ME3-24 Level2 v10.13

Non-Proprietary Security Policy

Version: 1.07
Date: October 29, 2010

Corporate Headquarters
Rajant Corporation
400 East King Street
Malvern, PA 19355
Tel: (484) 595-0233
Fax: (484) 595-2444

http://www.rajant.com

1. INTRODUCTION **3**
1.1 Purpose 4
1.2 Module Identification 4
1.3 Module Description. 4
2. MODES OF OPERATION **7**
2.1 Non-FIPS140-2 Compliant Mode of Operation. 7
2.2 FIPS140-2 Compliant Mode of Operation 7
3. PORTS AND INTERFACES **10**
4. IDENTIFICATION AND AUTHENTICATION POLICY **13**
4.1 Assumption of roles 13
5. ACCESS CONTROL POLICY **15**
5.1. Roles supported by cryptographic module 15
5.2. Services provided by cryptographic module 16
5.3. Cryptographic Keys and CSPs Employed by Cryptographic Module 17
5.4 Zeroization 23
5.5 Initialization / Factory defaults 25
6. OPERATIONAL ENVIRONMENT **26**
7. SECURITY RULES **27**
7.1 Secure Configuration of the Module 27
7.2 Secure Operation. 28
7.3 Setting FIPS Mode 30
8. PHYSICAL SECURITY **32**
8.1 Physical Security Mechanisms. 32
9. SELF-TESTS **35**
10. MITIGATION OF OTHER ATTACKS POLICY **37**
11. ACRONYMS **38**

1. INTRODUCTION

The ME3-24 BreadCrumb® by Rajant Corporation is a wireless mesh networking device that allows for rapid deployment of mobile wireless networks. 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 (IEEE 802.11a, 802.11b, 802.11g, and Ethernet).

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 and provides redundant data paths in most configurations.

Although this document focuses on the ME3-24 BreadCrumb® model, Rajant provides a number of different models capable of communicating with one another. The following figure illustrates a typical BreadCrumb® network consisting of Rajant's SE, ME, XL, and WE models. Functionally as networking modules these devices are equivalent. Applicability of each is determined by its power and range. WE modules are lightweight units worn by personnel on the ground, ME modules are used on aerial and small vehicles, XL modules are used as rugged long-range mesh nodes, and SE modules are used as shorter-range mesh nodes. This creates a mobile meshed network that is constantly reshaping and adapting to changing conditions.

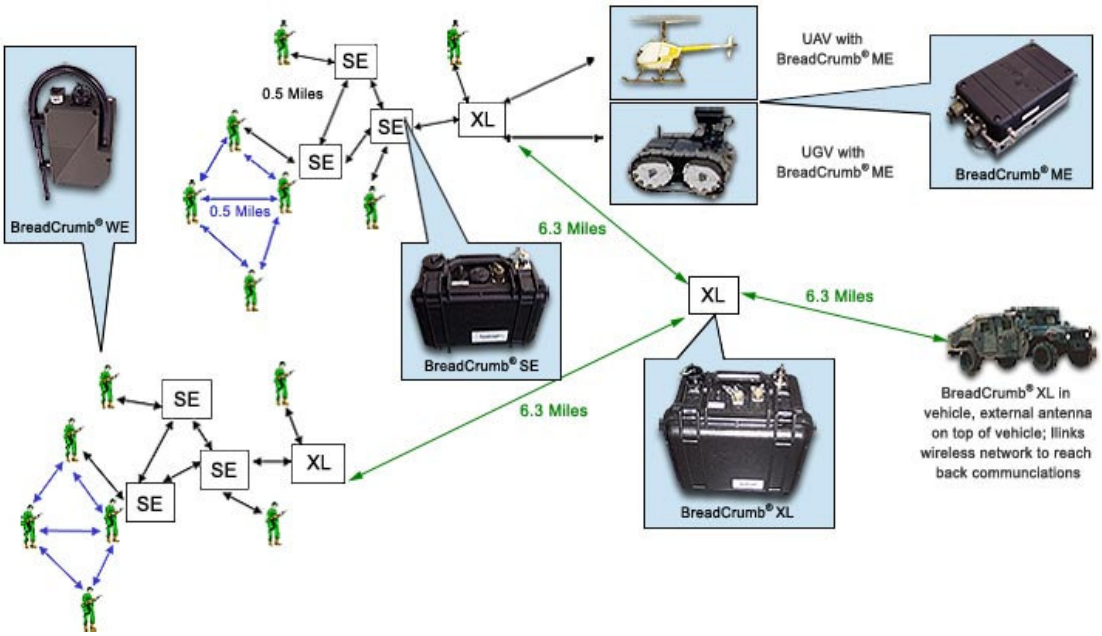

Figure 1.1: Example BreadCrumb® Device Deployment

Data is encrypted over two types of links: *STA links* are wireless client device connections; that is, an 802.11a, b, or g wireless association between a client device and a BreadCrumb® device. *Peer links* are links automatically established and maintained between BreadCrumb® devices. Data communications between client devices may pass through any number of peer links, including zero (in the event that both client devices are associated to the same BreadCrumb® device).

In this document, the term "BreadCrumb® device" includes both the ME3-24 and other BreadCrumb® models.

1.1 Purpose.

The purpose of this document is to provide a specification of the ME3-24 and describe the rules under which the module operates.

1.2 Module Identification.

Hardware Version / Model: ME3-24 BreadCrumb®
Software / Firmware version: Ver. 10.13

1.3 Module Description.

The Rajant Corporation ME3-24 is a multi-chip standalone cryptographic module 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	3
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	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	2
	Overall	**2**

Table 1.1: ME3-24 Security Level Requirements Met

The casing of the module is a 2-part sealed aluminum case with no openings or doors.

