Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12

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

Document Version 1.0

August 3, 2020

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

Contents

FIPS 140-2 Non-Proprietary Security Policy 1
Level 2 Validation 1
1 Introduction 3
1.1 Purpose 3
1.2 Models 3
1.3 Module Validation Level 3
1.4 References 4
1.5 Terminology 4
1.6 Document Organization 4
2 Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access Points, Version 8.10, 16.12 5
2.1 Cryptographic Module Physical Characteristics 5
2.2 Module Interfaces 5
2.2.1 Cisco Aironet 1562i 6
2.2.2 Cisco Aironet 1562e/d/ps 9
2.2.3 Cisco Aironet 2802i and 3802i 12
2.2.4 Cisco Aironet 2802e and 3802e/p 14
2.2.5 Cisco Aironet 4800 17
2.3 Roles and Services 19
CO Authentication 19
User Authentication 20
User Services 20
Crypto Officer Services 21
2.4 Unauthenticated Services 21
2.5 Physical Security 22
2.5.1 Cisco Aironet 1562i Tamper Evident Label Placement 22
2.5.2 Cisco Aironet 1562e/d/ps Tamper Evident Label Placement 23
2.5.3 Cisco Aironet 2802i and 3802i Tamper Evident Label Placement 25
2.5.4 Cisco Aironet 2802e and 3802e/p Tamper Evident Label Placement 26
2.5.5 Cisco Aironet 4800 Tamper Evident Label Placement 28
2.6 Cryptographic Algorithms 30
Approved Cryptographic Algorithms 30
Non-Approved but Allowed Cryptographic Algorithms 33
2.7 Cryptographic Key Management 33
2.8 Self-Tests 37
3 Secure Operation of the Cisco Aironet Access Points 38
4 Acronyms 40

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12 referred to in this document as Access Points (APs). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and may be freely distributed.

1.2 Models

- Cisco Aironet 1562e Access Point with (HW: 1562e)
- Cisco Aironet 1562i Access Point with (HW: 1562i)
- Cisco Aironet 1562d Access Point with (HW: 1562d)
- Cisco Aironet 1562ps Access Point with (HW: 1562ps)
- Cisco Aironet 2802e Access Point with (HW: 2802e)
- Cisco Aironet 2802i Access Point with (HW: 2802i)
- Cisco Aironet 3802e Access Point (HW: 3802e)
- Cisco Aironet 3802i Access Point (HW: 3802i)
- Cisco Aironet 3802p Access Point (HW: 3802p)
- Cisco Aironet 4800 Access Point (HW: 4800)

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/groups/STM/index.html.

1.3 Module Validation Level

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

Table 1 Module Validation Level

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
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	**Overall module validation level**	**2**

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1.4 References

This document deals only with operations and capabilities of the Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12 cryptographic module security policy. More information is available on the routers from the following sources:
`

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/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.5 Terminology

In this document, the Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12 are referred to as access points, APs or the modules.

1.6 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 Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access points, Version 8.10, 16.12 and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for secure 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

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2 Cisco Aironet 1562e/i/d/ps, 2802e/i, 3802e/i/p, 4800 Wireless LAN Access Points, Version 8.10, 16.12

The Cisco Aironet 1560, 2800, 3800, and 4800 Series Access Points are highly versatile and deliver the most functionality of any access points in the industry. For organizations paving the way for the new 802.11ac Wave 2 standard, the Cisco Aironet 1560, 2800, 3800, and 4800 Series are the perfect solution. The access points go beyond getting ready for the new standard, providing the ultimate in flexibility and versatility.

2.1 Cryptographic Module Physical Characteristics

Each access point is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “back,” “left,” “right,” and “bottom” surfaces of the case. Included in this physical boundary is the ACT2Lite module (certificate #2125).

