FIPS 140-2 Security Policy for Cisco Aironet CAP3602E and CAP3602I Wireless LAN Access Points

June 28, 2013
Version 1.4

Contents

This security policy contains these sections:

- Overview, page 2
- Physical Security Policy, page 4
- Secure Configuration, page 5
- Roles, Services, and Authentication, page 6
- Cryptographic Key Management, page 8
- Disallowed Security Functions, page 11
- Self Tests, page 11
- Obtaining Documentation, Support, and Security Guidelines, page 12

Cisco Systems, Inc.
www.cisco.com

Overview

The Cisco Aironet CAP3602E and CAP3602I (herein collectively called “the modules”) are wireless access points that support the IEEE 802.11a/b/g Wi-Fi standards for wireless LAN communications, and the CAP3602E and CAP3602I are 802.11n and 802.11n draft 2.0 WiFi CERTIFIED. The modules support the IEEE 802.11i standard for wireless LAN security. They are multiple-chip standalone cryptographic modules, compliant with FIPS 140-2 Level 2 requirements overall and Level 3 requirements for Design Assurance.

In the FIPS mode of operations, the modules support Control and Provisioning of Wireless Access Points (CAPWAP) and Management Frame Protection (MFP). CAPWAP, together with X.509 certificates, authenticates the module as a trusted node on the wired network. CAPWAP protects all control and bridging traffic between the controller and the modules with DTLS encryption. The modules secure all wireless communications with Wi-Fi Protected Access 2 (WPA2). WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. In the FIPS mode of operation, the modules use the following cryptographic algorithm implementations:

- AES CBC, ECB, CMAC and CCM (firmware)
- AES CBC, CMAC and CCM (hardware)
- AES CBC (hardware)
- SHA-1 (firmware)
- SHA-1 (hardware)
- HMAC SHA-1 (firmware)
- HMAC SHA-1 (hardware)
- X9.31 Random Number Generator (firmware)
- RSA Sign/Verify (firmware)

The modules also implement a non-Approved NDRNG used to seed the Approved RNG.

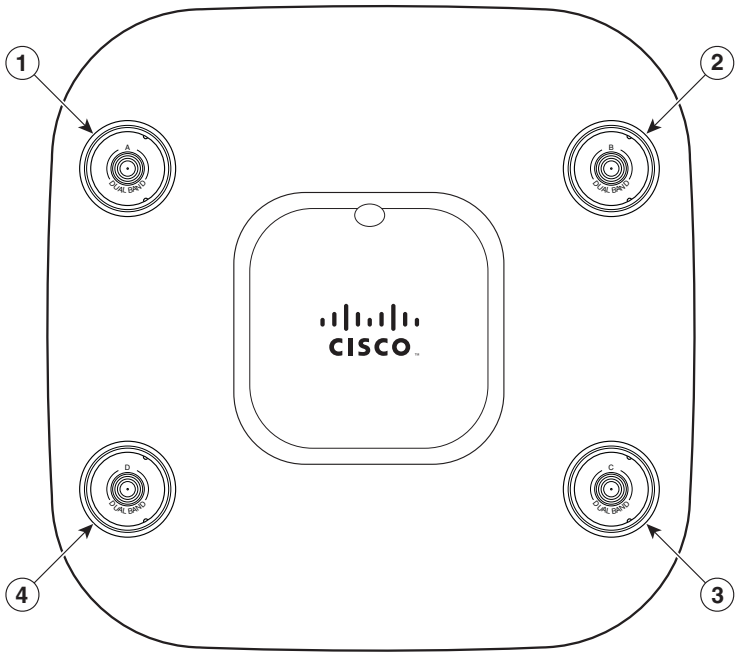
This document details the security policy for the CAP3602E and CAP3602I cryptographic modules. This document is non-proprietary and may be freely distributed.

The evaluated platforms are summarized in Table 1.