Its major internal components are:

- Cambria GW2350 SBC with 2 on-board Ethernet controllers, 32MB flash, 128MB SDRAM, 2 USB ports, discrete digital IO, and a Type III Mini-PCI socket.
- Mini-PCI wireless controller – Ubiquiti XR2 module
- Power conversion board
- Battery board with internal Battery and Battery charger circuitry
- Switch board for interconnections between SBC and peripheral connectors

External access to module is through components mounted on front of casing:

- 18pin Amphenol connector provides interfaces for:
    - Power port to connect external battery or power supply
    - 2 Ethernet ports for clear-text connections
    - USB port used for upgrades
- Wlan antenna used for wireless / encrypted traffic
- Pushbutton switch is used for module reset / zeroization.
- Status LED displays the internal status of the module through patterns of flashes and colors.

Ethernet interfaces provide a "clear text zone" in which no encryption is provided by the ME3-24 (with the exception of administrative communications via TLS encryption). These interfaces are expected to be connected to a trusted network, and may be disabled entirely by an administrator.

A wlan interface creates up to four 'Encrypted Zones' (via up to four ESSIDs) where all traffic is expected to be encrypted. The architecture of the module as a hardware device is supplemented by functionality of the operating system and a set of software programs and applications used to implement its design. The module's software resides on internal flash disk and provides a mobile network infrastructure capable of assuring secure connectivity to external devices over an extended area. To implement such a network, the module uses 'Peer' interfaces which allow modules from the BreadCrumb® family to

associate into groups capable of routing incoming external traffic throughout an area covered by the network. In addition to client and peer to peer traffic, separate communications are used to allow for CO and Administrator sessions to setup, monitor, and audit the module's functions.

The module can be configured to work in FIPS140-2 compliant or FIPS140-2 non-compliant mode. Descriptions of these modes and of the module's functionality are presented in the following chapters.

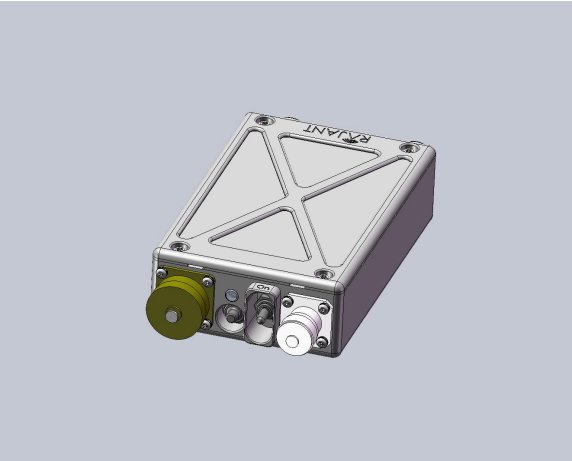

Figure 1.2: External view of the ME3-24 module.

This model may be worn by an individual, be attached to a vehicle, or be installed as a static infrastructure for a wide variety of networking applications. Regardless of the application, the physical configuration of the ME3-24 is the same.

2. MODES OF OPERATION

The default mode of operation for the ME3-24 module is FIPS 140-2 non-compliant. Only operators with Crypto Officer 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 compliant mode, non-approved methods are enabled.

When in non-FIPS compliant mode:

- WEP authentication for STAs is allowed,
- WPA Enterprise and WPA2 Enterprise authentication for STAs is allowed,
- TKIP encryption for STAs is allowed,
- The internal crypto libraries are switched to non-FIPS mode,
- Power-up initializations do not execute any FIPS-required power-up self-tests and
- Peer-to-Peer communications are allowed unencrypted and without authentication.

Crypto Algorithm	Notes
RC4	Non-FIPS mode only
MD5	Non-FIPS mode only
Diffie-Hellman	Non-FIPS mode only

Table 2.1 Non FIPS-approved algorithms

2.2 FIPS140-2 Compliant Mode of Operation.

The algorithms used by the module in FIPS140-2 compliant mode are presented in table 2.2 below. FIPS compliant mode is the 'Approved' mode of operation. FIPS mode must

be configured by the Crypto-Officer after power-up and is not activated until the device is rebooted. FIPS mode will remain active across multiple reboots until reconfigured by a Crypto Officer, after which another reboot is required to deactivate FIPS mode.

FIPS 140-2 compliant mode is indicated through a distinct flashing pattern of the Output Status LED. The LED's 'FIPS-on' pattern is shown every 5sec in form of a flashing magenta color with period of 100ms ON -100ms OFF: repeating as long as FIPS140-2 mode is enabled.

Crypto Algorithm	Cert #
AES CBC, and CFB	1300
AES ECB, and CCM	1301
RSA	622
SHA1	1191
HMAC-SHA1	756
ANSI X9.31 A2.4 conformant PRNG	724

Table 2.2: FIPS Approved Crypto Algorithms.

The following occurs when the module is started in FIPS140-2 compliant mode:

- Internal crypto engines are initialized to FIPS mode,
- WEP authentication is disabled,
- WPA/WPA2 Enterprise authentication is disabled
- TKIP encryption for STAs is disabled
- WPA/WPA2 personal authentication is enabled,
- Per-packet encryption is enabled
- Per-packet authentication is enabled

- FIPS mode is enabled for TLS administrative connections
- FIPS mode is enabled for peer-to-peer encryption and authentication, and
- FIPS required power-up self-tests are executed

FIPS compliant mode affects operation of the module in following areas:

- Power-up self-tests are executed as described in section 9, Self-Tests.
- No clear text traffic is allowed through the encrypted zones (wlan0)
- External STA connections are IEEE802.11.i/RSN compliant using CCM protocol and pre-shared secret key (WPA2-PSK) for authentication.
- Peer-to-Peer connections are executed with per-packet encryption and authentication.
- Administrative sessions (CO / Administrator) are executed over a FIPS-mode TLS encrypted link with strict user authentication using role-based passwords.
- FIPS approved key generation methods are used:
    - RSA keys generation
    - AES key generation

For random values generation a FIPS-compliant PRNG is utilized (ANSI X9.31 A2.4 2Key Triple-DES).

