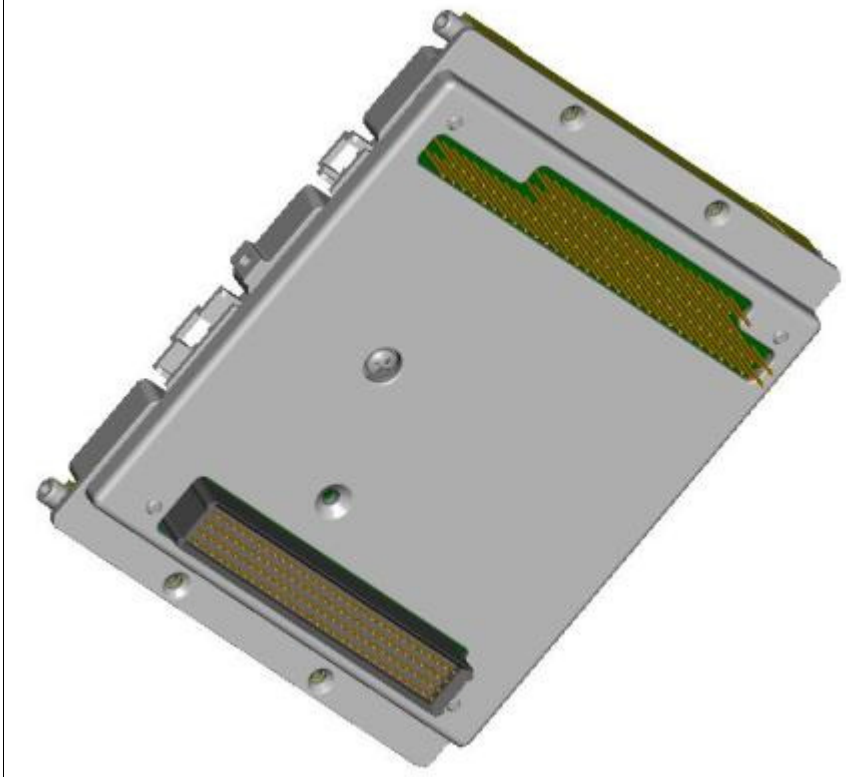
FIPS 140-2 Non-Proprietary Security Policy for

C3201WMIC-TPAK9 (802.11b/g Wireless Mobile Interface Card for the Cisco 3200 Series; with thermal plates)



Version 1.2
June 20, 2008

Table of Contents

Overview

The C3201WMIC-TPAK9 (802.11b/g Wireless Mobile Interface Card for the Cisco 3200 Series; with thermal plates), (herein called "the module" or the "WMIC") provides wireless connectivity for the Cisco 3200 Series Mobile Access Router. The module can be configured as 802.11g Wireless Access Point, 802.11g Wireless Root Bridge or 802.11g Wireless Work Group Bridge and supports the 802.11b/g wi-fi standards for communications, and 802.11i for security. It is a multiple-chip embedded cryptographic module, compliant with all requirements of FIPS 140-2 Level 2.

In the FIPS mode of operations, the module supports the Preshared Key (PSK) mode of authentication for network communications, and uses the following cryptographic algorithm implementations:

Algorithm	Certificate Number
AES	#370, #799
AES-CCM	#11
SHA-1	#797
HMAC-SHA-1	#439
X9.31 RNG	459

This document details the security policy for the C3201WMIC-TPAK9 WMIC with the Firmware Version S3201W7K9-12308JK (IOS Version 12.3(8)JK) and Hardware Version 800-25522-02.

Physical Security Policy

The Crypto Officer shall place tamper evident labels on the removable cover and on the radio according to the following steps (see pictures below for reference):

1. Remove any grease, dirt, or oil from the cover by using alcohol-based cleaning pads before applying the tamper evidence labels. The module temperature should be above 10° C (50° F).
2. Place a tamper evident label from the top to bottom thermal plate, near the center of the edge, opposite from the header connections on the site (see top label on Figure 1).
3. Place a tamper evident label on the side opposite the radio, covering the hole in the thermal plate (center label on Figure 2).