2.2 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, status output, and power. The logical interfaces and their mapping are described in the following tables:

Table 2: Module Physical Interface/Logical Interface Mapping

Router Physical Interface	FIPS 140-2 Logical Interface
Radio Antennas, Ethernet ports and SFP ports (1562 only)	Data Input Interface
Radio Antennas, Ethernet ports and SFP ports (1562 only)	Data Output Interface
Radio Antennas, Ethernet ports	Control Input Interface
SFP ports (1562 only) USB Port (2800/3800,4800 not used in FIPS mode)	
Radio Antennas, LEDs, Ethernet ports, USB port (2800/3800,4800 not used in FIPS mode)	Status Output Interface
SFP ports (1562 only)	
Power plug and PoE port	Power Interface
Console port	N/A – Covered with tamper seals.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.2.1 Cisco Aironet 1562i

Figure 1: Front

The left-hand bolt on the front is for the SFP port. The right-hand screw on is hides an ethernet/POE port.

Figure 2: Rear

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 3: Left

The covering screw hides the Power-In.

Figure 4: Right

The covering screw hides the console connection.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 5: Top

Figure 6: Bottom

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.2.2 Cisco Aironet 1562e/d/ps

Figure 7: Front

The silver ports are the external antenna ports. The other two are mentioned in Figure 1.

Figure 8: Back

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 9: Left

The covering screw hides the Power-In.

Figure 10: Right

The covering screw hides the console connection.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 11: Top

Figure 12: Bottom

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.2.3 Cisco Aironet 2802i and 3802i

Figure 13: Front

Figure 14: Back

From left to right: Console port, USB port, Ethernet port, POE port, Dc Power-In

Figure 15: Left

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 16: Right

Figure 17: Top

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 18: Bottom

2.2.4 Cisco Aironet 2802e and 3802e/p

Figure 19: Front

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 20: Back

From left to right: DC Power-In, POE port, Ethernet port, USB port, Console port.

Figure 21: Right

Figure 22: Left

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 23: Top

Figure 24: Bottom

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.2.5 Cisco Aironet 4800

Figure 25: Front

Figure 26: Back

From left to right: DC Power-In, POE port, 5 gig Ethernet port, 1 gig Ethernet Port, USB port, Console port

Figure 27: Right

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 28: Left

Figure 29: Top

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

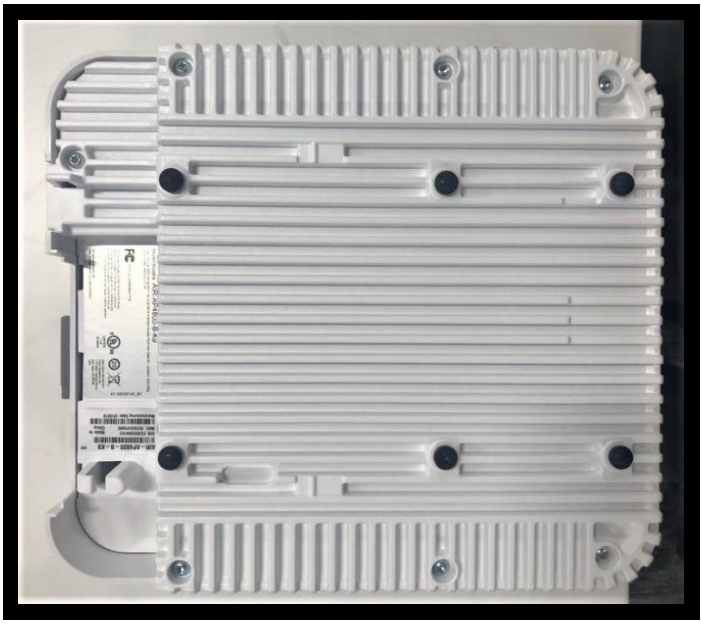

Figure 30: Bottom

2.3 Roles and Services

The module supports the roles of Crypto Officer and User. The CO role is fulfilled by the wireless LAN controller on the network that the module communicates with, and performs routine management and configuration services, including loading session keys and zeroization of the module. Role-based authentication is supported by the module. The User role is fulfilled by wireless clients. The module does not support a maintenance role.

