Vocera Communications, Inc.
Vocera Cryptographic Module

Hardware Version: 88W8686
Software Version: 1.0
Firmware Version: 1.0

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation
Document Version 2.0

Prepared for:

Vocera Communications, Inc.
525 Race Street
San Jose, CA 95126
Phone: (408) 882-5100
Fax: (408) 882-5101
http://www.vocera.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Vocera Cryptographic Module from Vocera Communications, Inc.. This Security Policy describes how the Vocera Cryptographic Module meets the security requirements of Federal Information Processing Standard (FIPS) Publication 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/index.html.

The Vocera Cryptographic Module is referred to in this document as cryptographic module, hybrid module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Vocera website (http://www.vocera.com) contains information on the full line of products from Vocera.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Executive Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Vocera. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Vocera and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Vocera.

2 Vocera Cryptographic Module

2.1 Overview

The Vocera® Communications System is a breakthrough wireless platform that provides hands-free voice communications throughout an 802.11b/g-networked building or campus. The Vocera Communications System consists of two key components:

- The Vocera System Software, which runs on a standard Windows server, controls and manages call activity.
- The Vocera B2000 Communications Badge allows users to converse over a Wireless Local Area Network (WLAN).

A typical Vocera system deployment is shown in Figure 1 below.

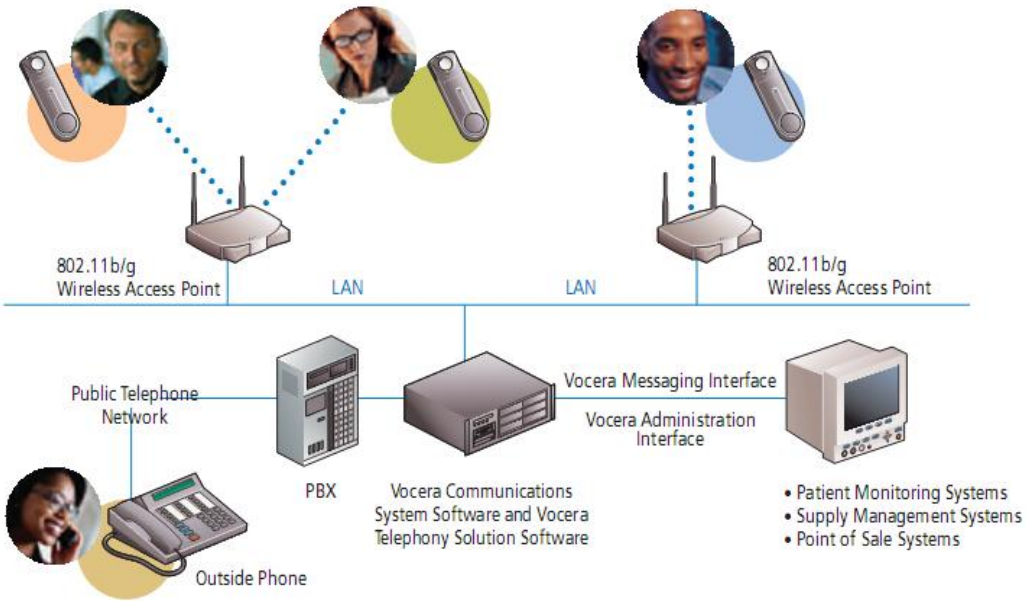

Figure 1 – Typical Vocera Communications System Deployment

The Vocera B2000 Communications Badge (see Figure 2) is a small, virtually hands-free wireless device that acts as the interface to the Vocera Communications System. The wearable badge is controlled using voice commands, and enables instant two-way voice conversation, text messaging, and alerts. The badge communicates with other Vocera communications devices or with the Vocera System Software server (typically referred to as the Vocera Server) securely over a protected channel. With optional Vocera telephony solution software, the badge can also make and receive telephone calls through the Vocera Server via a private branch exchange (PBX). The badge employs a high-performance antenna for improved transmit and receive sensitivity.