Figure1 - Placement of Tamper Evident Labels

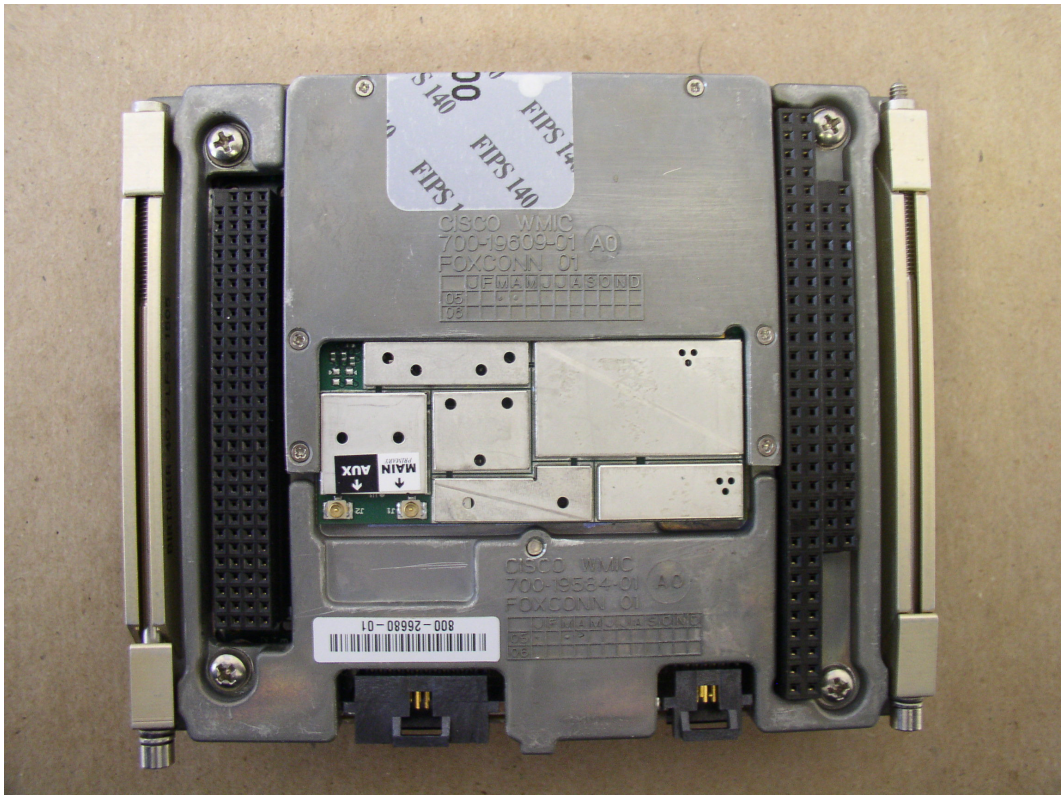
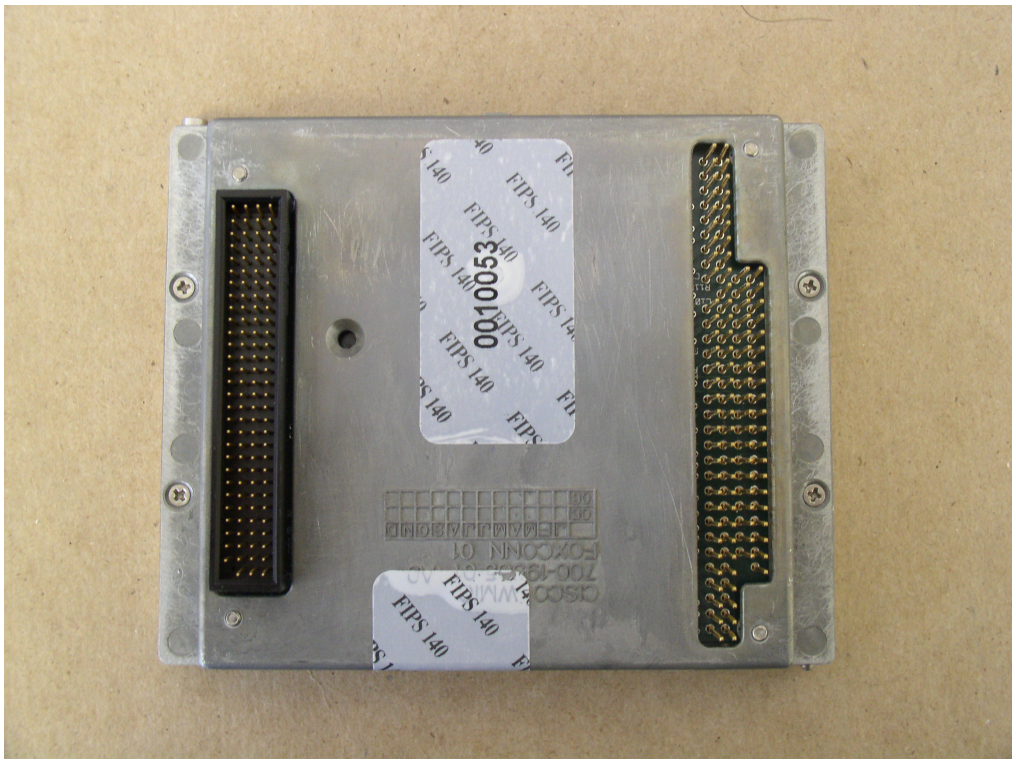


