



Rajant BreadCrumb ME4-2409  
Level 2, v11.4.0-FIPS  
FIPS 140-2 Non-Proprietary Security Policy

<http://rajant.com/>

Version 1.07

June 29, 2016

Cryptographic Module Validation Program

<http://csrc.nist.gov/groups/STM/cmvp/>

## Table of Contents

1 Introduction.....	4
1.1 Purpose.....	4
1.2 Module Identification.....	4
1.3 Security Level.....	5
1.4 Cryptographic Module Overview.....	6
1.4.1 Cryptographic Module Block Diagram.....	7
2 Modes of Operation.....	8
2.1 Non-FIPS 140-2 Compliant Mode of Operation.....	8
2.2 FIPS 140-2 Compliant Mode of Operation.....	9
3 Identification and Authentication Policy.....	10
3.1 Strength of Authentication Mechanisms.....	11
3.1.1 Crypto Officer, Administrator, Viewer.....	11
3.1.2 Peers.....	11
4 Access Control Policy.....	12
4.1 Cryptographic Keys and CSPs Employed.....	12
4.2 Service Matrix and CSP Access.....	14
5 Secure Operation and Rules.....	16
5.1 Security Rules.....	16
5.2 Physical Security.....	17
5.2.1 Application of the Tamper Evidence Material.....	17
6 External Views, Ports, and Interfaces.....	18
6.1 Logical Interface Mappings.....	19
7 Electromagnetic Interference / Electromagnetic Compatibility.....	20
8 Self-Tests.....	21
9 Mitigation of Other Attacks.....	23
10 Glossary.....	24

## Index of Tables

Table 1: Module Identification.....	4
Table 2: Security Level Requirements Met by Section of FIPS 140-2.....	5
Table 3: Non-FIPS-Approved Algorithms.....	8
Table 4: FIPS 140-2 Approved Algorithms.....	9
Table 5: Roles and Required Identification and Authentication.....	10
Table 6: Strength of Authentication Mechanism.....	11
Table 7: Cryptographic Keys and CSPs Employed.....	13
Table 8: CSP Access by Service.....	14
Table 9: External Views and Interfaces: ME4-2409 (enclosure is cryptographic boundary).....	18

# 1 Introduction

## 1.1 Purpose

The purpose of this document is to provide a specification of the Rajant BreadCrumb model ME4-2409 (the “module”) running firmware version 11.4.0-FIPS and to describe the security rules under which this model operates.

For convenience, the term “module,” “ME4,” and "BreadCrumb®" (the registered tradename for Rajant's overall product family) are used throughout this document to refer to this product.

## 1.2 Module Identification

Hardware Version / Model	Description	Firmware Version
ME4-2409	2 radios: 2.4 GHz and 900 MHz	11.4.0-FIPS

*Table 1: Module Identification*

### 1.3 Security Level

The modules described in this document are multi-chip standalone cryptographic modules as defined by the FIPS 140-2 standard. The cryptographic module meets security level 2 requirements overall. The following table indicates the security level requirements met by each section of FIPS 140-2.

Section	Name	Security 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 Interference / Electromagnetic Compatibility (EMI/EMC)	2
9	Self Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	<b>Overall:</b>	<b>2</b>

*Table 2: Security Level Requirements Met by Section of FIPS 140-2*

## 1.4 Cryptographic Module Overview

The BreadCrumb by Rajant Corporation is an 802.11 (Wi-Fi) and Ethernet compatible wireless mesh networking device that allows for rapid deployment of mobile wireless networks in a wide variety of environments. It is lightweight, capable of communicating via up to four different radio frequencies, and is designed to be completely mobile as carried by a vehicle or an individual. The BreadCrumb is powered by an external source. The BreadCrumb's cryptographic boundary is the physical enclosure of the device. The enclosures of the ME4 is fully depicted in Chapter 6 of this document.

BreadCrumb devices automatically detect other BreadCrumb devices and dynamically route packets through the resulting wireless mesh on behalf of commercially available off-the-shelf client devices. The module contains between 2 and 4 radios depending on model.

BreadCrumb devices can be used to provide instant wireless network coverage of areas with arbitrary shape and size and to extend and connect other networks with minimal configuration. Rajant's proprietary OSI layer two meshing protocol allows for rapid adaptation to moving infrastructure (e.g., networked ground and air vehicles) and provides redundant data paths in most configurations.