CO Authentication

The Crypto Officer (Wireless LAN Controller) authenticates to the module through the CAPWAP protocol, using an RSA key pair with 2048 bits modulus, which has an equivalent symmetric key strength of 112 bits. 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-chance 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 9.7 x10^24 attempts per minute, which far exceeds the operational capabilities of the modules to support. The fastest network connection supported by the modules over Management interfaces is 1Gb/s. Hence, at most 1×10^9 × 60s = 6×10^10 = 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is:

1: (2^112 possible keys / ((6 × 10^10 bits per minute) / 112 bits per key))
1: (2^112 possible keys / 535,714,286 keys per minute)
1: 9.7 × 10^24

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

User Authentication

The module performs mutual authentication with a wireless client through EAP-TLS or EAP- FAST protocols. EAP-FAST is based on EAP-TLS and uses EAP-TLS key pair and certificates. The RSA key pair for the EAP-TLS credentials has modulus size of 2048 bits, thus providing 112 bits of strength. 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 chance 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 9.7 x10^24 attempts per minute, which far exceeds the operational capabilities of the modules to support. The fastest network connection supported by the modules over Management interfaces is 1Gb/s. Hence, at most 1×10^9 × 60s = 6×10^10 = 60,000,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is:

1: (2^112 possible keys / ((6 × 10^10 bits per minute) / 112 bits per key))
1: (2^112 possible keys / 535,714,286 keys per minute)
1: 9.7 × 10^24

.

Please notice that RSA used in CO role (RSA 2048 bits) or User role (RSA 2048 bits) authentication above only performs RSA signature verification. More information can be obtained in section 2.6 in this document.

User Services

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

Table 3: User Services (w = write, d = delete, x = execute)

Services & Access	Description	Keys & CSPs
Run Network Functions	MFP • Validating one AP with a neighboring AP's management frames using infrastructure MFP • Encrypt and sign management frames between AP and wireless client using client MFP	802.11 Pairwise Transient Key (PTK), 802.11 Group Temporal Key (GTK), 802.11 Key Confirmation Key (KCK) 802.11 Key Encryption Key (KEK), 802.11 Pairwise Transient Key (PTK) – (w, d, x)
	CCKM • Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP.	
	802.11 • Establishment and subsequent data transfer of an 802.11 session for use between the wireless client and the AP.	
Random Number Generator (SP800-90A)	Provide random bits when necessary for cryptographic functions.	Seed/entropy input, V, C, and Key – (w, x)

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Crypto Officer Services

The Crypto Officer services consist of the following:

Table 4: Crypto Officer Services (w = write, d = delete, x = execute)

Services & Access	Description	Keys & CSPs
Configure the AP	Configure the AP based on the steps detailed in section 3 (Secure Operation of the Cisco Aironet Access Points) of this document.	N/A
View Status Functions	View the configuration, routing tables, active sessions, memory status, packet statistics, review accounting logs, and view physical interface status.	N/A
Manage the AP	Log off users, view complete configurations, view full status, manage user access, update firmware and restore configurations.	N/A
Perform Self-Tests	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A
DTLS Data Encrypt	Enabling DTLS data path encryption between controller and AP.	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption Key (CAPWAP session key), DTLS Integrity Key, DTLS ECDSA private key, Infrastructure MFP MIC Key – (w, d, x)
Configure 802.11	Establishment and subsequent data transfer of an 802.11 session for use between the client and the access point.	802.11 Group Temporal Key (GTK), 802.11 Key Confirmation Key (KCK) 802.11 Key Encryption Key (KEK), 802.11 Pairwise Transient Key (PTK) – (w, d, x)
Cisco Root CA	Manufacturing CA for hardware identity.	RSA Public/Private Key pair – (x, d)
Cisco Mfg CA	Manufacturing CA for hardware identity.	RSA Public/Private Key pair – (x, d)
Random Number Generator (SP800-90A)	Provide random bits when necessary for cryptographic functions.	Seed/entropy input, V, C, and Key – (w, x)
Zeroization	Zeroize CSPs and cryptographic keys by calling cycling power (shutdown and reload) to zeroize all cryptographic keys stored in DRAM. The CSPs (Cisco Mfg CA publc key and Cisco root CA public key) stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed

2.4 Unauthenticated Services

The following are the list of services for Unauthenticated Operator:

System Status: An unauthenticated operator can observe the system status by viewing the LEDs on the module, which show network activity and overall operational status.
Power Cycle: An unauthenticated operator can power cycle the module. A solid green LED

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

indicates normal operation and the successful completion of self-tests.

The module does not support bypass capability.

2.5 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 2 physical security requirements. This section describes placement of tamper-evident labels on the module. The enclosure is production grade. Labels must be placed on the device(s) and maintained by the Crypto Officer in order to operate in a FIPS approved state. For FIPS 140 security level 2 scenarios, the tamper-evident labels are required to meet physical security requirements.

The APs (Access Points) are required to have Tamper Evident Labels (TELs) applied in order to meet the FIPS requirements. Specifically, AIR-AP-FIPSKIT= contains the necessary TELs required for the AP. The CO on premise is responsible for securing and having control at all times of any unused tamper evident labels. Below are the instructions to TEL placement on the AP's. There is no special preparation of the surface needed before applying the TELs.

2.5.1 Cisco Aironet 1562i Tamper Evident Label Placement

Figure 31: Tel Placement 1

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 32: TEL Placement 2

Figure 33: TEL Placement 3 and 4

Figure 34: TEL Placement 5

2.5.2 Cisco Aironet 1562e/d/ps Tamper Evident Label Placement

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 35: TEL Placement 1

Figure 36: TEL Placement 2

Figure 37: TEL Placement 3 and 4

Figure 38: TEL Placement 5

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.5.3 Cisco Aironet 2802i and 3802i Tamper Evident Label Placement

Figure 39: TEL Placement 1

Figure 40: TEL Placement 2

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 41: TEL Placement 3

Figure 42: TEL Placement 4

2.5.4 Cisco Aironet 2802e and 3802e/p Tamper Evident Label Placement

Figure 43: TEL Placement 1

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 44: TEL Placement 2

Figure 45: TEL Placement 3

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 46: TEL Placement 4

2.5.5 Cisco Aironet 4800 Tamper Evident Label Placement

Figure 47: TEL Placement 1

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

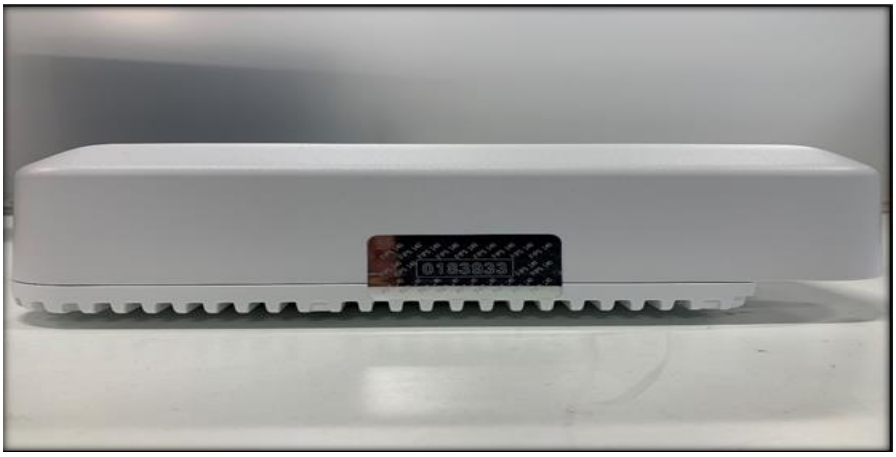

Figure 48: TEL Placement 2

Figure 49: TEL Placement 3

Figure 50: TEL Placement 4

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the security appliance cover. Because the tamper evident seals 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 seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word "OPEN" may appear if the label was peeled back.