3. PORTS AND INTERFACES

The ME3-24 BreadCrumb® contains six logical interfaces for information flow as shown in table 3.1 and described below.

Logical Interface App	Physical Interface	Interface Type	Role
Zeroize Note 1*	Zeroize/Status Button, wlan0, eth0, eth1	Control Input,	CO
bcledd	Status LED	Status Output	CO / Administrator
bcconfigd	wlan0, eth0, eth1	Data Input, Data Output, Input control Status Output	CO / Administrator
TLS Listener	wlan0, eth0, eth1	Data Input, Data Output,	CO / Administrator
Secure Data Transfer, Packet Capture	wlan0, eth0, eth1	Data Input, Data Output	USER / PEER.
Upgrade/Firmware Manager	USB host, wlan0, eth0, eth1	Data Input Data Output	CO / Administrator.

Table 3.1: ME3-24 – mapping of logical and physical interfaces

Note 1*: Logical Interface App. 'zeroize' can be executed using external zeroize/status button or selecting 'zeroize' from 'BCAPI' interface during CO session.

Zeroization process is described in section 5.4 Zeroization.

Ethernet ports (eth0, eth1) accept plaintext data from the wired network that will be encrypted prior to wireless retransmission, and produce plaintext data that is decrypted from encrypted wireless transmissions. These interfaces may also be used for CO/Administrator configuration sessions using a TLS-encrypted link.

One physical radio (wlan0) provides three logical interfaces:

- Secure Data Transfer (RSN / IEEE802.11i handshake / stateMachine),
- TLS Listener (BCAPI session interface)
- bcconfigd (service for 'BCAPI' - remote CO/Admin session)

BCAPI is Rajant's BreadCrumb® Application Programming Interface, which provides developers with a convenient means of administering BreadCrumb® devices from their applications. BCAPI is a TLS client of the module through which all administrative communications are sent. It is a part of a client application running outside of the module and is not part of the module validation.

A 'zeroize/status' button allows for zeroization of keys and passwords and the clearing of all settings to factory defaults.

'bcledd' handles the display of internal module status by setting status LED color and flashing rate.

The BreadCrumb® device peer interface produces and accepts encrypted inter-BreadCrumb® device communications only. The Access Point provides conventional Wi-Fi encrypted access point capabilities to client devices.

The TLS listener accepts TLS connections for CO/Administrator/Viewer sessions. bcconfigd is a server application listening and executing BCAPI session commands through TLS connections. Finally, a USB host interface provides software upgrade services.

Interface	Function
Power switch	Toggle switch to control power.
Status LED	Tri-color LED (allows for combination of colors: red, green, blue, cyan, magenta, yellow, white)
Zeroize/status button	Momentary push-button
Wlan	Wireless interface: One 802.11b/g mini-PCI radio (internal to device, with external antenna connector) with up to four ESSIDs
Antenna interface	Female N-type connector for wireless interface antenna

Interface	Function
Auxiliary Connector	18-pin connector: via adapter cable brings out: eth0 (RJ-45), eth1 (RJ45), USB host, power input (6-16VDC; minimum 9VDC required to charge internal battery)

Table 3.2: ME3-24 Physical Interfaces

The mapping of the module's logical interface types is presented in table 3.3 below:

Logical Interface	Physical Interface
Data Input	wlan0, eth0, eth1, USB,
Data Output	wlan0, eth0, eth1
Control Input	wlan0, eth0, eth1, zeroize/status button
Status Output	status LED, eth0, eth1, wlan0

Table 3.3 – Mapping of Logical Interface Types to Physical Interfaces

4. IDENTIFICATION AND AUTHENTICATION POLICY

4.1 Assumption of roles

The ME3-24 cryptographic module supports three distinct operator roles: Cryptographic Officer (CO), Administrator, and Viewer. These roles are authenticated by username / password. Additional roles supported are Peer and User (STA). Peers authenticate to the ME3-24 using the NAK established by the CO or negotiated LAK. The User role is authenticated via a shared WPA2 PSK key. Default usernames / passwords for each operator role are assigned at factory. Default values are intended only to use for first time CO authentication when they must be changed. The minimum password length allowed is 8 characters. Concurrent logins are allowed. Different usernames / passwords used to log-in assure separation of roles during concurrent sessions.

Role	Type of Authentication	Authentication Data	Factory Defaults
Crypto Officer	Role-based	Username and 8 char password	Username: 'co' Password: 'breadcrumb-co'
Administrator	Role-based	Username and 8 char password	Username: 'admin' Password: 'breadcrumb-admin'
View	Role-based	Username and 8 char password	Username: 'view' Password: 'breadcrumb-view'
Peer	Role-based	NAK(by CO) or LAK(negotiated)	
User	Role-Based	Shared WPA2 PSK key	

Table 4.1: Roles and Authentication

Note: CSPs with factory default values in the above table are explicitly overwritten with zeroes during zeroization process. Default values are restored on first post-zeroization boot.

Authentication Mechanism	SOF
Min. 8 char password	Note 1 below
2048-bit RSA Key (TLS link authentication) 256-bit key (HMAC-SHA-1-80)	112 80
256-bit key (AES WPA2-PSK)	256

Table 4.2: Strength of Authentication Mechanisms.

Note 1: password strength is calculated as the probability of guessing the password in a single trial.

This probability is estimated based upon a minimum password length of 8 characters and a minimum of 62 available characters (digits, small letters, and uppercase letters).

$P = 1 / 62^8 = 1$ in 218,340,105,584,896 probability of guessing the password in a single trial. This is less than required (1 in 1,000,000).

The actual chance of guessing is much smaller because the pool of characters is determined by unicode UTF-8 encoding which supports up to 38950 characters.