An example of the module's implementation in a meshed network is shown in the following figure. The ME4 is shown as one of various possible devices from the BreadCrumb product family, creating a meshed network for mobile implementations. The mobile network will reconfigure itself automatically as necessary to adapt to changing environments, connecting together peer devices as they are discovered.

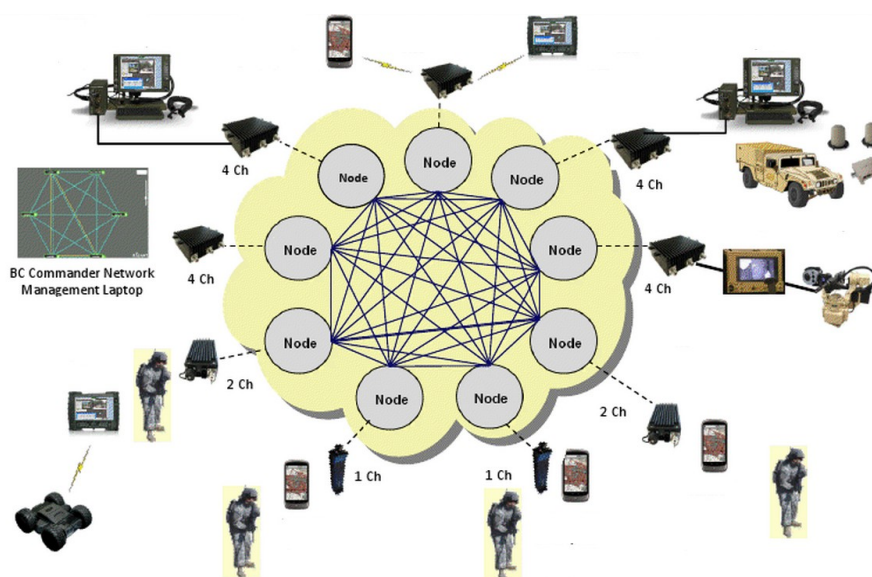


Figure 1: Example of ME4 deployment with other members of BreadCrumb® family

### 1.4.1 Cryptographic Module Block Diagram

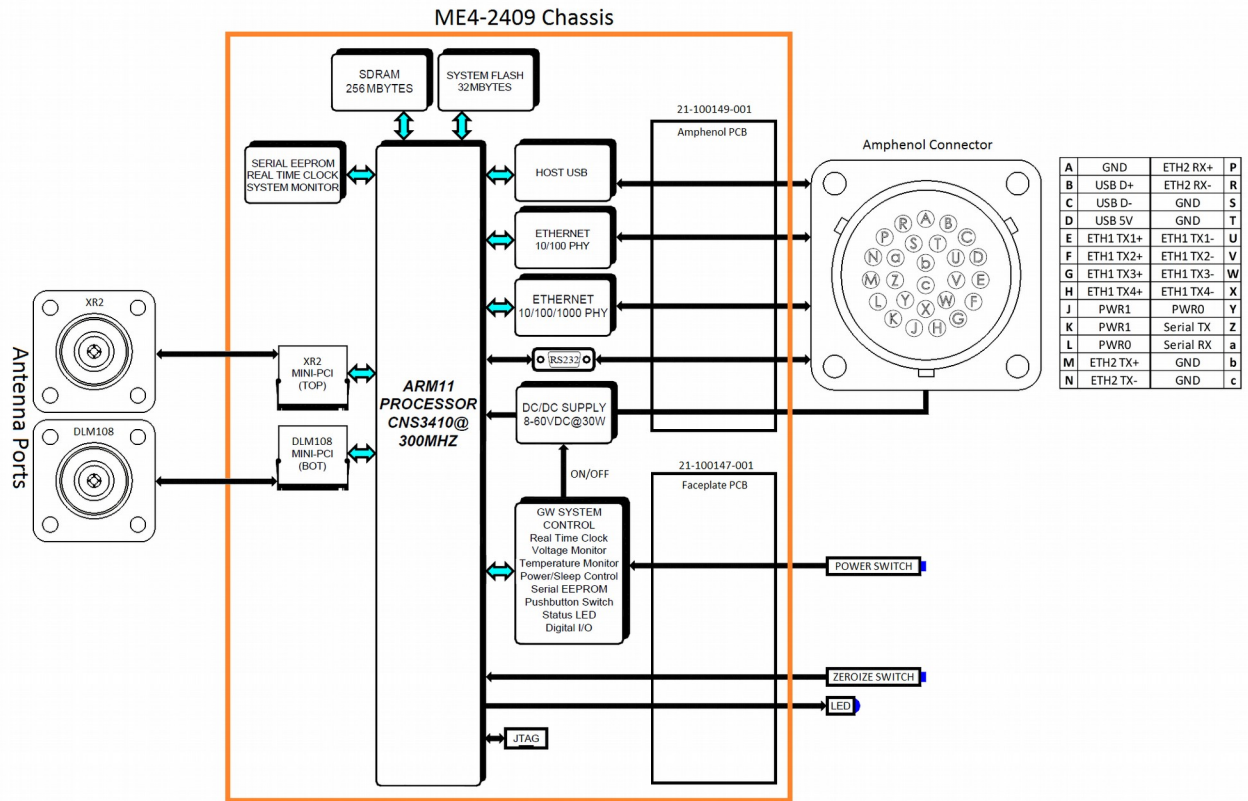


Figure 2: ME4-2409 Cryptographic Module Block Diagram

## 2 Modes of Operation

The default mode of operation for the module is FIPS 140-2 non-compliant. Only operators with Crypto Officer (CO) credentials can change the FIPS compliance mode of the module. Any changes to the module's FIPS compliance mode take effect after it is rebooted.

### 2.1 Non-FIPS 140-2 Compliant Mode of Operation

When the module is configured to work in non-FIPS 140-2 compliant mode, non-approved methods are enabled:

- Wireless clients (STAs) are allowed
- WEP authentication for STAs is allowed
- WPA Enterprise and WPA2 Enterprise authentication for STAs is allowed
- Non-Approved algorithms are allowed

Crypto Algorithm	Notes
RC4	Non-FIPS mode only
AES-TKIP	Non-FIPS mode only
AES-CCMP	Non-FIPS mode only
Camellia-CBC	Non-FIPS mode only
Triple-DES-CBC	Non-FIPS mode only
PBKDF2	Non-FIPS mode only

*Table 3: Non-FIPS-Approved Algorithms*