Figure 2 – Vocera B2000 Communications Badge

Communications are protected via industry-standard secure wireless communications protocols. The security functionality is provided by the Vocera Cryptographic Module (VCM) embedded in the badge. Various applications on the Vocera badge make use of the VCM to establish a secure connection with the Vocera Server and with other Vocera communications devices. All cryptographic services needed by the badge are provided by the VCM.

For FIPS purposes, the VCM has been evaluated as a hybrid cryptographic module. A hybrid module is a special type of software/firmware module that makes use of specialized hardware components within the physical boundary of the target device. In this case, the VCM is composed of software libraries running on a Texas Instruments (TI) applications processor (OMAP5912), firmware running on a high-performance Marvell WLAN chip (part number 88W8686), and all of the required components are contained within the Vocera badge. The hybrid module software was tested on a Vocera B2000 badge using Vocera Embedded Linux Version 1.0 running on a Texas Instruments OMAP5912 (single-user mode).

Versioning for the module's components is as follows:

- Hardware: 88W8686
- Software: 1.0
- Firmware: 1.0

The Vocera Cryptographic Module is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[1]	1
9	Self-tests	1
10	Design Assurance	1

[1] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
11	Mitigation of Other Attacks	N/A[2]
14	Cryptographic Module Security Policy	1

2.2 Module Interfaces

The Vocera Cryptographic Module is a hybrid module that meets overall Level 1 FIPS 140-2 requirements. All of the module's components are entirely encapsulated by the logical cryptographic boundary as shown in Figure 3 below. Figure 3 below shows that the hybrid module includes software libraries running on the applications processor and firmware running on the WLAN chip all residing inside the logical cryptographic boundary.

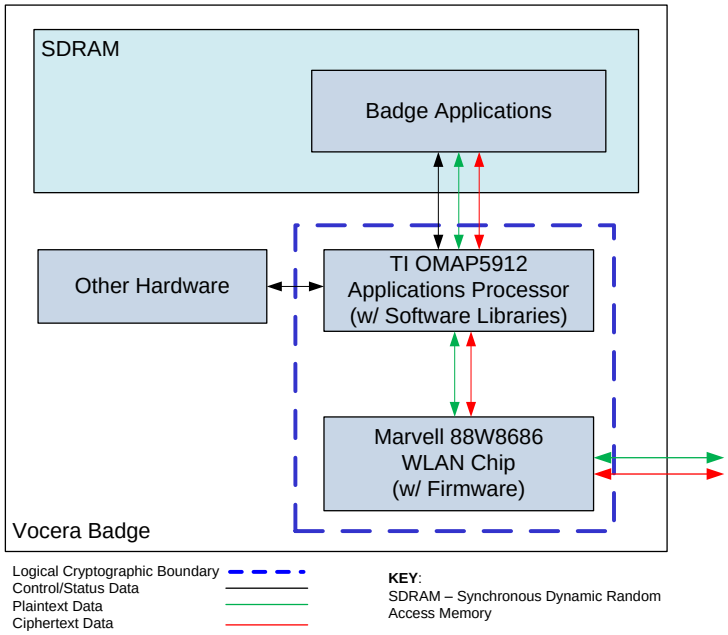

Figure 3 – Logical Cryptographic Boundary

As is required by the FIPS 140-2 Implementation Guidance, the module's interfaces are provided only via the software component of the module. Thus, the hybrid module's interfaces consist solely of the available APIs. The APIs are grouped into four logically distinct FIPS 140-2 categories:

- Data Input
- Data Output
- Control Input
- Status Output

The target platform for the module is a Vocera Communications B2000 Badge. As such, the VCM's logical interfaces described above map to the physical ports and interfaces provided by the badge. Those ports and interfaces are:

- Badge display
- Buttons (Call button, hold/DND[3] button, and menu buttons)

[2] N/A – Not applicable
[3] DND – Do Not Disturb

- Speaker
- Microphone
- Indicator light
- Headset jack
- Wireless Local Area Network (WLAN) interface (not exposed on the badge cover)
- Contact pins

NOTE: While included here for completeness, the entire Vocera B2000 Badge is not within the boundary of the cryptographic module described in this policy document. Only the components as illustrated in Figure 3 comprise the module.

