Cisco Catalyst 4506-E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45-E and WS-X4748-RJ45V+E)

FIPS 140-2 Level 1

Non-Proprietary Security Policy

Overall Level 1 Validation

Version 0.5

September 9, 2016

Table of Contents

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 4506-E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45-E and WS-X4748-RJ45V+E). This security policy describes how the modules listed below meet the security requirements of FIPS 140-2, and how to operate the switch with on-board crypto enabled in a secure FIPS 140-2 mode.

The switch included as part of the FIPS 140-2 validation may be configured in the following configurations running IOS-XE 3.7.0E firmware.

Chassis Part Number	Supervisor Cards	Line Cards
WS-C4506-E	Single supervisor card WS-X45-SUP7-E	Line card WS-X4748-RJ45V+E
		Line card WS-X4748-RJ45-E
	Single supervisor card WS-X45-Sup7L-E	Line card WS-X4748-RJ45V+E
		Line card WS-X4748-RJ45-E

Table 1: Module Configurations

1.1 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.

The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

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 http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 Terminology

In this document, the Cisco Catalyst WS-C4506-E with the configurable Supervisor cards and Line cards are referred as the C4500-E Switch, the switch or the module. Each of these items can be individually mentioned in this document. Cisco WS-C4506-E can be referred to as the chassis. Cisco WS-X45-SUP7-E and WS-X45-Sup7L-E are referred to

as the Supervisor cards. Cisco WS-X4748-RJ45-E and WS-X4748-RJ45V+E are referred to as Line cards.

1.3 FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package includes:

Vendor Evidence

Finite State Machine

Other supporting documentation as additional references

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc.

2 The Module Description

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Catalyst 4500 series switches with the VPN Services Port Adapter offer versatility, integration, and security to branch offices. With numerous network modules and service modules available, the modular architecture of the Cisco switches easily allows interfaces to be upgraded to accommodate network expansion. The Catalyst switch provides a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 1 requirements, as a multi-chip standalone module.

The switch includes cryptographic algorithms implemented in IOS-XE image executed in Rommon, and hardware ASICs. The Line card ASICs implement Cisco TrustSec protocol (CTS) supporting IEEE 802.1AE for Layer 2 CTS and contain hardware implementations of the GCM and ECB modes of the AES algorithm.

The switch supports the Cisco TrustSec protocol which provides policy-based access control, identity-aware networking, and data confidentiality and integrity. The switch also supports SSH and TLS to provide remote administrative access to the module.

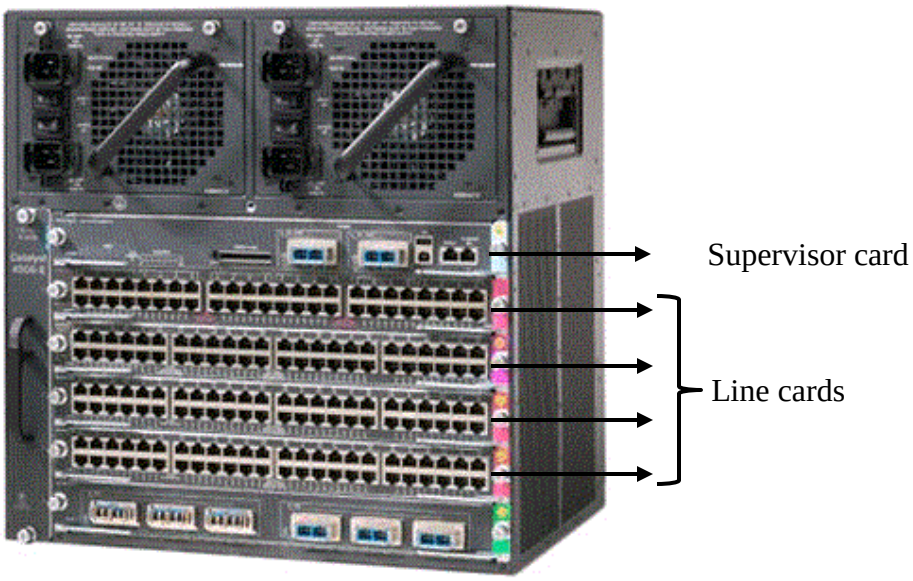

Figure 1: Catalyst 4506-E Switch with a Supervisor card and four line cards

2.1 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**1**

Table 2: Module Validation Level

3 Cryptographic Boundary

The cryptographic boundary is defined as being the physical enclosure of the chassis.