Table 1 Evaluated Platforms

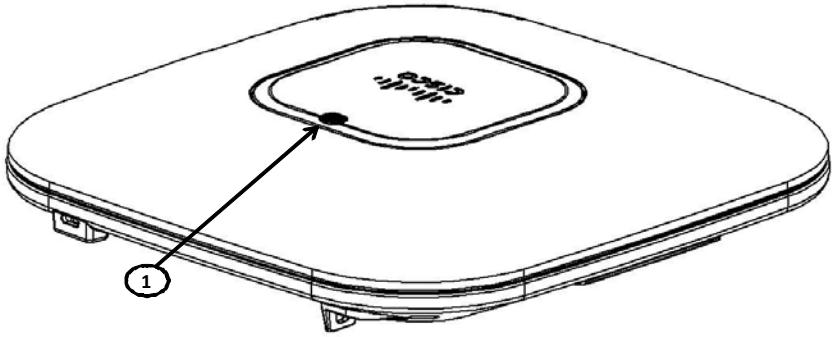
Model	Firmware Version	Hardware Revision
CAP3602E	7.2.103.0, 7.2.115.1, or 7.2.115.2	B0
CAP3602I	7.2.103.0, 7.2.115.1, or 7.2.115.2	B0

Figure 1 Access Point 3602E Model



1	Dual-band antenna connector A	**3**	Dual-band antenna connector C
2	Dual-band antenna connector B	**4**	Dual-band antenna connector D

Figure 2 Access Point 3602I Model



1	LED indicator

Physical Security Policy

This section describes placement of tamper-evident labels on the module. Labels must be placed on the device(s) and maintained by the Crypto Officer in order to operate in the FIPS approved mode of operation.

The cryptographic boundary of the Cisco Aironet 3602E and 3602I Access Points is defined by the hard outer casing, which surrounds all the hardware and firmware components.

The Crypto-Officer should inspect the seals for evidence of tamper as determined by their deployment policies (every 30 days is recommended). If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact Cisco.

Label Placement on the CAP3602E and CAP3602I

Remove any grease, dirt, or oil from the module by using alcohol-based cleaning pads, before applying the tamper-evidence labels. The chassis temperature should be above 10° C (50°F).

The seal placement is identical for the CAP3602E and CAP3602I (FIPS kit AIR-AP-FIPSKIT=, version B0): one (1) seal is placed underneath the bottom metal cover to prevent access to the Console port (see Figure 3). The FIPS kit also includes a metal guard, that goes over the Mode button. The metal guard physically prevents the Mode button from being pressed. The seal also covers the metal guard.

Figure 3 Seal Covering Console Port and Mode Button

Two (2) seals are placed over the specified two (2) screws on corners of the plastic module enclosure (see Figure 4) to prevent the screws from being removed without evidence of tamper and ensure that the enclosures are opaque. Three (3) seals are placed over the module connector slot to prevent access to the module.

Figure 4 Seals Covering Screws On Module Enclosure and Module Connector Slot

Secure Configuration

This section details the steps used to securely configure the modules to operate in FIPS 140-2 mode of operations. 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 operations 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.

Configure CCKM (Cisco Centralized Key Management)

CCKM is Cisco's wireless key management and is an optional mode permitted by this security policy. CCKM uses the same cipher suite as 802.11i; however, it has a slightly different key management scheme to support wireless client fast roaming between access points. Wireless client must comply with the updated CCKM specification described in CCXv5 in the FIPS mode of operation. 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.

Note The module does not participate in the CCKM key establishment but rather assists in passing data between the client and the RADIUS server.