For multiple tries:

- Approach 1: with 5 sec delay between authentication attempts, no more then 12 guesses per minute may be attempted. The odds of guessing within one minute are 12 in 218,340,105,584,896 = 1 in 18,195,008,798,741, which is less then 1 in 100,000.

- Approach 2: to have a chance better than 1 in 100,000, 218,340,105,584,896 / 100,000 = 2,183,401,055 authentication attempts per minute would be required.

5. ACCESS CONTROL POLICY

5.1. Roles supported by cryptographic module

The ME3-24 supports the following roles:

1. Crypto Officer: The Crypto Officer role performs all security functions provided by the ME3-24 and manages the administrator users. The Crypto Officer uses a remote session over a TLS link to configure the ME3-24. The Crypto Officer authenticates to the ME3-24 using a username and password.

2. Administrator: The Administrator performs general ME3-24 configuration such as defining networking settings, performing self-tests, and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator. The Administrator authenticates to the ME3-24 using a username and password.

3. Viewer: The Viewer role is a read-only equivalent to the Administrator role. The Viewer is allowed to audit and view system logs. The Viewer authenticates to the ME3-24 using a username and password.

4. Peer: The Peer role is assumed by other BreadCrumb® devices that establish radio communication with a ME3-24. No CO security functions are available to Peers. Peers authenticate to the ME3-24 using the NAK established by the CO or negotiated LAK as specified by Rajant's meshing protocol and encrypt traffic to one another using the NEK established by the CO.

5. User: The User role is permitted to communicate with ME3-24s without establishing a Peer relationship. This communication takes the form of IEEE 802.11a/b/g client associations or via Ethernet. IEEE 802.11a/b/g client associations are authenticated via a shared WPA2 PSK key which is manually input into the ME3-24 by the CO.

5.2. Services provided by cryptographic module

Role	Service	Notes
CO	ME3-24 configuration	1. Set FIPS mode if not set. 2. Set non-default passwords 3. Enter Keys NAK, NEK, WPA2-PSK 4. Update firmware if needed. 5. Reboot if required to finalize setup.
CO	Key Entry	Enter keys: WPA2-PSK, NAK, and NEK using secure connection.
CO	Key / CSP Zeroization	Execute 'zeroize' through BCAPI client or using external button
CO	Show Status	1. View Status via Status LED by pressing zeroize/status Button, 2. View module's status through BCAPI interface
CO	Self-Tests	Run Self-Tests by rebooting module
CO	Ethernet ports enable/disable	Part of configuration – through BCAPI interface
CO	Manage administrators	Set / Change CO, Admin, and Viewer passwords using BCAPI interface.
Administrator	Manage network services	Enable / disable ports through BCAPI interface, configure radio channels, etc.
Viewer	Audits / views system logs	View system data and logs through BCAPI interface
Peer	Encryption/Decryption	
User (external clients)	Encryption/Decryption	

Table 5.2: Services Authorized for Roles (C3)

5.3. Cryptographic Keys and CSPs Employed by Cryptographic Module

The keys and CSPs employed by the module are listed in Table 5.3 below:

- Factory Public Key – (1)
- System HMAC Key – (1)
- Key Encryption Key (KEK) – (1)
- Network Authentication Key (NAK) – (1)
- Network Encryption Key (NEK) –(1)
- Link Authentication Key (LAK) – (1) (per peer connection)
- SendPK and RecvPK (used in LAK establishment) - (1) (per peer connection)
- Public/Private RSA keys – (1)
- WPA2 PSK key – (up to 4)

Passwords:

- Passwords – (3)

PRNG seeds:

- Random seed
- Random seed key

Key / SRDI	**Type**	**Storage**	**Use**	**Zeroization**	**Factory Default**
Factory Public Key	RSA 2048-bit	Plain Text in flash memory	Authenticates firmware updates prior to installation	N/A	N/A
OpenSSL HMAC Key	HMAC key 128-bit	Plain Text hardcoded (in RAM)	Tests integrity of OpenSSL module's source	N/A	N/A

Key / SRDI	Type	Storage	Use	Zeroization	Factory Default
KEK (Key Encryption Key)	AES 256-bit	Plain Text in flash memory	Used to encrypt private RSA key	Note (*)	
NAK (Network Authentication Key)	256-bit HMAC-SHA-1	Plain Text in flash memory	Authenticates broadcast packets within a BreadCrumb® device network	Note (*)	All '0's Note(**)
LAK (Link Authentication Key)	256-bit HMAC-SHA-1	Plain Text in RAM (*)	Authenticate unicast packets between BreadCrumb® devices	Note (*)	
SendPK, RecvPK	256-bit random number	Plain Text in RAM (*)	Establish LAK	Note (*)	N/A
NEK (Network Encryption Key)	AES 256-bit	Plain Text in flash memory	Encrypts all packets within a BreadCrumb® device network	Note (*)	All '0's Note(**)
Public Key	RSA 2048 bit	Plain Text in flash memory	Used to establish TLS connections	N/A	
Private Key	RSA 2048 bit	Encrypted by KEK in flash memory	Unique to each device; generated on first boot after zeroization or factory initialization. Used to establish TLS connections	Private RSA key is encrypted with KEK and becomes unreadable after KEK is zeroized	
WPA2-PSK	AES 256 bit	Plain Text in	Used for client device	Note (*)	All '0's