Figure 2 - Placement of Tamper Evident Labels



Roles, Services and Authentication

Roles

The module supports operator access via the local console port. Remote access is not permitted. The module supports role based authentication of Users and Crypto Officers, which are the only roles supported by the module. Only one Crypto Officers password can exist.

Services

All services can be viewed by typing "?" from within the appropriate roles. This command will show all the services available to the role currently logged in.

The services provided are summarized in Table 1. Additional detail is provided in the accompanying documentation, particularly in the Cisco 3200 Series Wireless MIC Software Configuration Guide.

Table 1 – Module Services

Service	Role	Purpose
Cryptographic Operations	User, Crypto Officer	Encryption and decryption of data in transit (using approved algorithms) via 802.11i with WPA2 in preshared key mode, WEP (not permitted in FIPS mode of operations).
Self Test	User, Crypto	Cryptographic algorithm tests Software integrity tests

	Officer	
System Status	User, Crypto Officer	The LEDs show the network activity and overall operational status
Key Management	Crypto Officer	Key and parameter entry Key output Key zeroization
Module Configuration	Crypto Officer	Selection of non cryptographic configuration settings
Module Debugging	Crypto Officer	Crypto officers can review all system parameters and values for troubleshooting

User Authentication

Passwords for all Users and Crypto Officers shall be configured to be 8 or more characters, including both numbers and letters. The Configure Authentication Data section describes the commands to set up the passwords. Following this guidance will result in a password space of 2.8 trillion possible passwords.

In addition, remote network connections are authenticated by means of a 256 bit Preshared Key (PSK). An attacker would have a 1 in 2^{256} change 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 $1.5x10^{72}$ attempts per minute, which far exceeds the operational capability of the module to support.

Secure Configuration

Configuration of the module shall be performed only over a local link via the console connection. The Crypto Officer must ensure that the PC that is used for console connection is a stand-alone or a non-networked PC. Remote access is not permitted.

The following steps shall be performed in order to prepare the secure configuration for the module. Following these steps shall ensure that the module operates in FIPS approved mode of operations, and that non-allowed algorithms are not used.

Configure Authentication Data

The enable secret (i.e. the password for the Crypto Officer) shall be selected to be 8 or more characters, including numbers and letters.

```
bridge> enable
Password:
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# enable secret [PASSWORD]
```

User password shall be set using:

```
bridge> enable
Password:
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# username name password 0 password
```

The user password shall be selected to be 8 or more characters, including numbers and letters.

These password strength requirements for the the enable secret and user password

Configure Ciphersuites for 802.11i

Only encrypted traffic can be processed by the module. The only 802.11i ciphersuite permitted is aes-ccm. Only encrypted traffic can be processed by the module. This may be set using the following command syntax:

```
bridge> enable
Password:
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface dot11Radio 0
bridge(config-if)# encryption mode cipher aes-ccm
```

Configure Pre-shared Keys for 802.11i

The only WPA2 mode permitted by this security policy is the Pre-shared Key (PSK) mode. Generation of pre-shared keys is outside the scope of this security policy, but they should be entered as 64 hexadecimal values (256 bits) by the following command syntax:

```
bridge> enable
Password:
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface dot11Radio 0
bridge(config-if)# ssid samplessid
bridge(config-if-ssid)# authentication open
bridge(config-if-ssid)# authentication key-management wpa
bridge(config-if-ssid)# wpa-psk hex 0 f42c6fc52df0ebef9ebb4b90b38a5f90
2e83fe1b135a70e23aed762e9710a12e
```

Disable Automatic Firmware Upgrades

The only IOS firmware image permitted in approved mode of operations is S3201W7K9-12308JK. To disable automatic firmware upgrades, run the following command:

```
bridge> enable
Password:
```

```
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# no boot upgrade
```

In addition to disabling automatic firmware upgrades, the Crypto Officer is not permitted a manual upgrade of the module firmware.