## 2.2 FIPS 140-2 Compliant Mode of Operation

The algorithms used by the module in FIPS 140-2 compliant mode are presented in the table below. FIPS 140-2 compliant mode is the validated mode of operation. This mode must be configured by the CO after power-up and is not activated until the module is rebooted. This mode will remain active across multiple reboots until reconfigured by a CO (after which another reboot is required to deactivate this mode), or until the module is zeroized.

FIPS 140-2 compliant mode is indicated through a distinct flashing patten of the Status LED. The LED's "FIPS-ON" pattern is shown approximately every five seconds in the form of a flashing magenta color repeating a cycle of 100 ms ON, 100 ms OFF, repeating as long as FIPS 140-2 compliant mode is enabled. Note: The LED itself must be enabled in order for this indicator to display.

Crypto Algorithm	Reference	Certificate #
AES-ECB (encrypt; key sizes: 128, 192, 256 bits)	NIST SP 800-38A	3445
AES-CBC (encrypt/decrypt; key sizes: 128, 256 bits)	NIST SP 800-38A	3445
AES-GCM (encrypt/decrypt; key sizes: 128, 192, 256 bits)	NIST SP 800-38D	3445
AES-CTR (encrypt; key sizes: 128, 192, 256 bits)	NIST SP 800-38A	3445
AES-GMAC (encrypt/decrypt; key sizes: 128, 192, 256 bits)	NIST SP 800-38D	3445
SHA1	FIPS 180-4	2845
HMAC-SHA1	FIPS 198-1	2194
SHA224	FIPS 180-4	2845
HMAC-SHA224	FIPS 198-1	2194
SHA256	FIPS 180-4	2845
HMAC-SHA256	FIPS 198-1	2194
SHA384	FIPS 180-4	2845
HMAC-SHA384	FIPS 198-1	2194
SHA512	FIPS 180-4	2845
HMAC-SHA512	FIPS 198-1	2194
RSA (2048-bit Key Generation)	FIPS 186-4	1765
RSADP Primitive	FIPS 186-4 RSA, RSADP	531
HMAC-based DRBG (SHA-512)	FIPS 198-1, NIST SP 800-90A	842
SP800-108 Counter Mode KDF	NIST SP 800-108	64
KDF 800-135 (TLS)	NIST SP 800-135	539