Key / SRDI	**Type**	**Storage**	**Use**	**Zeroization**	**Factory Default**
Keys		flash memory	authentication		Note(**)
PMK (Pair-wise Master Key) : copy of WPA2-PSK	AES 256 bit	Plain Text in RAM	Used to derive PTK key	Note (*)	
PTK (Pair-wise Transient Key) Bit 0 – 127 Bit128-255 Bit 256-383	Compound key: KCK key KEK key TK1 key	Plain Text in RAM	Used to protect link between STA and the AP	Note (*)	
GMK (Group Master Key)	AES 256 bit	Plain Text in RAM	Used to derive GTK key	Note (*)	
GTK (Group Transient Key)	AES-CCMP 128 bit	Plain Text in RAM	Protects multicast / broadcast msgs to STAs	Note (*)	
PRNG Seed	64bit random number	Plain Text In RAM	Seed to PRNG	Note (*)	
PRNG Seed Key	64 bit random number	Plain Text in RAM	Seed Key for PRNG	Note (*)	
TLS Session Key	Key type is negotiated with the administrative client program to be the stronger shared cipher of:	Plain Text in RAM	Used for encryption after TLS link is established.	N/A	

Key / SRDI	Type	Storage	Use	Zeroization	Factory Default
	-256-bit AES/CBC -128-bit AES/CBC Note(****)				
System HMAC Key	256-bit HMAC-SHA-1 key	Plain Text in flash memory	Full system integrity check during boot process Note(***)	N/A	

Table 5.3: Key / SRDI Table

NOTES:

Zeroization process is initiated by button press or by remote command via BCAPI interface, as explained in detail in section '*5.4 Zeroization*'.

(*) RAM-based and flash-memory-based CSPs are explicitly overwritten with zeroes during zeroization process.

(**) CSPs with default values in the above table are explicitly overwritten with zeroes during zeroization process. Default values are restored on first post-zeroization boot.

(***) Binary of entire software module is subject to integrity test as required by FIPS 140-2 section 4.9.1.

(****) Per the TLS specification <http://www.ietf.org/rfc/rfc2246.txt>, a connecting client provides a list of supported ciphers. The server (ME3-24) selects the strongest of the ciphers it shares with the client and communicates the result. TLS key negotiation is per the TLS specification and as explicitly permitted in *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, section 7.1.

Service	Role	Key / CSP	Storage	Access
Key Encryption	CO	KEK: 256-bit AES key encrypts RSA private key	Plain Text in internal flash memory	X
Authentication	CO	Password	Plain Text in internal flash memory	X
Authentication	Administrator	Password	Plain Text in internal flash memory	X
Authentication	Viewer	Password	Plain Text in internal flash memory	X
Authentication	Peer	RSA Private Key LAK (Link Authentication Key), SendPK, RecvPK NAK (Network Authentication Key)	Encrypted by KEK in internal flash memory Plain Text in RAM Plain Text in internal flash memory	X X X
Authentication	User (Client devices)	Knowledge of Secret Key	Plain Text in internal flash memory	X
Key Entry	CO	NEK (Network Encryption Key) AES-256	Plain Text in internal flash memory	W
Key Entry	CO	NAK (Network Authentication Key) HMAC-SHA1	Plain Text in internal flash memory	W

Service	Role	Key / CSP	Storage	Access
Key Entry	CO	RSA public key	Plain Text in RAM	W
Key Entry	CO	AES client authentication key (WPA2 PSK)	Plain Text in internal flash memory	W
Key Generation	CO	RSA private key Note(*)	Encrypted by KEK in internal flash memory	W
Zeroization	CO	<All keys and authentication data>	Overwrite key encryption key, configuration, and all CSPs in internal flash memory with zeros.	W (over-written w/ defaults)
Self-Tests	CO, Administrator	None	N/A	X
Show Status	CO, Administrator	None	N/A	R
Encryption	User	AES key	Plain Text in internal flash memory	X
Decryption	User	AES key	Plain Text in internal flash memory	X

R=Read, W=Write, E=Edit, X=Execute

Table 5.4: Access Rights within Services (C4)

Notes:

(*) RSA private key is generated internally using FIPS approved PRNG cert #455

Key Generation

Three of the keys listed in tables 5.3 and 5.4 merit further discussion. These are the LAK (Link Authentication Key), KEK (Key Encryption Key), and RSA key-pair. These keys generated internally and never transported outside of the module.

The LAK key is generated during Peer Link establishment, and the KEK and RSA keys are generated as necessary during power up initialization. Below are highlights of both processes.

LAK generation

All BreadCrumb® devices in a network share common NAK and NEK keys. When two modules connect, they establish a Peer Link. Rajant's protocol governing Peer Links allows connecting modules to authenticate each other and to establish a common Link Authentication Key (LAK) used throughout this connection for per packet authentication. The SendPK and RecvPK are automatically created and used during this process. When transmitted between connecting modules, they are encrypted via AES Key Wrap using the NEK.

KEK and RSA key-pair generation:

The KEK resides in flash memory. If not present during power up it is re-generated, a new RSA key-pair is created, and the new RSA private key is encrypted using the KEK key and stored in flash memory.

5.4 Zeroization

Zeroization is a process in which all CSPs are cleared. It is equivalent to restoring factory default values. Zeroization can be executed using an external button or through 'BCAPI' interface as shown in screenshot below.