The physical features of the badge are also shown in Figure 4 below.

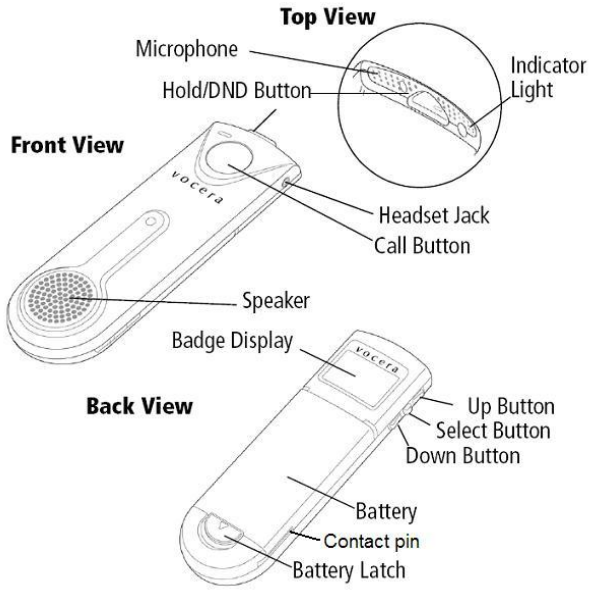

Figure 4 – Physical Features of the Vocera B2000 Badge

The data and control inputs made via the badge microphone, WLAN, and buttons are translated into the logical data and control inputs made via the API calls to the hybrid module. Likewise, the data and status outputs made via API call returns from the hybrid module are translated into the data and status outputs made to the WLAN, badge display, speaker, and indicators.

Table 2 below provides a mapping of the physical (i.e. badge) and logical (i.e. module) interfaces to the appropriate interface category.

Table 2 – Interface Mappings

Interface Category	Physical Interface	Logical Interface
Data Input	WLAN, Microphone, headset Jack	Function calls that accept, as their arguments, data to be used or processed by the module.
Data Output	WLAN, Headset Jack, Speaker	(i) Arguments for a function that specify where the result of the function is stored or (ii) returned as a return value.

Interface Category	Physical Interface	Logical Interface
Control Input	WLAN (for roaming), Call Button, DND Button (Hold to power-off), Select Button, and Contact Pins (power to the module)	Function calls utilized to initiate the module and the function calls used to control the operation of the module.
Status Output	Badge Display Screen	Return values for function calls

2.3 Roles and Services

The module does not support authentication of operators. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer (CO) role and User role. The module does not require an operator to authenticate; role of the operator is implicitly assumed.

2.3.1 Crypto-Officer Role

The Crypto-Officer role has the ability to manage the module and monitor the status. Descriptions of the services available to the Crypto-Officer role are provided in the table below. Table 3 also lists the Critical Security Parameters (CSPs) that are accessed by the services, as well as the module component that provides the service.

Table 3 – Mapping of Crypto-Officer Role's Services to Type of CSP Access

Service	Description	Type of CSP Access	Provided By
Perform Self-test	Run self-tests at power-up or on-demand	None	Software libraries
Show status	Monitor status	None	Software libraries

2.3.2 User Role

The User role is used to secure communication services. Descriptions of the services available to the User role are provided in Table 4. The table also lists the CSPs that are accessed by the services, as well as the module component that provides the service.