All of the functionality described in this publication is provided by components within this cryptographic boundary. The chassis incorporates one or more Supervisor cards and one or more Line cards.

4 Cryptographic Module Ports and 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 four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The module also supports a power interface.

The following table identifies the features on the module covered by this Security Policy:

Physical Interface	Logical Interface
10/100/1000Mbps Ethernet ports 10G SFP+ Ethernet ports Console Port Management Port	Data Input Interface
10/100/1000Mbps Ethernet ports 10G SFP+ Ethernet ports Console Port Management Port	Data Output Interface
10/100/1000Mbps Ethernet ports 10G SFP+ Ethernet ports Console Port Management Port	Control Input Interface
10/100/1000Mbps Ethernet ports 10G SFP+ Ethernet ports Console Port Management Port LEDs	Status Output Interface
Power Plug	Power Interface

Table 3: Module Interfaces

5 Roles, Services, and Authentication

Authentication is role-based. Each user is authenticated upon initial access to the module. There are two roles in the Switch that may be assumed: the Crypto Officer (CO) role and the User role. The administrator of the Switch assumes the CO role in order to configure and maintain the Switch using CO services, while the Users exercise security services over the network.

5.1 User Role

The role is assumed by users obtaining general security services. From a logical view, user activity exists in the data-plane. Users are authenticated using EAP methods and 802.1X-REV, and their data is protected with 802.1AE protocols. EAP and 802.1X-REV can use password based credentials for User role authentication – in such a case the user passwords must be at least eight (8) characters long, including at least one letter and at least one number character (enforced procedurally). If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89

x 32 x 10. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

EAP and 802.1X-REV can also authenticate the User role via certificate credentials by using 2048 bit RSA keys – in such a case the security strength is 112 bits, so the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $8.65x10^{31}$ attempts per second, which far exceeds the operational capabilities of the module to support.

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:

Services	Description	Keys and CSPs Access
Secured Dataplane	MACsec Network Functions: authentication, access control, confidentiality and data integrity services provided by the MACsec protocol	Diffie-Hellman private key, Diffie-Hellman public key, Diffie- Hellman Shared Secret, MACsec Security Association Key (SAK), MACsec Connectivity Association Key (CAK), MACsec Key Encryption Key (KEK), MACsec Integrity Check Key (ICK), Pairwise Master Key (PMK), Protected Access Credential (PAC) Key, Pairwise Transient Key (PTK), Key Confirmation Key (KCK) (r, w, d)
IPsec VPN	Negotiation and encrypted data transport via IPSec VPN	User password, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)

Table 4 - User Services

5.2 CO Role

This role is assumed by an authorized Crypto Officer (CO) connecting to the switch via CLI through the console port and performing management functions and module configuration. Additionally, the stack master is considered CO for stack members. From a logical view, CO activity exists only in the control plane. IOS prompts the CO for their username and password, and, if the password is validated against the CO's password in IOS memory, CO is allowed entry to the IOS executive program. The module supports RADIUS and TACACS+ for authentication of CO.