Table 4: FIPS 140-2 Approved Algorithms

Additional algorithms used in the approved mode are as follows:

- NDRNG (used to seed the DRBG with 640 bits of entropy)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)

### 3 Identification and Authentication Policy

The module supports three distinct operator roles: Crypto Officer (CO), Administrator, and Viewer. These roles are authenticated by role-specific passphrases. An additional system role assumed by other modules on the same network is the Peer. Peers authenticate to the module via a key derived from a shared network key (NK).

Default passphrases for each operator role and a default NK are assigned at the factory and post zeroization of the module. Default values are intended only to use for first-time CO authentication in a controlled environment, when they must be changed. The minimum passphrase length allowed is 8 characters. Concurrent logins are allowed. Different role/passphrase combinations used to log-in assure separation of roles during concurrent sessions.

Role	Type of Authentication	Authentication Data
Crypto Officer	Role based / passphrase	role name + SHA384(passphrase module-generated-nonce) (transmitted over TLS-encrypted link)
Administrator	Role based / passphrase	role name + SHA384(passphrase module-generated-nonce) (transmitted over TLS-encrypted link)
Viewer	Role based / passphrase	role name + SHA384(passphrase module-generated-nonce) (transmitted over TLS-encrypted link)
Peer	Role based via GMAC or HMAC via shared key using one of the following (configurable by CO): <ul style="list-style-type: none"> <li>• AES-GMAC 128</li> <li>• AES-GMAC 192</li> <li>• AES-GMAC 256</li> <li>• HMAC-SHA1</li> <li>• HMAC-SHA224</li> <li>• HMAC-SHA256</li> <li>• HMAC-SHA384</li> <li>• HMAC-SHA512</li> </ul>	GMAC or HMAC of exchanged data

*Table 5: Roles and Required Identification and Authentication*

### 3.1 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
passphrase	53 bits (minimum passphrase length, US keyboard character set) <sup>1</sup> 160 bits (minimum passphrase length, full Unicode character set) <sup>2</sup> This exceeds FIPS 140-2 requirements as described in section 3.1.1, below.
AES-GMAC 128	128 bits
AES-GMAC 192	192 bits
AES-GMAC 256	256 bits
HMAC-SHA1	256 bits
HMAC-SHA224	256 bits
HMAC-SHA256	256 bits
HMAC-SHA384	256 bits
HMAC-SHA512	256 bits

Table 6: Strength of Authentication Mechanism

#### 3.1.1 Crypto Officer, Administrator, Viewer

The minimum passphrase length is eight characters.

When a BCAPI client connects to a module, the module immediately generates and transmits a deterministically-generated, universally unique 80-bit nonce. The client responds with a role name (“view”, “admin”, or “co”, corresponding to the three operator roles listed above) and an authentication token computed by taking the SHA384 hash of the passphrase concatenated to the nonce. The session is permitted by the module to continue only if a valid response is received.

The probability of a successful passphrase guess in a single attempt using the character set described in <sup>1</sup> is  $1/(95^8)$ , which lower than  $1/1,000,000$  as required by FIPS 140-2 requirements. Each login attempt requires a new TLS connection which takes over one second to establish. At an impossible rate of 100 attempts per second, the odds of guessing are  $6,000/(95^8)$ , which is less than  $1/100,000$  as required by FIPS 140-2.

#### 3.1.2 Peers

When two modules establish Peer connections with one another, authentication is performed using a key derived from their shared Network Key set by the CO. The authentication mechanism is configurable by the CO and may use any of the algorithm/key size combinations listed in the table above.

1 Assuming a 95-element passphrase character set consisting of A-Z, a-z, 0-9, space, and the 32 special characters ! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } ; ' : " , . / < > ? \ | ` ~ , entropy calculation is  $\log_2(95^8) \approx 52.6$

2 Assuming the full 1,112,064 Unicode character set is used for passphrases, entropy calculation is  $\log_2(1,112,064^8) \approx 160.7$

## **4 Access Control Policy**

### ***4.1 Cryptographic Keys and CSPs Employed***

All stored keys are encrypted via the KEK using AES256-GCM, which includes authentication providing an integrity check.