Table 4 – Mapping of User Role's Services to Type of CSP Access

Service	Description	Type of CSP Access	Provided By
Initiate crypto operation	Creates an environment to carry out cryptographic operation	None	Software libraries
Generate random number	Generate random bytes based on ANSI[4] X9.31 Appendix A.2.4.	ANSI X9.31 PRNG seed – Read, write, execute ANSI X9.31 PRNG key – Read, execute	Software libraries
EAPOL[5]-Key Message operations	Format EAPOL-Key message	802.11i Pairwise Master Key (PMK) – Read, execute	Software libraries
EAPOL operation	Transmit and receive EAP[6] messages using EAPOL	802.11i PMK – Read, write, execute	Software libraries

[4] ANSI – American National Standards Institute
[5] EAPOL – Extensible Authentication Protocol Over LAN (Local Area Network)
[6] EAP – Extensible Authentication Protocol

Service	Description	Type of CSP Access	Provided By
Four-way handshake	Process four-way handshake	802.11i PMK – Read, execute 802.11i Temporal Key – Write, execute	Software libraries
HMAC[7] operation	Generate HMAC value	HMAC key – Read, execute	Software libraries
Protected EAP (PEAP) operation	Perform PEAP operation	RSA public key – Read, execute TLS[8] Authentication Key – Execute TLS Session Key – Execute 802.11i PMK – Read, write, execute ANSI X9.31 PRNG seed – Execute ANSI X9.31 PRNG key – Execute	Software libraries
Hashing operation	Generate SHA-1 digest	None	Software libraries
TLS operation	Perform TLS operation	TLS Authentication Key – Write, execute TLS Session Key – Write, execute	Software libraries
Zeroization	Zeroize keys utilized by the module	RSA Public Key - Execute TLS Authentication Key - Execute TLS Session Key - Execute 802.11i PMK - Execute 802.11i Temporal Key - Execute HMAC Key - Execute AES Key - Execute ANSI X9.31 PRNG Seed - Execute ANSI X9.31 PRNG Key - Execute	Software libraries

2.4 Physical Security

The Vocera Cryptographic Module is a hybrid module, which in FIPS terminology is a multi-chip standalone embodiment. The module consists of production-grade components that include standard passivation techniques, meeting Level 1 requirements.

Further, while the module has no enclosure of its own, it is intended to run on the Vocera Communications B2000 Badge. Thus, while the badge case is not a part of the module, the module is also protected by the hard plastic cover of the Vocera badge, which surrounds all the module's hardware, software, and firmware components. A physical block diagram of the target device is shown in Figure 5 below.

[7] HMAC – (Keyed-) Hash Message Authentication Code
[8] TLS – Transport Layer Security