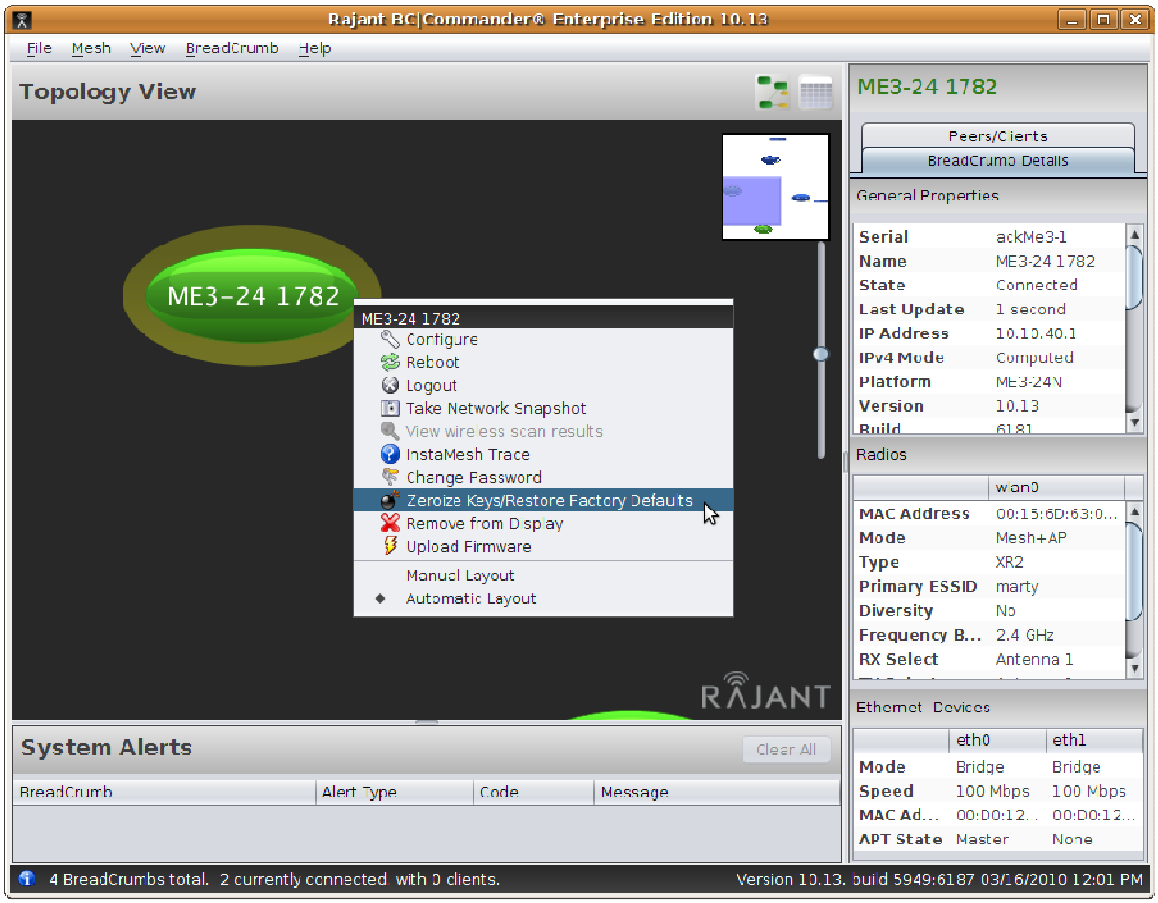

Figure 5.1: Zeroization / restoring factory defaults using BCAPI interface.

Keys are stored in two locations, RAM (as plaintext) for normal operations, and on dedicated partition of internal flash memory (CSP partition) (as plaintext or encrypted by KEK). The KEK itself is stored in flash CSP partition. The zeroization process halts normal operations, and overwrites with zeroes the flash CSP partition and the RAM based CSPs.

Remote zeroization may be initiated by a Crypto Officer through any BCAPI client. Using BC|Commander, Rajant's standard BreadCrumb® network administration tool included with all BreadCrumbs® and itself a BCAPI client, remote zeroization is initiated by right-clicking on the device and choosing "Zeroize/restore defaults" from the pop-up menu.

To zeroize a device using the device's buttons, press and hold 'zeroize/status button' for 10sec. This button is in a recessed casing to avoid accidental zeroization. The status LED, if enabled, will blink yellow to indicate zeroization in progress. The status LED, if enabled, will then flash an error code to indicate that zeroization is complete and that the device will automatically reboot after 30 seconds.

After it reboots, the ME3-24 will generate a new RSA key-pair and revert other keys to factory default keys and will join an existing mesh (if any is in the area) that uses the default settings. If no such mesh is in the area, the device will not be able to communicate with any other devices.

5.5 Initialization / Factory defaults

Initialization is a process in which default factory values are restored. This process is identical to zeroization as described above.

This action will zeroize the module and restore factory default configuration.

6. OPERATIONAL ENVIRONMENT

The module's operational environment is not modifiable – Operational Environment rules do not apply.

7. SECURITY RULES

7.1 Secure Configuration of the Module

This is a description of exactly what the CO has to do if the ME3-24 is newly "out of the box" and the CO wishes to configure the device for secure operations in FIPS-compliant mode.

1. Enable FIPS-compliant mode
2. Change the default settings when configuring the module for the first time. This includes default co, admin, and view passwords, default NEK and NAK, and default WPA2-PSK key.
3. Configure the module in accordance with guidance found in the CO Guidance documents.
4. Enforce a strong password policy and change passwords on a regular basis.
5. Secure upgrade using USB storage as needed.
6. Inspect module regularly for damage, intrusion, and tampering.
7. Assure that the module is installed in a secure location in a secure manner.
8. Assure that access to the module is restricted to authorized personnel.
9. Use a trusted host for remote administration and monitoring.
10. Inspect newly arrived modules.
11. Verify that the firmware installed is FIPS-compliant. This may be verified by observing a magenta blinking pattern on the module's LED every five seconds or by checking the "FIPS Supported" and "FIPS Enabled" fields in the BreadCrumb Detail panel of the BC|Commander network management application.
12. Zeroize all cryptographic keys prior to terminating a network configuration.
13. Zeroize unit before sending to factory for repairs.
14. Ensure that the shared secret key is given only to trusted Users.
15. Ensure that all keying operations (NAK, NEK, and WPA2-PSK keys) are performed over a direct Ethernet connection to the ME3-24 BreadCrumb® being configured.

7.2 Secure Operation.

The ME3-24 physical interfaces exposed to the outside world are:

- ethernet ports eth0, eth1
- wireless port wlan0,
- power connector for external power source,
- power switch,
- USB port,
- Zeroize/status button,
- status LED.

The status indicator shows the current status of the module via patterns of flashing colored light.