Key/CSP	Type	Storage	Use	Roles & Access	Input / Generation	Output	Zeroization	Default Value
System HMAC Key	256-bit HMAC-SHA1	Plaintext in flash memory	Supports power-up system integrity test	CO, Admin, View (E)	Set at factory (constant)	N/A	N/A	N/A
KEK	256-bit AES-GCM	Plaintext in flash memory	Encrypts configuration and all following stored keys/CSPs prior to storage in flash memory	CO, Admin (E)	Generated HMAC-based DRBG (SHA-512)	N/A	Overwritten by zeros	N/A
NK	256-bit Key Production Key (SP800-108 KDF)	Encrypted by KEK in flash memory	Master key used to derive intermediate Key Production Keys	CO (W)	Manually supplied by CO	N/A	Unreadable following KEK zeroization	0 <sup>256</sup>
Intermediate KPKs (multiple)	256-bit Key Production Key (SP800-108 KDF)	Plaintext in RAM	Used to derive packet encryption, MAC encryption, and per-hop authentication keys	CO, Admin, Viewer, Peer (E)	Generated SP800-108 from NK	N/A	Overwritten by zeros	N/A
Packet Encryption Keys (multiple)	128,192,256-bit AES GCM 128,192,256-bit AES CTR	Plaintext in RAM	Encryption/decryption of mesh traffic	CO, Admin, Viewer, Peer (E)	Generated SP800-108 from Intermediate KPKs	N/A	Overwritten by zeros	N/A
MAC Encryption Keys (multiple)	128,192,256-bit AES GCM 128,192,256-bit AES CTR	Plaintext in RAM	Encryption/decryption of Ethernet MAC headers	CO, Admin, Viewer, Peer (E)	Generated SP800-108 from Intermediate KPKs	N/A	Overwritten by zeros	N/A
Per-Hop Authentication Keys (multiple)	128,192,256-bit AES-GMAC 512-bit HMAC-SHA1 512-bit HMAC-SHA224 512-bit HMAC-SHA256 1024-bit HMAC-SHA384 1024-bit HMAC-SHA512	Plaintext in RAM	Peer authentication and authentication of mesh traffic	CO, Admin, Viewer, Peer (E)	Generated SP800-108 from Intermediate KPKs	N/A	Overwritten by zeros	N/A
CO, Administrator, and Viewer Passphrases	Minimum 8-character Unicode	Encrypted by KEK in flash memory	Used to authenticate CO, Administrator, and Viewer roles	CO (W) CO, Admin, Viewer (E)	Manually Supplied by CO	N/A	Unreadable following KEK zeroization	breadcrumb-co breadcrumb-admin breadcrumb-view
TLS RSA Keypair	2048-bit RSA	Encrypted by KEK in flash memory	Used to accept TLS connections from CO, Administrator, or Viewer	CO, Admin, Viewer (E)	Generated NIST SP 800-90A DRBG	Public Key: shared during TLS negotiation Private Key: N/A	Unreadable following KEK zeroization	N/A
TLS Session Key (AES CBC)	Negotiated with TLS client per TLS specification (RSA Key Wrap, 2048-bit key)	Plaintext in RAM	Used to encrypt TLS session	CO, Admin, Viewer (E)	Negotiated with TLS client per TLS specification	N/A	Overwritten by zeros	N/A
HMAC DRBG internal state "V"	512-bit internal HMAC-SHA512 state "V" (SP 800-90A HMAC DRBG)	Plaintext in RAM	Internal working state of HMAC DRBG	CO (W)	0x00 <sup>64</sup> updated via HMAC update of entropy seed	N/A	Overwritten by zeros	N/A
HMAC DRBG internal state "Key"	512-bit internal HMAC-SHA512 state "Key" (SP 800-90A HMAC DRBG)	Plaintext in RAM	Internal working state of HMAC DRBG	CO (W)	0x01 <sup>64</sup> updated via HMAC update of entropy seed	N/A	Overwritten by zeros	N/A
HMAC DRBG internal state "seed"	640-bit entropy	Plaintext in RAM	Internal working state of HMAC DRBG	CO (W)	640-bit entropy set at system initialization	N/A	Overwritten by zeros	N/A

Table 7: Cryptographic Keys and CSPs Employed

**Note:** the TLS protocol has not been reviewed or tested by the CAVP and CMVP. Please see NIST document SP800-131A for guidance regarding the use of non FIPS-approved algorithms.