CO passwords must be at least eight (8) characters long, including at least one letter and at least one number character (enforced procedurally). If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

The CO role is responsible for the configuration of the switch. The services available to the CO 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:

Services	Description	Keys and CSPs Access
Configure	Define network interfaces and settings, create command aliases, set the protocols the switch will support, enable interfaces and network services, set system date and time, and load authentication information.	Enable password (r, w, d)
Manage	Log off users, shutdown or reload the switch, manually back up switch configurations, view complete configurations, manage user rights, and restore switch configurations.	Enable password (r, w, d)
Define Rules and Filters	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	Enable password (r, w, d)
View Status Functions	View the switch configuration, routing tables, active sessions, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Enable password, User password (r, w, d)
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, skeyid, skeyid_d, SKEYSEED, IPsec encryption key, IPsec authentication key (r, w, d)
Configure Remote Authentication	Set up authentication account for users and devices using RADIUS or TACACS+	RADIUS secret, RADIUS Key wrap key, TACACS+ secret (r, w, d)

Services	Description	Keys and CSPs Access
HTTPs	HTTP server over TLS (1.0).	TLS Server RSA private key, TLS Server RSA public key, TLS pre-master secret, TLS session keys, TLS authentication keys, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman Shared Secret, SSH RSA private key, SSH RSA public key, SSH session key, SSH session authentication key (r, w, d)
SNMPv3	Configure SNMPv3 MIB and monitor status.	SNMPv3 Password, snmpEngineID, SNMP session key (r, w, d)
IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The CO has access to all User services.	User Password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 8, Zeroization column.	All CSPs (d)

Table 5 - Crypto Officer Services

5.3 Unauthorized Role

The services for someone without an authorized role are: passing traffic through the device, view the status output from the module's LED pins, and cycle power.

5.4 Services Available in Non-FIPS Mode of Operation

The cryptographic module in addition to 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. The module is considered to be in a non-FIPS mode of operation when it is not configured per the *Secure Operation* (section 10) section. The FIPS approved services listed in Table 6 become non-approved services when using any non-approved algorithms or non-approved key or curve sizes.

Services [1]	Non-Approved Algorithms
IPsec	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
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
SNMP v1/v2	Hashing: MD5 Symmetric: DES

Table 6 - Non-approved algorithms in the Non-FIPS mode services

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

6 Physical Security

Cisco Catalyst 4506-E with Supervisor and Line Cards is a multi-chip standalone cryptographic module. The module meets FIPS 140-2 level 1 physical security requirements as production grade equipment.

7 Cryptographic Algorithms

7.1 Approved Cryptographic Algorithms

The module supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms included in the module for use in the FIPS mode of operation.

[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.

Algorithm	Algorithm Implementation Name		
	IOS Common Cryptographic Module (IC2M) within Cat4K (Firmware Implementation)	**IOS-XE Image Signing Implementations (Firmware Implementation)**	**Cat4K ASIC Algorithm Implementation (Hardware Implementation)**
AES 128/192/256 bits (ECB, CBC, GCM)	#2624		
AES (ECB, GCM; 128 bits)			#2057
Triple-DES (CBC, 3-key)	#1575		
SHS (SHA-1/256/384/512)	#2200		
SHS (SHA-512)		#2198	
HMAC (SHA-1/256/384/512)	#1622		
RSA (KeyGen; PKCS1_V1_5; Sig (gen/ver) 2048 bits)	#1341 and #2083		
RSA (PKCS1_V1_5; Sig (ver) 2048 bits)		#1339	
DRBG (AES CTR-256)	#403		
KBKDF (SP800-108)	#98		
CVL Component (SP800-135 KDF for IKEv2, TLS, SSH, SNMPv3)	#877		

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.
- The AES-GCM IV generation method from each of AES #2624 (GCM used in IPSec Protocol) and AES #2057 (GCM used in MACsec Protocol) is in compliance with IG A.5, scenario #1. The IV in respective AES-GCM is constructed in compliance with RFC 6071 (IPSec Protocol) or MACsec protocol. In MACsec service, IPSec is used to protect the RADIUS traffics. The module is in compliance with SP 800-57, Part 3, Rev.1. The module generates new AES-GCM keys if the module loses power.
- The SSH, TLS, SNMPv3 and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