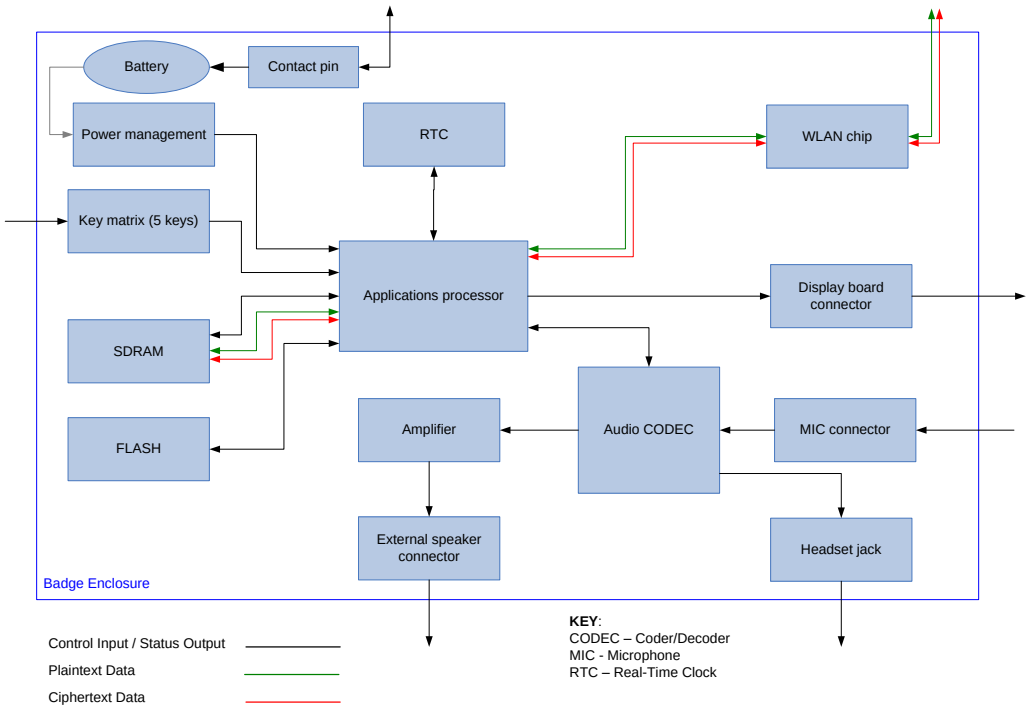

Figure 5 – Physical Block Diagram of the Module's Target Device

2.5 Operational Environment

The module is intended for use on a Vocera B2000 badge using Vocera Embedded Linux Version 1.0 running on a Texas Instruments OMAP5912. For FIPS 140-2 compliance, this is considered to be a single-user operational environment due to the fact that only one operator can be in possession of a given Vocera badge (which hosts the module) at any given time. The module is not intended to operate on any platform other than the Vocera badge. As such, all keys, intermediate values, and other CSPs remain only in the process space of the operator using the module. The operating system uses its native memory management mechanisms to ensure that outside processes cannot access the process space used by the module.

2.6 Cryptographic Key Management

The Vocera Cryptographic Module implements the following FIPS-Approved or allowed algorithms listed in Table 5.

Table 5 – Algorithm Certificate Numbers for Cryptographic Libraries

Approved or Allowed Security Function	Certificate Number
AES 128-, 192-, 256-bit in Cipher-Block Chaining (CBC)	980
AES 128-bit in ECB[9] and CCM[10]	835
SHA-1	950
HMAC using SHA-1	551

[9] ECB – Electronic Code Book
[10] CCM – Counter with Cipher Block Chaining-Message Authentication Code

Approved or Allowed Security Function	Certificate Number
ANSI X9.31 Appendix A.2.4 PRNG	556
RSA 1024-, 1536-, 2048-bit encryption/decryption for key transport[11]	N/A

The module also implements the following non-FIPS-Approved algorithms listed below. Note that these algorithms are used only as underlying algorithms within the TLS communications protocol, and as such, are allowed for use per FIPS Implementation Guidance D.2.

Table 6 – Non-FIPS-Approved Functions

Non-FIPS-Approved Function	Certificate Number
HMAC Message Digest 5 (MD5)	N/A
MD5	N/A

The module supports the critical security parameters listed in Table 7:

[11] Caveat: key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
HMAC Integrity Test Key	HMAC SHA-1 key	Hard-coded in the module	Never exits the module	Hard-coded in the module in plaintext	Replacing the software libraries	HMAC SHA-1-based module self-integrity test
RSA Public Key	RSA 1024-, 1536-, 2048-bit public key	Externally generated; automatically sent to the module	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Key transport during TLS handshake for PEAP phase 1
TLS Authentication Key	HMAC SHA-1 key	Internally generated	Encrypted during TLS handshake	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Data authentication for TLS sessions for PEAP phase 2
TLS Session Key	AES 128-bit key	Internally generated	Encrypted during TLS handshake	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	TLS session Encryption/Decryption of authentication related messages in PEAP phase 2
802.11i Pairwise Master Key	256-bit shared secret	For Pre-shared: externally generated; enters the module in plaintext For PEAP: internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the 802.11i session is closed	Partial input to construct 802.11i Temporal Key used in 802.11i protocol
802.11i Temporal Key	AES 128-bit key	Internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the 802.11i session is closed	Used to create secure tunnel for wireless data transmission.
HMAC Key	HMAC SHA-1 key	Internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the API service is terminated	Used for Keyed-Hash Message Authentication in the module
ANSI X9.31 PRNG Seed	128-bytes of seed value	Internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the API service is terminated	FIPS-Approved random number generation
ANSI X9.31 PRNG Key	AES 128-bit key	Hard-coded in the module	Never exits the module	Hard-coded in the module in plaintext	Replacing the software libraries	FIPS-Approved random number generation