Zeroize/status button allows for zeroization of the module and restoration of the module's factory default settings.

All other interfaces allow access to the module only through predefined logical interfaces assigned to the module's roles or not activated at all.

The Crypto Officer and Administrator have direct access to the module through a remote API and must authenticate to module according to their roles. These are the only roles capable of configuring and administering the module. If any other maintenance is required, the module must be returned to the factory.

The Viewer role has read-only access to the module allowing for audits / log viewing capabilities.

The module is FCC compliant (Part 15, Subpart J, Class B) hardware platform that satisfies FIP PUB 140-2 security level 2 hardware requirements.

The FCC Product ID for the ME3-24 is **FCC ID VJA-ME3.**

The FCC accredited laboratory used by Rajant is:

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

The module includes a status LED in order to provide user feedback. This LED is capable of displaying seven colors (red, blue, green, cyan, magenta, yellow, and white) and blinking in order to indicate various operational states.

Errors and warnings include numeric codes to indicate the type of error or warning that has occurred. These codes are indicated via a blink cycle including short and long pauses. Each digit of an error or warning code is displayed as a number of blinks separated by short pauses. Individual digits are separated by a longer pause. The end of the code is indicated by a longer pause still. The code then repeats.

For example, code 312 would be indicated by the repeating cycle:

(3) ON short pause ON short pause ON long pause
(1) ON long pause
(2) ON short pause ON very long pause

Warnings are indicated with a yellow light and allow ME3-24 operations to continue.

Errors are indicated with a red light and halt ME3-24 operations.

FIPS mode is indicated by fast flashing pattern of magenta light as described in “2.2. FIPS140-2 Compliant Mode of Operation”.

7.3 Setting FIPS Mode

To set FIPS Mode, the CO must ensure that the workstation running the administration software is directly connected to the device via Ethernet. The device will not accept keys over its wireless interface.

The screenshot below is from the standard BC|Commander management application provided by Rajant, which uses Rajant's management API. The instructions may vary slightly if a different application using the API is used. Please note that the BC|Commander management application is not part of the module and has not been validated under FIPS 140-2.

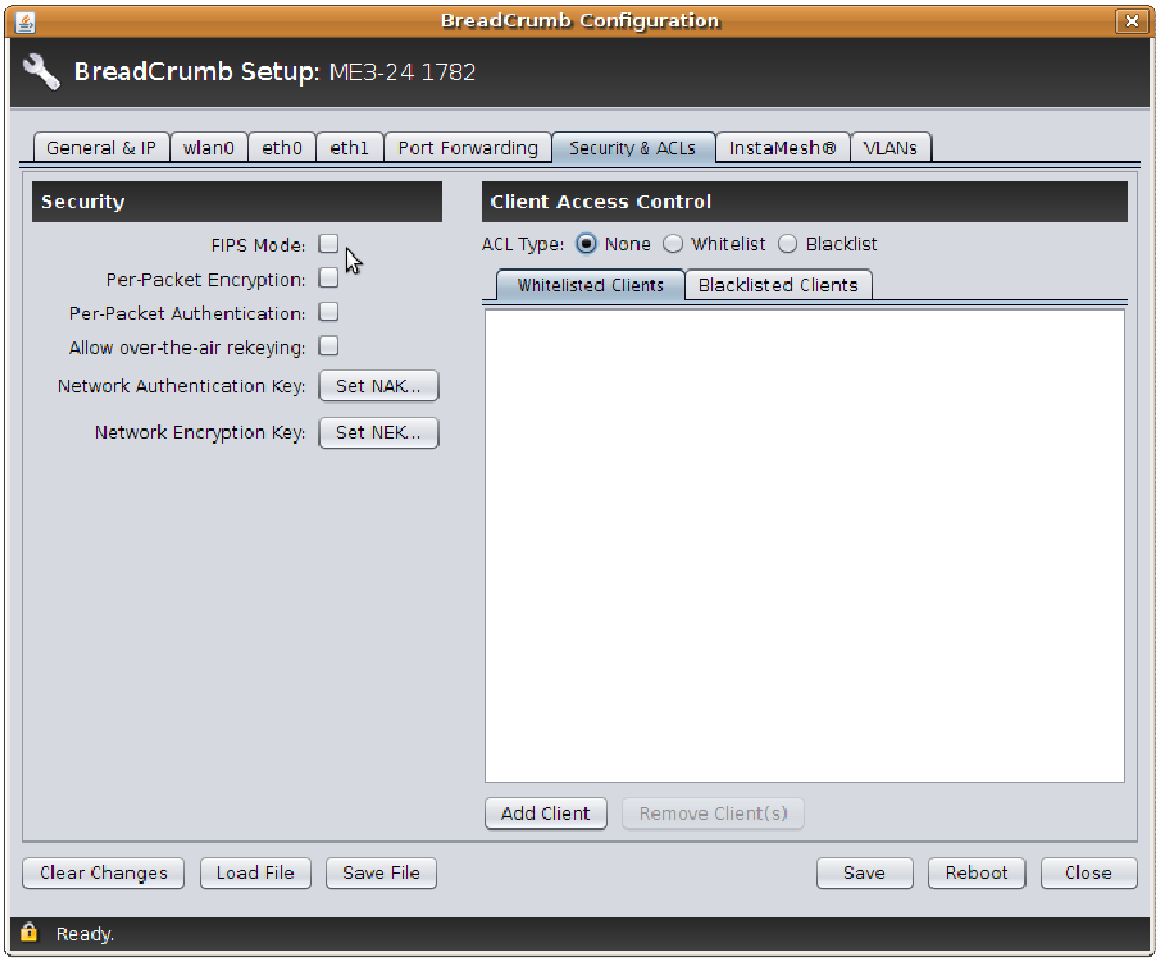

Figure 7.1: Setting FIPS mode.