7.2 Non-FIPS Approved, but Allowed Cryptographic Algorithms

The cryptographic module implements the following non-approved algorithms, but they are allowed to be used in a FIPS 140-2 mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- AES (Cert. #2624, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)
- NDRNG (entropy source for DRBG; at minimum 256 bits can be obtained)
- HMAC MD5 is allowed in FIPS mode strictly for TLS
- MD5 is allowed in FIPS mode strictly for TLS

7.3 Non-FIPS Approved and not Allowed Cryptographic Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in a FIPS 140-2 mode of operation:

- Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- RSA (key wrapping; non-compliant less than 112 bits of encryption strength)
- DES
- HMAC MD5
- MD5
- RC4

8 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the CO role login, and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Note that the command **fips zeroize all** will zeroize a large majority of the listed CSPs. The CTS specific CSPs will require the **cts key zeroize** CLI. The module supports the following cryptographic keys and critical security parameters (CSPs):

ID	Algorithm	Description	Storage	Zeroization Method
General Keys/CSPs				
Enable password	Password	Variable (8+ characters). The password used to authenticate the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by overwriting with new password
User password	Password	Variable (8+ characters). The password used to authenticate the User role. This CSP is created by the CO role and entered by the User role.	NVRAM (plaintext)	Zeroized by overwriting with new password
RADIUS secret	Shared Secret	Variable (8+ characters). The RADIUS shared secret Used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by "# no radius-server key" command
RADIUS Key wrap key	AES CBC	128/256 bits. Secures communication with RADIUS authentication server. This CSP is entered by the Crypto Officer.	DRAM (plaintext)	Zeroized when data structure is freed
TACACS+ secret	Shared Secret	Variable (8+ characters). The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by "# no tacacs-server key" command
DRBG entropy input	SP 800-90A CTR_DRBG	256-bits. HW based entropy source output used to construct the seed.	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG Seed	SP 800-90A CTR_DRBG	384-bits. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG V	SP 800-90A CTR_DRBG	128-bits. Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form.	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG Key	SP 800-90A CTR_DRBG	256-bits. This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Automatically when the switch is power cycled
Diffie-Hellman private key	Diffie-Hellman	224, 256 or 379 bits. DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Automatically after shared secret generated

ID	Algorithm	Description	Storage	Zeroization Method
Diffie-Hellman public key	Diffie-Hellman	2048, 3072, or 4096 bits. DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Automatically after shared secret generated
Diffie-Hellman Shared Secret	Diffie-Hellman	2048, 3072, or 4096 bits. DH shared secret derived in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Zeroized upon deletion
SSH				
SSH RSA private key	RSA	2048 bits. The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
SSH RSA public key	RSA	2048 bits. The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
SSH session key	Triple-DES/AES	192-bits/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 (SSH).	DRAM (plaintext)	Automatically when SSH session terminated
SSH session authentication key	HMAC SHA	160/256/384/512-bits. It is used to authenticate all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is internally derived by the module.	DRAM (plaintext)	Automatically when SSH session terminated
TLS				
TLS Server RSA private key	RSA	2048 bits. The TLS server private key used in TLS connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
TLS Server RSA public key	RSA	2048 bits. The TLS server public key used in TLS connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
TLS pre-master secret	Shared Secret	384-bits. Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated

ID	Algorithm	Description	Storage	Zeroization Method
TLS session keys	Triple-DES/AES	192-bits/256-bits. This is the TLS session key. It is used to encrypt all TLS data traffics traversing between the TLS client and server. This key is derived via key derivation function defined in SP800-135 KDF (TLS)	DRAM (plaintext)	Automatically when session terminated
TLS authentication keys	HMAC SHA	160/256/384/512-bit. This is the TLS authentication key. It is used to authenticate all TLS data traffics traversing between the TLS client and server. This key is internally generated by the module.	DRAM (plaintext)	Automatically when session terminated
MACsec				
MACsec Security Association Key (SAK)	AES-GCM	128 bits. This key, internally generated by SP800-90A DRBG, is used for creating Security Associations (SA) for encrypting/decrypting the MACsec data plane traffic.	MACsec PHY (plaintext)	Automatically when session expires
MACsec Connectivity Association Key (CAK)	AES-GCM	128 bits. A CO configured preshared secret key possessed by members of a MACsec connectivity association to secure control plane traffic.	MACsec PHY (plaintext)	Automatically when session expires
MACsec Key Encryption Key (KEK)	AES-GCM	128 bits. Used to transmit SAKs to other members of a MACsec connectivity association. Internally generated by SP800-90A DRBG.	MACsec PHY (plaintext)	Automatically when session expires
MACsec Integrity Check Key (ICK)	Secret	128 bits. Used to verify the integrity and authenticity of MPDUs. Internally generated by SP800-90A DRBG.	MACsec PHY (plaintext)	Automatically when session expires
CTS (Cisco TrustSec)				
Pairwise Master Key (PMK)	AES-GCM	256 bits. The CO configured preshared PMK is used to derive the PTK (Pairwise Transient Key) which in turn is used in the session encryption (symmetric) key generation process.	NVRAM (plaintext)	Zeroized by “cts key zeroize” command
Protected Access	AES-CBC	256 bits. The PAC, derived from PMK, is dynamically provisioned in EAP-FAST	NVRAM (plaintext)	Zeroized by "clear cts pacs” command

ID	Algorithm	Description	Storage	Zeroization Method
Credential (PAC) Key		phase 0. The PAC-key is a shared secret that is used to secure further communications.		
Pairwise Transient Key (PTK)	AES-GCM	256 bits. Used to encrypt SAP payloads during SAP protocol implementations. This key is derived from PMK.	DRAM (plaintext)	Zeroized automatically when SAP implementation is terminated
Key Confirmation Key (KCK)	HMAC-SHA-1	160 bits. This key derived from PMK, is used to protect SAP payloads integrity during SAP protocol implementations	DRAM (plaintext	Zeroized automatically when SAP implementation is terminated

IPSec

skeyid	Shared Secret	160 bits. A shared secret known only to IKE peers. It is established via key derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Automatically when session expires
skeyid_d	Shared Secret	160 bits. A shared secret known only to IKE peers. It is derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Automatically when session expires
SKEYSEED	Shared Secret	160 bits. A shared secret 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)	Automatically when session expires
IKE session encryption key	TRIPLE-DES/AES	192-bit Triple-DES or a 256-bit AES. The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when session expires
IKE session authentication key	HMAC-SHA1	160 bits. The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when session expires

ID	Algorithm	Description	Storage	Zeroization Method
ISAKMP preshared	Pre-shared Secret	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by overwriting with new secret
IKE Authentication private Key	RSA	2048 bits. RSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
IKE Authentication public Key	RSA	2048 bits. RSA public key used in IKE authentication. This key is internally generated by the module.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
IPSec Authentication key	HMAC-SHA-1	160 bits. The IPsec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when session expires
IPSec encryption key	TRIPLE-DES/AES/AES-GCM	192 bits Triple-DES or 128/192/256 bits AES. The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined	DRAM (plaintext)	Automatically when session expires
SNMPv3				
SNMPv3 Password	Secret	256 bits. Configured by the CO, this secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	NVRAM (plaintext)	Zeroized by overwriting with new secret
snmpEngineID	Shared secret	32 bits. Unique string to identify the SNMP engine. CO configures the shared secret.	NVRAM (plaintext)	Overwritten with new engine ID
SNMP session key	AES	128 bits. Encrypts SNMP traffic. This key is derived via key derivation function defined in SP800-135 KDF (SNMP).	DRAM (plaintext)	Automatically when session expires

Table 8 - Cryptographic Keys and CSPs

9 Self-Tests

The module includes 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. The module implements the following power-on self-tests:

