numbering
Front	 <p>The front view of the NCS1004 server chassis shows six red boxes numbered 1 through 6. Box 1 is on the left edge near the top. Box 2 is on the bottom edge near the center. Box 3 is on the bottom edge near the right. Box 4 is on the top edge near the right. Box 5 is on the bottom edge near the right, below box 3. Box 6 is on the bottom edge near the right, below box 5.</p>
Back	 <p>The back view of the NCS1004 server chassis shows five red boxes numbered 7 through 11. Box 7 is on the left edge near the top. Box 8 is on the left edge near the top, to the right of box 7. Box 9 is on the top edge near the center. Box 10 is on the top edge near the right. Box 11 is on the top edge near the right, to the right of box 10.</p>
Bottom	 <p>The bottom view of the NCS1004 server chassis shows three red boxes numbered 2, 5, and 6. Box 2 is on the left edge near the bottom. Box 5 is on the left edge near the top. Box 6 is on the left edge near the top, above box 5. The word "Front" is printed in red on the left edge, between boxes 5 and 6.</p>




View	NCS1004 – TEL Placement and Numbering
Top	
Left	
Right	

Table 9: NCS1004 TELs Placement

Applying Tamper Evidence Labels

Step 1: Turn off and unplug the module before cleaning the chassis and applying labels.

Step 2: Clean the chassis of any grease, dirt, or oil before applying the tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.

Step 3: Apply the labels to cover the module as shown in the figures above.

The tamper evident labels are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the module will damage the tamper evident labels or the material of the security appliance cover. Because the tamper evident labels have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the security appliance has not been tampered with. Tamper evident labels can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices.

Inspection of the tamper seals should be incorporated into facility security to include how often to inspect and any recording of the inspection. It is recommended inspection of TELs occur at least every 30 days but this is the facilities Security Manager decision.

8. Secure Operation

The Cisco Network Convergence System 1004 Cryptographic Module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

The module was validated with firmware version IOS XR 7.0.1. It is the only allowed firmware version for FIPS-approved mode of operation. The Crypto Officer must configure and enforce the following initialization steps.

8.1 Initial Setup

1. The Crypto Officer must apply tamper evidence labels as described in of this document. Please be aware that the USB ports (Two on the Controller Card) were disabled by a tamper evident label and shall not be used while in FIPS mode. All configuration will be done from the CLI.

2. Configure Password

To be considered FIPS compliant, the Crypto Officer shall follow up the requirements from section 3 in this document to update the default password by using the following command

- a. `ios# username <username> password <password>`

3. Enable FIPS mode

- a. `ios# configure`
 - b. `ios# crypto fips-mode`
 - c. `ios# commit`
 - d. `ios# reload location all`

4. Configure SNMPv3

- a. `ios# configure`
 - b. `ios# snmp-server view`
 - c. `ios# snmp-server group`
 - d. `ios# snmp-server user username groupname v3 auth sha auth-password priv aes priv-password`

5. Configure SSHv2
 - a. ios# configure
 - b. ios# ssh server v2

6. Configure Syslog over TLSv1.2
 - a. ios# configure
 - b. ios# crypto ca trustpoint
 - c. ios# subject-name
 - d. ios# enrollment url
 - e. ios# enrollment retry count
 - f. ios# enrollment retry period
 - g. ios# rsakeypair
 - h. ios# crypto ca authenticate
 - i. ios# logging tls-server syslogserver
 - j. ios# severity debugging
 - k. ios# address ipv4
 - l. ios# debug crypto pki errors
 - m. ios# debug crypto pki messages
 - n. ios# debug crypto pki transactions

7. Configure IKEv2
 - a. Proposal
 - i. ios# configure
 - ii. ios# ikev2 proposal <proposal-name>
 - iii. ios# encryption {aes-gcm-256} {aes-gcm-128} {aes-cbc-256} {aes-cbc-192} {aes-cbc-128}
 - iv. ios# integrity {sha-1} {sha-256} {sha-384} {sha-512}
 - v. ios# prf {sha-1} {sha-256} {sha-384} {sha-512}

 - b. Policy
 - i. ios# configure
 - ii. ios# ikev2 policy <policy-name>
 - iii. ios# proposal <proposal-name1 proposal-name2 proposal-name3>
 - iv. ios# match address local { ipv4-address }

 - c. Keyring
 - i. ios# configure
 - ii. ios# keyring <keyring-name>
 - iii. ios# peer <peer-block name>
 - iv. ios# address {ipv4-address [mask]}
 - v. ios# pre-shared-key <key>

 - d. Profile
 - i. ios# configure
 - ii. ios# ikev2 profile <profile-name>
 - iii. ios# match identity remote address {ipv4-address [mask]}
 - iv. ios# keyring <keyring-name>
 - v. ios# lifetime <seconds>

8. Configure OTNSec
 - a. OTNSec Policy
 - i. ios# configure
 - ii. ios# otnsec-policy <policy-name>
 - iii. ios# cipher-suite AES-GCM-256
 - iv. ios# security-policy must-secure
 - v. ios# sak-rekey-interval <seconds>

9. Verify FIPS mode is enabled
 - a. ios# show running-config
 - b. output:
crypto fips-mode
end

Note: Detailed Cisco NCS1004 configuration guidance can be found at the following links

- Configuration Guide for Cisco NCS 1004, IOS XR Release 7.0.1
<https://www.cisco.com/c/en/us/td/docs/optical/ncs1004/70x/configuration/guide/b-configuration-guide-ncs1004-r701.html> (Updated: June 24, 2020)