2.7 Self-Tests

The Vocera Cryptographic Module performs the following self-tests at power-up:

- Software Integrity Check using HMAC SHA-1
- Firmware Integrity Check using HMAC SHA-1
- Known Answer Tests (KATs)
    - AES ECB and CCM mode KAT
    - AES CBC mode KAT
    - ANSI X9.31 Appendix A.2.4 PRNG KAT
    - HMAC SHA-1 (known answer test performed as part of power-up integrity test)
    - SHA-1 (known answer test performed as part of HMAC SHA-1 known answer test)

The Vocera Cryptographic Module performs the following conditional self-tests:

- Continuous PRNG test (CRNGT) for FIPS-Approved random number generator

The module is capable of performing on-demand self-tests via power cycle, which restarts the module. If any error occurs during the power-up self-test execution, the module enters an error state and outputs the error over the module's status output interface. If the module encounters an error during a conditional self-test, it will transition to a soft error state and attempt to clear the error on its own. Failing to clear the soft error leads the module to an error state and operator intervention is required at that point. An operator may attempt to clear a power-up or conditional self-test error by restarting the module (which requires power-cycling the host badge); however, if the error does not clear, then the Badge must be sent to Vocera for service.

2.8 Mitigation of Other Attacks

The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Vocera Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in a FIPS-Approved mode of operation.

3.1 Initial Setup

The module operates on a Vocera B2000 Badge, and uses both a general-purpose and a proprietary OS. The module inherently operates in single-user mode due to the fact that only one operator can be in possession of the Vocera badge hosting the module at any given time.

While the module itself operates only in a FIPS-Approved mode of operation, the Vocera badge must be configured to support the use of the module. The Crypto-Officer is responsible for configuring the Vocera badge to make proper use of the module.

The CO must enable FIPS support on the badge properties via the Vocera Software System. Instructions to manage the Vocera badge via the Vocera Software System are provided in the *Vocera Badge Configuration Guide* document available to the Crypto-Officer via Vocera's website (http://vocera.com/documentation/default.aspx). Vocera Software System provides user-friendly utility tools and a web-based administrator console to configure and manage the entire Vocera system.

Vocera badges are configured to make use of the Vocera Cryptographic Module by updating a badge configuration file called "badge.properties". This update is accomplished via a utility called the Badge Properties Editor. Instructions on updating the badge.properties file to employ the module are as follows:

1. From the Windows **Start** menu, choose Programs > Vocera > Badge Utilities > Badge Properties Editor.

   The Badge Properties Editor will appear.

2. From the **Badge Type** drop-down menu, choose "B2000".

3. Select the **Security** tab (shown in Figure 6 below) and do the following:

   - Check the "Enable FIPS" checkbox.
   - From the **Authentication** drop-down menu, select "WPA-PSK" or "WPA-PEAP".
   - From the **Encryption** drop-down menu, select "AES-CCMP"