Cryptographic Key Management

Cryptographic keys are stored in flash (for long term keys and security parameters) and in SDRAM (for active RSNAs).

The PSK (aka PMK) is electronically input into the module in plain text by the CO over a local console connection. The GMK is generated in the module using X9.31 FIPS approved PRNG. All other keys (KCK, KEK, TK and GTK) are derived using the 802.11i Key derivation protocol. The GTK is output to the client encrypted with the KEK.

Table 2 shows the cryptographic keys and CSPs used by the module, and Table 3 shows the services that can access the keys and CSPs.

Table 2 – Cryptographic Keys and CSPs

Name	Algorithm	Storage	Description and Zeroization
PRNG seed	X9.31	SDRAM	This is the seed for X9.31 PRNG. It is updated periodically after the generation of 400 bytes – after this it is reseeded with router-derived entropy; hence, it is zeroized periodically. Also, the operator can reset the router to zeroize this CSP.
PRNG seed key	X9.31	SDRAM	This is the seed key for X9.31 PRNG. It is seeded with the output from a non-approved PRNG.
Enable secret	Shared secret	Flash	The obfuscated password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.
User password	Shared secret	Flash	Role based authentication data for a user. This password is zeroized y overwriting it with a new password.
PSK (aka PMK)	Shared secret	Flash	The 802.11i preshared key (PSK). In the evaluated configuration, the PSK is used as the pairwise master key (PMK). It is zeroized by overwriting with a new value.
ANonce	Random value	SDRAM	Authenticator nonce. Generated with Approved RNG during four-way handshake and zeroized when the handshake is complete.
802.11i Key Confirmation Key (KCK)	HMAC SHA-1	SDRAM	The KCK is used by IEEE 802.11i to provide data origin authenticity in the 4-Way Handshake and Group Key Handshake messages. Zeroized when the RSNA terminates.
Key Encryption Key (KEK)	AES	SDRAM	The KEK is used by the EAPOL (Extensible Authentication Protocol over LAN) Key frames to provide confidentiality in the 4-Way Handshake and

			Group Key Handshake messages. Zeroized when the RSNA terminates.
Temporal Key (TK)	AES-CCM	SDRAM	The TK, also known as the CCMP key, is the 802.11i session key for unicast communications. Zeroized when the RSNA terminates.
Group Master Key (GMK)	Random Value	SDRAM	The GMK is a precursor to the GTK i.e., GMK is used to derive GTK according to the 802.11i protocol. Zeroized when the RSNA terminates.
Group Temporal Key (GTK)	AES-CCM	SDRAM	The GTK is the 802.11i session key for multicast communications. Zeroized when the RSNA terminates.

Table 3 – Key/CSP Access by Service

Role	Service	Key Access
User/Crypto Officer	Cryptographic Operations	• Generate ANonce, GMK • Derive KCK, KEK, GTK and TK
	Self Test and Initialization	• Zeroize ANonce, KCK, KEK, TK, GMK and GTK • Initialize PRNG Seed
	System Status	• None
Crypto Officer	Key Management	• Read/Write PSK
	Module Configuration	• Read/Write User and Crypto Officer Passwords
	Module Debugging	• Read all module parameters

Disallowed Security Functions

The following cryptographic algorithms are not approved, and may not be used in FIPS mode of operations. Following the secure configuration steps above shall ensure that these algorithms are not used.

- RC4
- MD5
- HMAC MD5
- RSA

Self Tests

The following self tests are performed by the module:

- Firmware integrity test
- Power on self test of AES, AES-CCM, SHA-1, HMAC SHA-1 and X9.31 RNG algorithms
- Continuous random number generator test for Approved and non-approved RNGs.