Connect AP to a Controller

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

Set Primary Controller

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 operating in FIPS mode:

```
> 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.

Save and Reboot

After executing the above commands, you must save the configuration and reboot the wireless LAN controller:

```
> save config
> reset system
```

Roles, Services, and Authentication

This section describes the roles, services, and authentication types in the security policy.

Roles

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

Services

The services provided are summarized in Table 2.

Table 2 Module Services

Service	Role	Purpose
Self Test and Initialization	CO	Cryptographic algorithm tests, firmware integrity tests, module initialization. **Note** Module initialization can be obtained either by the CO resetting the access point remotely or by someone with physical access to the module manually cycling the power.
System Status	CO	Show the network activity and overall operational status.
Key Management	CO	Key and parameter entry, key output, key zeroization.
Module Configuration	CO	Selection of non-cryptographic configuration settings.
CAPWAP	CO	Establishment and subsequent data transfer of a CAPWAP session for use between the module and the CO.
802.11i	User, CO	Establishment and subsequent data transfer of an 802.11i session for use between the wireless client and the AP.
CCKM	User, CO	Establishment and subsequent data transfer of a CCKM session for use between the wireless client and the AP.
MFP	User, CO	• 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
DTLS data encrypt	CO	Enabling optional DTLS data path encryption for Office Extend APs.[1]

1. For further DTLS data configuration information, see the *Cisco Wireless LAN Controller Configuration Guide.*

An unauthenticated operator may observe the System Status by viewing the LEDs on the module which show network activity and overall operational status. A solid green LED indicates normal operation and the successful completion of self-tests. The module does not support a bypass capability in the approved mode of operations.

Crypto Officer Authentication

The Crypto Officer (Wireless LAN Controller) authenticates to the module through the CAPWAP protocol, using an RSA key pair with a 2048 bit modulus. NIST SP 800-57 defines this modulus size as having effective 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 $5.2x10^{28}$ attempts per minute, which far exceeds the operational capabilities of the module to support.

User Authentication

Users are authenticated to the module by means of the Temporal Key (TK). The TK portion of the 802.11i Pairwise Transient Key (PTK) is 128 bits. An attacker would have a 1 in 2^{128} 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 $3.4x10^{33}$ attempts per minute, which far exceeds the operational capability of the module to support.

Cryptographic Key Management

Cryptographic keys are stored in flash and in SDRAM for active keys.

The DTLS Pre-Master Secret is generated in the AP using the approved DRNG. The DTLS Pre-Master Secret is used to derive the DTLS Encryption and Integrity Keys. 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 using an RSA key pair. All traffic between the AP and the controller is encrypted in the DTLS tunnel. Keys such as the 802.11i, CCKM and MFP keys are input into the module encrypted with the DTLS session key over the CAPWAP session. The module does not output any plaintext secret or private cryptographic keys.

Table 4 lists the secret and private cryptographic keys and CSPs used by the module. Table 5 lists the public keys used by the module. Table 6 lists the access to the keys by service.

Table 3 Secret and Private Cryptographic Keys and CSPs

Name	CSP Type	Storage	Description and Zeroization
PRNG seed key	X9.31	SDRAM temporarily	This is the seed key for the PRNG. It is statically stored in the code and is zeroized when the controller image is erased during zeroization procedure.
PRNG seed	X9.31	SDRAM	This is the seed for the PRNG. It is generated using the reg_add_fresh_entropy function. It is zeroized during the zeroization procedure.

Table 3 Secret and Private Cryptographic Keys and CSPs (continued)

Name	CSP Type	Storage	Description and Zeroization
cscoIdCertPriv Key	RSA	Flash	This is the AP's RSA private key. It is zeroized during the zeroization procedure.