1. Select the device to configure and right-click on it. Choose "Configuration" from the popup menu. This will show the tabbed interface shown above. Choose "Security and ACLs" to modify security settings.

2. To enable FIPS mode, check the FIPS mode checkbox. This will automatically enable per-packet encryption and authentication on the ME3-24 BreadCrumb® regardless of the associated settings displayed on the screen. This setting must be saved to the device via the "Save" button at the bottom of the window.

3. After the setting have been changed and saved, the device must be rebooted. Use the "Reboot" button at the bottom of the window or right-click on the device back in the main application and choose "Reboot" from the popup menu.

8. PHYSICAL SECURITY

8.1 Physical Security Mechanisms.

Fig 8.1 ME3-24 module views with 'loctite' compound over screws and switch mounting (blue color / L label) for tamper evidence and resistance. (views not to scale)

The module's hardware is manufactured to meet FIPS 140-2, Level 2 Physical Security requirements. The module is enclosed in an aluminum 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(R) 425, mfg. part no. 42540, available from Rajant) covering the chassis access screws. This is shown in views of the module chassis in Fig 8.1 above.

It is the responsibility of the Cryptographic Officer to ensure that the screws are covered with the cyanoacrylate material delivered with the module in such a way that it prevents access to or viewing of internal module components without breaking the tamper evidence material. Table 8.1 below specifies all physical security activities applicable to the user site.

Below is the procedure required when applying tamper evidence material to chassis access screws. This procedure applies to the module serviced at the manufacturer's site. The module is not field-serviceable and whenever tamper evidence is detected the module should be taken out of service and replaced with a secure unit from the manufacturer.

Application of the tamper evidence 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 Fig 8.1 to select screws to which Loctite material is to be applied (Visible blue coloring around screws / label 'L'). Using alcohol, clean well the chassis areas around the screws and wait until completely dry. Use Loctite sealant from container packed with the module. Shake the sealant container. To open the sealant make a diagonal cut at the tip of its applicator.

Apply three to four drops of the sealant on each marked screw (Fig 8.1 top views – connectors and main cover) so that sealant completely covers the drive slot and flows around the screw head and adheres to chassis around the screw. Wait until dry.

Follow with hexagonal screws holding buttons and switches as marked on Fig 8.1 bottom views. Apply a single drop of sealant on each of these screws to cover corner of the screw. Sealant must adhere to the screw and to the chassis so that screw cannot be unfastened without breaking the sealant.

Note: for full curing leave module in room temperature for 4 hours.

Physical Security Mechanisms	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Inspect module regularly for damage, intrusion, and tampering.	daily	Test carefully that tamper-proof compound over screws does not show signs of tampering
Assure that the module is installed in a secure location in a secure manner.	daily	Inspect that module was not relocated.
Assure that access to the module is restricted to authorized personnel.	daily	Inspect that module is not accessible to unauthorized personnel
Inspect newly arrived modules.	On arrival	Visually inspect for evidence of tampering or damage.

Table 8.1: Inspection / Testing of Physical Security Mechanisms. (C5)

9. SELF-TESTS

The Module runs the following at start-up:

Algorithm	Known Answer Test
AES	FIPS_selftest_aes(): KAT test
SHA1	FIPS_selftest_sha1(): KAT test
AES CCMP	init_crypto_ccmp_test(): KAT test
RSA	FIPS_selftest_rsa(): Pairwise and KAT
HMAC	FIPS_selftest_hmac(): KAT test
RNG	FIPS_selftest_rng(): KAT test

The module also runs the following conditional self-tests:

Test	Description
Continuous RNG Test:	Run whenever random number is generated using ANSX9.31 PRNG.
Manual Key Entry Test	CO's key entry is validated by dual entry test.
Load Test	When an upgrade image is generated its RSA signature is generated using a factory RSA private key. The corresponding public RSA key is then used to check signature of loaded files. Loading of a non-validated image will invalidate the module's FIPS 140-2 validation.
OpenSSL Software Integrity Test	At build time, the HMAC-SHA1 digest of binary of OpenSSL's entire FIPS Object Module is computed. This digest is then embedded in the module's binary image.

Test	Description
	Whenever this library is placed in FIPS mode, this embedded HMAC-SHA1 digest is compared with a new one computed against the module.
System Integrity Test	At build time the HMAC-SHA-1 digest of the entire system is computed. This digest is then embedded into the module's binary image. At power up time in FIPS mode, the system computes a new system digest and compares it to the embedded digest. Note that the system digest includes the OpenSSL library, which also has its own run-time integrity test described above.
Pairwise Consistency Test	Run on power up as a part of power up self-tests and every time an RSA key-pair is generated.

10. MITIGATION OF OTHER ATTACKS POLICY

The module is not designed to mitigate other attacks.

11. ACRONYMS

AES	Advanced Encryption Standard
BCAPI	BreadCrumb® Application Interface
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CSR	Certificate Signing Request
D-H	Diffie-Hellman (Key Exchange)
EDC	Error Detection Code
FIPS	Federal Information Processing Standard
FRAM	Ferromagnetic RAM
HMAC	(Keyed) Hash Message Authentication Code
KAT	Known Answer Test
KCK	EAPOL Key Confirmation Key (WPA)
KEK	Key Encryption Key
KEK	EAPOL Key Encryption Key (WPA)
LAK	Link Authentication Key, (Authenticates Peer 2 Peer connections)
NAK	Network Authentication Key (Authenticates broadcast packets)
NEK	Network Encryption Key
NIST	National Institute of Standards and Technology
RecvPK	CSP received from a peer during handshake process.
RSA	Key encryption method (authors: Rivets, Shamir, and Adelman)
SendPK	CSP sent to a peer during handshake process.
SOF	Strength of Function
SRDI	Security Relevant Data Item

SSL Secure Sockets Layer

TK1 Temporal Key (WPA)

TLS Transport Layer Security