The crypto officer is required to regularly check for any evidence of tampering. If evidence of tampering is found with the TELs, the module must immediately be powered down and all administrators must be made aware of a physical security breach.

NOTE: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

2.6 Cryptographic Algorithms

Approved Cryptographic Algorithms

The table below details the FIPS approved algorithms from each algorithm implementation. There are algorithm modes that were tested but are not used by the module. Table 5 only includes the algorithms, modes, and key sizes that are used by the modules.

Table 5 Approved Cryptographic Algorithms

Algorithm	Options	CiscoSSL FIPS Object Module	U-Boot
AES	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits AES-CCM: Key Lengths: 128, 256 bits AES-CMAC: Generation/Verification Key Lengths: 128, 256 bits AES-GCM: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits AES-KW: Modes: Decrypt, Encrypt Key Lengths: 128, 256 bits	5682	
SHS	CiscoSSL FIPS Object Module: SHA-1, SHA-256, SHA- 384, SHA-512 U-Boot: SHA-512	4554	3576

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

HMAC SHA	SHA-1, SHA-256, SHA-384, SHA-512	3783	
DRBG	SP 800-90A AES_CTR DRBG	2298	
RSA	CiscoSSL FIPS Object Module:: 186-4: Key Generation: Mod 2048 SHA: SHA-256 Mod 3072 SHA: SHA-256 Signature Generation 9.31: Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512 Signature Generation PKCS1.5: Mod 2048 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Signature Verification 9.31: Mod 2048 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512 U-Boot: 186-4: Signature Verification PKCS 1.5: MOD 2048 with Hash algorithm SHA-512	3057	2344

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

ECDSA	186-4: Key Pair Generation: Curves: P-256, P-384, P-521 Public Key Validation: Curves: P-256, P-384, P-521 Signature Generation: P-256 SHA: SHA-256, SHA-384, SHA-512 P-384 SHA: SHA-384, SHA-512 P-521 SHA: SHA-512 Signature Verification: P-256 SHA: SHA-256, SHA-384, SHA-512 P-384 SHA: SHA-384, SHA-512 P-521 SHA: SHA-512	1539	
CVL (SP800-135)	SSH KDF, TLS KDF	2074	
CVL (SP800-56A)	ECC CDH Curves: P-256, P-384, P-521	2073	
KBKDF (SP800-108)	Counter: MACs: HMAC-SHA-256	238	
CKG (SP800-133)	Vendor Affirmed		

- KTS (AES Cert. #5682; key establishment methodology provides 128 or 256 bits of encryption strength)
- KTS (AES Cert. #5682 and HMAC Cert. #3783; key establishment methodology provides 128 or 256 bits of encryption strength)

Note:

- The KDF (key derivation function) used in TLS and SSH protocol was certified by CAVP with CVL Cert. #2074.
- TLS and SSH protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
- Note that the TLS KDF CVL cert is listed because the module supports DTLS
- CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 4 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.
- There are algorithms, modes, and keys that have been CAVs tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/modulo shown in this table are implemented by the module.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Non-Approved but Allowed Cryptographic Algorithms

The module supports the following non-approved, but allowed cryptographic algorithms:

- Diffie-Hellman (CVL Cert. #2074, key agreement; key establishment methodology provides 112 bits of encryption strength);
- EC Diffie-Hellman (CVL Cert. #2073 with CVL Cert. #2074, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength)
- NDRNG

2.7 Cryptographic Key Management

Cryptographic keys are stored in either Flash or in DRAM for active keys.

