## Table of Contents

- **Overview** ........................................................................................................... 3
- **Physical Security Policy** .................................................................................. 3
- **Roles, Services and Authentication** ................................................................. 5
  - **Roles** ............................................................................................................. 5
  - **Services** ........................................................................................................ 5
  - **User Authentication** ..................................................................................... 6
- **Secure Configuration** ....................................................................................... 6
  - **Configure Authentication Data** .................................................................. 6
  - **Configure Ciphersuites for 802.11i** ......................................................... 7
  - **Configure Pre-shared Keys for 802.11i** ..................................................... 7
  - **Disable Automatic Firmware Upgrades** ..................................................... 7
- **Cryptographic Key Management** ...................................................................... 8
- **Disallowed Security Functions** ......................................................................... 9
- **Self Tests** ........................................................................................................ 9
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:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Certificate Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>#370, #799</td>
</tr>
<tr>
<td>AES-CCM</td>
<td>#11</td>
</tr>
<tr>
<td>SHA-1</td>
<td>#797</td>
</tr>
<tr>
<td>HMAC-SHA-1</td>
<td>#439</td>
</tr>
<tr>
<td>X9.31 RNG</td>
<td>459</td>
</tr>
</tbody>
</table>

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).
Figure 1 - 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

<table>
<thead>
<tr>
<th>Service</th>
<th>Role</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Operations</td>
<td>User, Crypto Officer</td>
<td>Encryption and decryption of data in transit (using approved algorithms) via 802.11 with WPA2 in preshared key mode, WEP (not permitted in FIPS mode of operations).</td>
</tr>
<tr>
<td>Self Test</td>
<td>User, Crypto</td>
<td>Cryptographic algorithm tests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software integrity tests</td>
</tr>
</tbody>
</table>
### 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 $1 in 2^{256}$ 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 $1.5 \times 10^{72}$ 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 f42c6fc52df0ebe9ebb4b90b38a5f902e83fe1b135a70e23aed762e9710a12e
```

**Disable Automatic Firmware Upgrades**

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

```
bridge> enable
Password:
```
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Algorithm</th>
<th>Storage</th>
<th>Description and Zeroization</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRNG seed</td>
<td>X9.31</td>
<td>SDRAM</td>
<td>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.</td>
</tr>
<tr>
<td>PRNG seed key</td>
<td>X9.31</td>
<td>SDRAM</td>
<td>This is the seed key for X9.31 PRNG. It is seeded with the output from a non-approved PRNG.</td>
</tr>
<tr>
<td>Enable secret</td>
<td>Shared secret</td>
<td>Flash</td>
<td>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.</td>
</tr>
<tr>
<td>User password</td>
<td>Shared secret</td>
<td>Flash</td>
<td>Role based authentication data for a user. This password is zeroized by overwriting it with a new password.</td>
</tr>
<tr>
<td>PSK (aka PMK)</td>
<td>Shared secret</td>
<td>Flash</td>
<td>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.</td>
</tr>
<tr>
<td>ANoncex</td>
<td>Random value</td>
<td>SDRAM</td>
<td>Authenticator nonce. Generated with Approved RNG during four-way handshake and zeroized when the handshake is complete.</td>
</tr>
<tr>
<td>802.11i Key Confirmation Key (KCK)</td>
<td>HMAC SHA-1</td>
<td>SDRAM</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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.

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

**Table 3 – Key/CSP Access by Service**

**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.