DTLS Pre-Master Secret	Shared secret	SDRAM	Shared secret generated by approved RNG for generating the DTLS encryption key.
DTLS Master Secret	Shared secret	SDRAM	Derived from DTLS Pre-Master Secret. Used to create the DTLS Encryption and Integrity Keys.
DTLS Encryption Key (CAPWAP Session Key)	AES-CBC	SDRAM	Session key used to encrypt and decrypt CAPWAP control messages.
DTLS Integrity Key	HMAC- SHA-1	SDRAM	Session key used for integrity checks on CAPWAP control messages.
Infrastructure MFP MIC Key	AES-CMAC	SDRAM	The 128 bit AES Key which is used to sign management frames when infrastructure MFP is enabled. It is zeroized during the zeroization procedure.
802.11i Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The PTK, also known as the CCMP key, is the 802.11i session key for unicast communications. This key also used to encrypt and sign management frames between AP and the wireless client. It is zeroized during the zeroization procedure.
802.11i Temporal Key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. It is zeroized during the zeroization procedure.
802.11i Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for broadcast communications. It is zeroized during the zeroization procedure.
Key Confirmation Key (KCK)	HMAC- SHA-1	SDRAM	HMAC-SHA-1 Key component of PTK.
Key Encryption Key (KEK)	AES-KeyWrap	SDRAM	AES Key Encryption Key component of PTK.
CCKM Pairwise Transient Key (PTK)	AES-CCM	SDRAM	The CCKM PTK is the CCKM session key for unicast communications. It is zeroized during the zeroization procedure.
CCKM Group Temporal Key (GTK)	AES-CCM	SDRAM	The CCKM GTK is the CCKM session key for broadcast communications. It is zeroized during the zeroization procedure.

Table 4 Public Keys

Name	Algorithm	Storage	Description and Zeroization
cscoDefaultNewRootCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the controller. It is zeroized during the zeroization procedure.
cscoDefaultMfgCaCert	RSA	Flash	Verification certificate, used with CAPWAP to authenticate the controller. It is zeroized during the zeroization procedure.
cscoIdCertPubKey	RSA	Flash	This is the AP's RSA public key.

Table 5 Key/CSP Access by Service

Service	Key Access
Self Test and Initialization	• Initializes PRNG Seed
System Status	• None
Key Management	• Read/Write Infrastructure MFP MIC Key, PTK, TK, GTK, KCK, KEK, CCKM PTK, CCKM GTK • Destroy all keys (with Key Zeroization command)
Module Configuration	• None
DTLS	• Uses cscoDefaultMfgCaCert, and cscoDefaultNewRootCaCert to authenticate Wireless controller • Generates DTLS Pre-Master Secret • Derives DTLS Master Secret • Derives the DTLS encryption and DTLS integrity keys to secure CAPWAP transactions between AP and Wireless controller
DTLS Data Encrypt	• Use DTLS Master Secret to derive DTLS Encryption Key and DTLS Integrity Key • Use DTLS Encryption Key and DTLS Integrity Key
CAPWAP	• Convey CSPs using DTLS, including: – Decrypt GTK and TK entry from the controller for 802.11i service – Decrypt CCKM PTK and GTK from the controller for CCKM service – Decrypt MFP MIC key entry from the controller for use in MFP service
802.11i	• Encrypt/decrypt using TK, GTK

Table 5 Key/CSP Access by Service (continued)

Service	Key Access
CCKM	• Encrypt/decrypt using CCKM PTK and GTK
MFP	• Sign AP management frames using Infrastructure MIC key • Encrypt and sign AP management frames using 802.11i PTK

Key Establishment

The module uses RSA key wrapping which provides 112-bits of effective key strength to establish 128-bit AES keys for DTLS. Keys are also entered into the module encrypted with the DTLS Encryption Key

Key Zeroization

All keys in the module may be zeroized by entering this command on the controller to which the access point is associated:

```
> config switchconfig key-zeroize ap ap-name
```

Disallowed Security Functions

These cryptographic algorithms are not approved, and may not be used in FIPS mode of operations:

- RC4
- MD5 (MD5 is allowed for use in DTLS)
- HMAC MD5

Self Tests

These self tests are performed by the modules:

- Firmware integrity test
- AES KAT (Firmware and Hardware)
- AES-CCM KAT (Firmware and Hardware)
- AES-CMAC KAT (Firmware and Hardware)
- SHA-1 KAT (Firmware and Hardware)
- HMAC SHA-1 KAT (Firmware and Hardware)
- RNG KAT (Firmware)
- RSA KAT (Firmware)
- Continuous random number generator test for Approved and non-Approved RNGs

Obtaining Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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