The DTLS Pre-Master Secret is generated in the AP using the approved DRBG. The DTLS Pre-Master Secret is used to derive the DTLS Encryption and Integrity Key. All other keys are input into the module from the controller encrypted over a CAPWAP session. During a CAPWAP session, the APs first authenticate to the Wireless LAN controller. All traffic between the AP and the controller is encrypted in the DTLS tunnel. Keys such as the 802.11, CCKM and MFP keys are input into the module encrypted with the DTLS session key over the CAPWAP session. Key generation and seeds for asymmetric key generation is performed as per SP 800-133 Scenario 1. The APs rely on the embedded ACT2Lite module (Certificate #2125) for entropy output for use by the SP 800-90A DRBG and secure storage of the SUDI RSA2 certificates used for DTLS authentication. The number of seed bits entering ("seeding") the CTR_DRBG(AES-256) is 384 bits and number of bits output from the DRBG is 128 bits. The module does not output any plaintext cryptographic keys.

Table 6: Cryptographic Keys and CSPs

Key/CSP Name	Algorithm	Description	Storage	Zeroization
General Keys/CSPs				
DRBG entropy input	SP 800-90A CTR_DRBG	256 bit. HW based entropy source output used to construct seed	DRAM (plaintext)	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	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 hardware-based entropy source.	DRAM (plaintext)	Power cycle

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

DRBG V	SP 800-90A CTR_DRBG	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 during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plain text)	Power cycle
DRBG Key	SP 800-90A CTR_DRBG	256-bits DRBG key used for SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG	DRAM (plaintext)	Power cycle
Diffie-Hellman public key	Diffie-Hellman (Group 14)	2048 bits DH public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	224 bits DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	2048 bits DH shared secret derived in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19 and 20)	P-256, P-384 and P-521 public key used in EC Diffie-Hellman exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19 and 20)	P-256, P-384 and P-521 private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Power cycle
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19 and 20)	P-256 ,P-384 and P-521 shared secret derived in EC Diffie-Hellman exchange	DRAM (plaintext)	Power cycle
Cisco Mfg CA public/private key	rsa-pkcs1-sha2, rsa-9.31-sha2	Public/Private Key pair used with CAPWAP to authenticate the AP. This is the RSA public key (MOD2048, MOD3072) used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new keys

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Cisco Root CA public/private key	rsa-pkcs1-sha2, rsa-9.31-sha2	Public/Private Key pair used with CAPWAP to authenticate the AP This is the RSA public key (MOD2048, MOD3072) used for signature verification. This key is loaded into the module at manufacturing.	Flash (plain text)	Overwrite with new keys
DTLS				
DTLS Pre-Master Secret	Shared Secret	Computed as specified in SP 800-135 section 4.2	DRAM (plain text)	Power cycle
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to derive DTLS encryption key and DTLS integrity key.	DRAM (plain text)	Power cycle
DTLS Encryption Key (CAPWAP session key)	AES-CBC, AES-GCM	128 and 256 bit DTLS session Key used to protect CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	DRAM (plain text)	Power cycle
DTLS Integrity Key	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	Session key used for integrity checks on CAPWAP control messages. It is derived from DTLS Master Secret via key derivation function defined in SP800-135 (TLS).	DRAM (plain text)	Power cycle
DTLS public/private key	RSA	MOD-2048, MOD-3072 generated by calling the SP 800-90A CTR- DRBG.	Flash (plaintext)	Overwrite with new keys
Infrastructure MFP MIC Key	AES-CMAC, AES-GMAC	This 128 and 256-bit AES key is generated in the controller using approved DRBG. This key is sent to the AP encrypted with the DTLS encryption key. This key is used by the AP to sign management frames when infrastructure MFP is enabled.	DRAM (plain text)	Power cycle