## 4.2 Service Matrix and CSP Access

The following table lists the services provided by the module, the roles authorized to access those services, and the related CSPs for each service. Individual CSPs are described in detail in the next section.

Role(s)	Service	Cryptographic Keys and CSPs	Access (R=Read, W=Write, E=Execute/Use)
CO	Enable/disable FIPS-compliant mode	FIPS compliant configuration setting	RW
CO	Set passphrases	co, admin, viewer passphrases	W
CO	Set Network Key	Network Key	W
CO	Enable/disable/configure packet encryption, MAC encryption, per-packet authentication	packet encryption, MAC encryption, per-packet authentication settings	RW
CO	Trigger internal automatic key generation via power up: Generate KEK and RSA keypair, derive internal keys from Network Key	KEK, RSA keypair, Network Key, HMAC DRBG internal states "V" and "Key"	W (KEK) W (RSA keypair, HMAC DRBG internal states) E (Network Key)
CO	Zeroize	all passphrase, key, and configuration data	E
CO	Initiate self-tests via power cycle	System HMAC Key	E
CO, Administrator	Zeroize via remote BAPI connection	all passphrase, key, and configuration data	E
CO, Administrator	Configure non-cryptographic module parameters	all configuration data except passphrases and keys	RW
CO, Administrator	Initiate self-tests via remote reboot	System HMAC Key	E
CO, Administrator	Encrypt configuration (automatic internal operation performed upon save of configuration data)	KEK	E
CO, Administrator, Viewer	Establish TLS sessions for configuration and monitoring	RSA keypair, passphrases, TLS session key	E R (RSA public key)
CO, Administrator, Viewer	Show status via remote BAPI connection	all configuration data except passphrases and keys	R
Peer	Encrypt/decrypt mesh traffic	NK, intermediate KPK, and packet encryption keys	E W (KPK and packet encryption keys upon first use)
Peer	Encrypt/decrypt Ethernet MAC header	NK, intermediate KPK, and MAC encryption keys	E W (KPK and MAC encryption keys upon first use)
Peer	Authenticate mesh traffic	NK, intermediate KPK, and per-hop authentication keys	E W (KPK and per-hop authentication keys upon first use)
Peer	Send/receive data through mesh	NK and derived keys	E

Table 8: CSP Access by Service

The following unauthenticated services require physical access to the module:

- Zeroize via zeroize button or USB
- Show status via LED
- Initiate self-tests via power cycle

## 5 Secure Operation and Rules

### 5.1 Security Rules

The Crypto Officer must perform the following steps for modules that are newly “out of the box” or have been zeroized:

1. Ensure FIPS-validated firmware version 11.4.0-FIPS is installed.
2. Apply tamper evidence (Loctite) as specified in Section 5.2.1. **The Loctite shall be installed for the module to operate in a FIPS-Approved mode of operation.**
3. Enable FIPS compliant mode.
4. Change the default passphrases for CO, Administrator, and Viewer roles.
5. Change the default Network Key.
6. Enable Per-Packet Encryption.
7. Enforce a strong passphrase policy and change passphrases on a regular basis.
8. Inspect module regularly for damage, intrusion, and tampering.
9. Assure that the module is installed in a secure location in a secure manner.
10. Assure that access to the module is restricted to authorized personnel.
11. Use a trusted host for remote administration and monitoring.
12. Inspect newly-arrived modules.
13. Regularly verify that the firmware is not indicating any errors. This can be performed remotely via BCAPI or visually at each module by observing a period red blinking pattern on the status LED.
14. Regularly verify that the firmware installed is in FIPS compliant mode. This can be performed remotely via BCAPI or visually at each module by observing a periodic magenta blinking pattern on the status LED.
15. Regularly inspect the tamper evidence labels to verify that they are intact.
16. Zeroize modules prior to terminating a network configuration.
17. Zeroize modules prior to sending to factory for repairs.
18. Ensure that the Network Key is given only to trusted Crypto Officers.