- IOS-XE Power-On Self-Tests Known Answer Tests (KATs):
    - AES (encryption and decryption) KATs
    - AES-CMAC KAT
    - AES-GCM (encryption and decryption) KATs
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-512 KAT
    - DRBG health test (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-512 KAT
    - RSA (sign and verify) KATs
    - Triple-DES (encryption and decryption) KATs
- IOS-XE Image Signing Implementations KATs (for Firmware Integrity Test):
    - RSA (verify) KAT
    - SHA-512 KAT
- Cat4K ASIC Algorithm Implementation KATs
    - AES-GCM (encryption and decryption) KATs

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to any other operations; this prevents the module from passing any data during a power-on self-test failure.

In addition, the modules also provide the following conditional self-tests:

- IOS-XE Firmware Implementation Conditional Tests
    - Continuous Random Number Generator Test for SP800-90A DRBG
    - Continuous Random Number Generator test for NDRNG
    - Conditional Bypass Test (IPsec Bypass)
    - RSA Pairwise Consistency Test

10 Secure Operation of the Cisco C4500-E Switch

The module meets all the overall Level 1 requirements for FIPS 140-2. Follow the setup instructions provided below to place the module in FIPS-approved mode. Operating this Switch without maintaining the following settings will remove the module from the FIPS approved mode of operation.

10.1 System Initialization and Configuration

1. The module must run the CAT4500e SUP7-E/SUP7L-E Universal Crypto Image version IOS-XE 3.7.0E (File name: cat4500e-universal.SPA.03.07.00.E.152-3.E.bin). This is the only allowable image for FIPS-approved mode of operation.
2. The CO must disable the ability to break from the console to the ROM monitor during startup. From the "configure terminal" command line, the CO enters the following syntax:

   no service password-recovery

3. The CO must create the "enable" password for the CO role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the CO first engages the "enable" command. The CO enters the following syntax at the "#" prompt:

   enable secret [PASSWORD]

4. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the CO enters the following syntax:

   line con 0

   password [PASSWORD]

   login local

5. The CO enables FIPS mode using the following command:

   Switch(config)# fips

6. The CO may configure the module to use RADIUS or TACACS+ for authentication. If the module is configured to use RADIUS, the Crypto-Officer must define RADIUS or shared secret keys that are at least 8 characters long, including at least one letter and at least one number. The RADIUS or TACACS+ traffics must be protected by an IPSec tunnel.
7. The CO shall only assign users to a privilege level 1 (the default).
8. The CO shall not assign a command to any privilege level other than its default.

10.2 Remote Access

1. SSH access to the module is allowed in FIPS approved mode of operation, using SSH v2 and a FIPS approved algorithm.
2. HTTPS/TLS access to the module is allowed in FIPS approved mode of operation, using SSLv3.1/TLSv1.0 and a FIPS approved algorithm.

10.3 Identifying Switch Operation in an Approved Mode

The following activities are required to verify that the module is operating in an Approved mode of operation.

1. Verify that the output of "The FIPS mode is on" was shown on the Command Line Interface after issuing command ‘show fips’ by Crypto Officer role.

11 Definition List

AES – Advanced Encryption Standard

CMVP – Cryptographic Module Validation Program

CSE – Communications Security Establishment

CSP – Critical Security Parameter

CTS – Cisco TrustSec

CVP – Component Validation List

DRBG – Deterministic Random Number Generator

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

HTTP – Hyper Text Transfer Protocol

KAT – Known Answer Test

LED – Light Emitting Diode

MAC – Message Authentication Code

NIST – National Institute of Standards and Technology

NVRAM – Non-Volatile Random Access Memory

RAM – Random Access Memory

NDRNG – Non-Deterministic Random Number Generator

SHA – Secure Hash Algorithm

SHS – Secure Hashing Standard

Triple-DES – Triple Data Encryption Standard