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

802.11				
802.11 Pairwise Transient Key (PTK)	AES-CCM, AES-GCM	The PTK is the 128 or 256 bit 802.11 session key for unicast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle
802.11 Group Temporal Key (GTK)	AES-CCM, AES-GCM	The GTK is the 128 or 256 bit 802.11 session key for broadcast communications. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle
802.11 Key Confirmation Key (KCK)	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384,	The KCK is used to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key. Computed as specified in SP800-108.	DRAM (plain text)	Power cycle
802.11 Key Encryption Key (KEK)	AES Key Wrap	128 or 256 bit AES KEK. The KEK is used by the EAPOL-Key frames to provide confidentiality in the 4-Way Handshake and Group Key Handshake messages. This key is generated in the WLAN controller (outside the cryptographic boundary) and is transported into the module encrypted by DTLS Encryption Key.	DRAM (plain text)	Power cycle

Note 1: The KDF infrastructure used in DTLS was tested against the SP 800-135 TLS KDF requirements and was certified by CVL Cert. #2074.

Note 2: The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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.

2.8 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 insure all components are functioning correctly.

- Firmware Integrity Test (u-boot) RSA 2048 with SHA-512
- CiscoSSL FIPS Object Module algorithm implementation
    - AES (CBC, GCM) encryption KAT
    - AES (CBC, GCM) decryption KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-384 KAT
    - SHA-512 KAT
    - HMAC SHA-1 KAT
    - HMAC SHA-256 KAT
    - HMAC SHA-384 KAT
    - HMAC SHA-512 KAT
    - ECDSA sign and verify KATs
    - EC Diffie-Hellman "Z" primitive KAT
    - KBKDF KAT
    - RSA sign and verify KATs
    - SP 800-90A DRBG KAT
    - SP 800-90A Section 11 Health Tests

The access points perform all power-on self-tests automatically at boot. 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 LAN's interfaces; this prevents the AP's from passing any data during a power-on self-test failure.

Conditional Tests performed:

- Continuous Random Number Generator Test to FIPS-approved DRBG
- Continuous Random Number Generator Test to NDRNG (output from embedded ACT2Lite entropy source module validation certificate #2125)
- ECDSA pairwise consistency test
- RSA pairwise consistency test

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

3 Secure Operation of the Cisco Aironet Access Points

This section details the steps used to securely configure the modules. The administrator configures the modules from the wireless LAN controller with which the access point is associated. The wireless LAN controller shall be placed in FIPS 140-2 mode of operation prior to secure configuration of the access points.

The Cisco Wireless LAN controller Security Policy contains instructions for configuring the controller to operate in the FIPS 140-2 approved mode of operation. Crypto Officer Guidance - System Initialization.

The Cisco Aironet Access Points series security appliances were validated with firmware versions 8.10 and 16.12. These two are the only allowable images for use in FIPS. Configuring the module without maintaining the following settings will make the module be non-operational (Hard Error). Only after successful completion of all required FIPS POSTs and the initialization steps detailed below, will the module be considered to be in a FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

1. Configure CCKM (Cisco Centralized Key Management)

    a. CCKM is Cisco's wireless key management permitted by this security policy. It uses the same cipher suite as 802.11. The following controller CLI command configures CCKM on a given WLAN:

    > config wlan security wpa akm cckm enable index

    Refer to the Cisco Wireless LAN Controller Configuration Guide for additional instructions.

2. Connect AP to a Wireless Controller

    a. Establish an Ethernet connection to the AP Cryptographic Module and a Wireless LAN controller configured for the FIPS 140-2 approved mode of operation.

3. Set Primary Controller

    a. Enter the following controller CLI command from a wireless LAN controller with which the access point is associated to configure the access point to communicate with trusted wireless LAN controllers:

    > config ap primary-base controller-name access-point

    Enter this command once for each trusted controller. Enter **show ap** summary to find the access point name. Enter **show sysinfo** to find the name of a controller.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4. Save and Reboot

    a. After executing the above commands, you must save the configuration and reboot the wireless LAN controller:
       > save config
       > reset system

5. Tamper Seals
    a. Once Configuration is set, the CO shall place tamper evident seals according to Section 2.5 in this document.

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

4 Acronyms

CCKM	Cisco Centralized Key Management
MFP	Management Frame Protection

© Copyright 2019 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.