The Crypto Officer is responsible for verifying that the module is in FIPS mode as indicated by the periodically blinking MAGENTA Status LED. This should be verified before use and regularly verified during continued use.



## **5.2 Physical Security**

The module's hardware is manufactured to meet FIPS 140-2 Level 2 physical security requirements. The module is enclosed in a hard aluminum metal casing and cannot be opened without specialized tools. There is no opening in the casing to give any visual or physical access to internal components. The module must be located in a controlled access area.

The tamper evidence is provided by the use of a cyanoacrylate material (Loctite® 425, mfg. Part no. 42540, available from Rajant) covering the chassis access screws. Screws requiring application are indicated in the appendices to this document.

### **5.2.1 Application of the Tamper Evidence Material**

The CO role shall be responsible for application of tamper evidence seals, periodic verification that installed seals have not been tampered with, and securing and having control at all times of any unused tamper evidence (cyanoacrylate) material.

Cyanoacrylate material should be applied in a clean environment at room temperature. Unpack the module and place it on a flat surface. Observe views of the module in the next section of this document to select screws to which material is to be applied (note blue indicator over seven (7) screws in figures). Using alcohol, clean well the chassis areas around the screws and wait until completely dry. Use cyanoacrylate material from container packed with the module. Shake the container. To open the container make a diagonal cut at the tip of its applicator.

Apply three to four drops of the sealant on each of the seven (7) screws marked in the diagrams so that sealant completely covers the drive slot and flows around the screw head and adheres to chassis around the screw. Wait until dry.

Note: for full curing leave module at room temperature for four hours.

## 6 External Views, Ports, and Interfaces

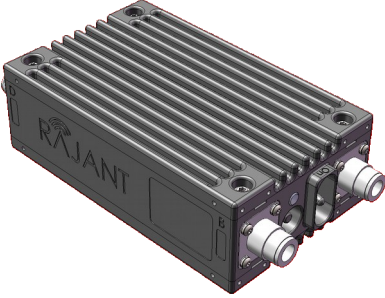
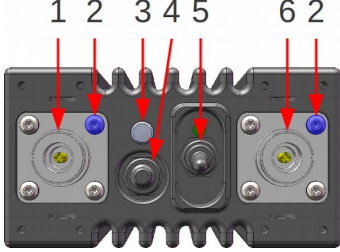
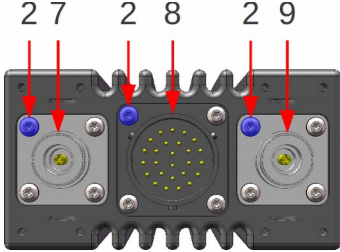
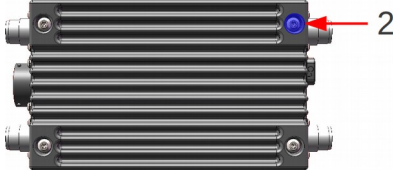
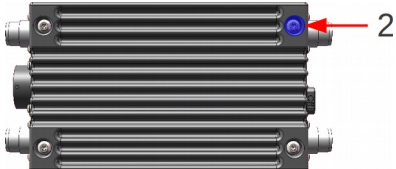
Crypto Module Views	Notes
	<p>General View: ME4-2409            Dimensions: 7.46" L x 3.75" W x 2.00" H            Tamper-resistant / tamper-proof through "Loctite" applied over screws.</p>
	<p>Front View</p> <ul style="list-style-type: none"> <li>1 – Type N female antenna connector (not used)</li> <li>2 – Loctite treated screw</li> <li>3 – Status LED</li> <li>4 – LED Configuration / Zeroize Keys and Restore Factory Defaults Switch</li> <li>5 – Power Switch</li> <li>6 – Type N female antenna connector (not used)</li> </ul>
	<p>Back View</p> <ul style="list-style-type: none"> <li>2 – Loctite treated screw</li> <li>7 – Type N female antenna connector (2.4 GHz Radio)</li> <li>8 – 26-Pin Amphenol Connector</li> <li>9 – Type N female antenna connector (900 MHz Radio)</li> </ul>
	<p>Top View</p> <ul style="list-style-type: none"> <li>2 – Loctite treated screw</li> </ul>
	<p>Bottom View</p> <ul style="list-style-type: none"> <li>2 – Loctite treated screw</li> </ul>

Table 9: External Views and Interfaces: ME4-2409 (enclosure is cryptographic boundary)

## 6.1 Logical Interface Mappings

<b>FIPS 140-2 Logical Interface</b>	<b>Physical Interface</b>
Data Input	wlan0,wlan1, eth0, eth1, USB
Data Output	wlan0,wlan1, eth0, eth1, USB
Control Input	wlan0,wlan1, eth0, eth1, USB, zeroize & status button
Status Output	wlan0,wlan1, eth0, eth1, USB, status LED

## 7 Electromagnetic Interference / Electromagnetic Compatibility

The FCC accredited laboratory used by Rajant for compliance testing of the BreadCrumb equipment is:

MET Laboratories, Inc.  
914 W. Patapsco Avenue  
Baltimore, MD 21230  
tel. 410-354-3300

The modules are FCC-compliant (Part 15, Subpart J, Class B) hardware platforms that satisfy FIPS PUB 140-2 security level 2 hardware requirements.

The FCC Product ID for the ME4-2409 is **FCC ID VJA-ME4-2409**

## 8 Self-Tests

The module provides self-tests both on power-up and conditionally. If a self-test fails then the module will enter a nonoperative error state. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions. Each error has a numeric code which is indicated externally via a blink pattern on the Status LED. For example, if the error number is 412, then the RED Status LED will blink four times (for the digit “4”), then pause, then blink once (for the digit “1”), then pause, then blink twice (for the digit “2”), followed by a longer pause. The sequence will then repeat.

Below are the possible FIPS error conditions that can occur as a result of self-tests and the associated numeric error codes:

Code	Error
41	FIPS power-on self-tests failed
411	FIPS DRBG power-on self-test failed
412	FIPS DRBG continuous test failed
413	FIPS DRBG health check failed
414	Kernel integrity check failed
415	File system integrity check failed
419	Pairwise consistency test failed

The power-up self tests consist of:

- Kernel integrity check (HMAC-SHA1)
- File system integrity check (HMAC-SHA1)
- Known answer tests for the following cryptographic functions:
  - AES-GCM (key sizes: 128, 192, 256 bits)
  - AES-CTR (key sizes: 128, 192, 256 bits)
  - AES-CBC (key sizes: 128, 256 bits)
  - AES-GMAC (key sizes: 128, 192, 256 bits)
  - HMAC-SHA-1
  - HMAC-SHA-224
  - HMAC-SHA-256
  - HMAC-SHA-384
  - HMAC-SHA-512
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384

- SHA-512
- DRBG
  
- RSA Pairwise Consistency Test (Key Generation)

Conditional tests consist of:

- CRNGT for NDRNG
- DRBG continuous test (confirming no repeated blocks)
- DRBG health check (run once every 1<<24 DRBG “generate()” operations)
- RSA Pairwise Consistency Test (run when new keys are created)
- Manual Key Entry Test; CO’s key entry is validated by dual entry test upon manual entry in BC| Commander management application.

## **9 Mitigation of Other Attacks**

The module is not designed to mitigate other attacks.

## 10 Glossary

<b>Term/Abbreviation</b>	<b>Description</b>
BCAPI	BreadCrumb Applications Programming Interface, a protocol for managing and monitoring Rajant BreadCrumb devices over a network.
BreadCrumb	Generic name for Rajant's wireless mesh networking devices, including the module of interest in this document (ME4-2409)
CO	Crypto Officer
CRNGT	Continuous Random Number Generator Test
DRBG	Deterministic Random Bit Generator
KEK	Key Encryption Key
KPK	Key Production Key
ME4	Name for a specific form factor in Rajant's BreadCrumb product line, including the ME4-2409 described in this document.
NDRNG	Nondeterministic Random Number Generator
NK	Network Key, a shared key installed on BreadCrums by a Crypto Officer from which other keys are derived.
STA	An 802.11 (Wi-Fi) wireless client station
TLS	Transport Layer Security, a cryptographic protocol for secure Internet communication
WEP	Wired Equivalent Privacy, a wireless network security standard for communications between Wi-Fi access points and clients.
WPA	Wi-Fi Protected Access, a wireless encryption standard for communications between Wi-Fi access points and clients.