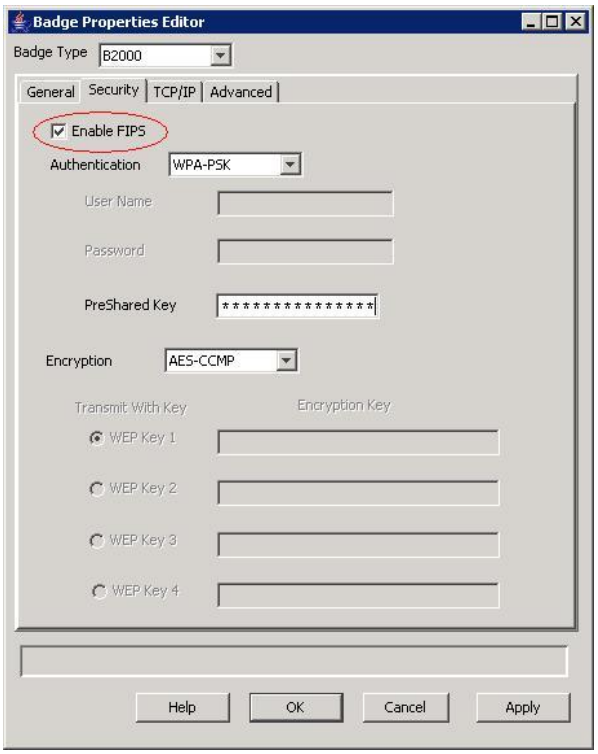

Figure 6 – Configuring the Badge Property File for FIPS Support

4. Press "OK" or "Apply" to save any changes.

5. Restart the Vocera Server from the web-based administrator console as instructed in the *Vocera Administration Guide*. The document can be found in Vocera's website (http://vocera.com/documentation/default.aspx).

   The badges.properties file on any connected badges will be automatically updated upon Server restart.

The badge operator must use the Info Menu on the badge to see the status of FIPS Mode. At this point, FIPS Mode should display that it is set to "on" without operator intervention. The version will show "1.0".

3.2 Crypto-Officer Guidance

While the Vocera badge must be configured to use the module, the module itself requires no set-up, as it only executes in a FIPS-Approved mode of operation. When the module is powered up, it runs the power-up self-tests. If the power-up self-tests complete successfully, the module is deemed to be operating in a FIPS-Approved mode of operation. Successful power-up self-tests displays the following message on the badge display screen.

"Power On Self Tests successful."

3.2.1 Management

The CO is also responsible for monitoring that the Vocera badge's FIPS configuration is maintained by using only FIPS-Approved functions. To maintain the FIPS configuration, the CO must ensure that 'ssh' services are disabled and that only those algorithms mentioned in Section 2.6 (Cryptographic Key Management) of this document are in use. Cisco Centralized Key Management (CCKM) is also disabled in the Vocera badge by default. The CO must not enable the protocol when running the badge in its FIPS configuration.

NOTE: The 'Vocera Only' option from the badge menu must not be used when running the badge in its FIPS configuration.

3.2.2 Zeroization

Since none of the cryptographic keys are stored persistently, they can be zeroized from SDRAM by simply powering off the Vocera badge. The only exception is the seed key which is hard-coded inside the module. In order to remove this key, the module's binaries must be replaced by re-applying the badge image. The CO can accomplish badge image re-application by selecting the 'Factory Reset' option from the Vocera Badge menu. Selection of this option will result in the application the badge's factory image (thus zeroizing the hard-coded seed key). At this point, the badge operator will need to follow the steps provided in both the "Restoring Factory Settings" section of the Vocera Badge Configuration Guide and Section 3.1 of this Security Policy to ensure that the module is operating in its FIPS-Approved manner.

3.3 User Guidance

Users employ the secure communications services provided by the module (listed in Table 4). Users are not responsible for the module's configuration. There is no specific guidance for Users, as the module always operates in a FIPS-Approved mode of operation.

4 Acronyms

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CCKM	Cisco Centralized Key Management
CCM	Counter Mode with Cipher Block Chaining - Message Authentication Code
CCMP	CCM Protocol
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CODEC	Coder/Decoder
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
DND	Do Not Disturb
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
MD	Message Digest
MIC	Microphone
N/A	Not applicable
NIST	National Institute of Standards and Technology
OS	Operating System
PBX	Private Branch Exchange
PEAP	Protected Extensible Authentication Protocol
PMK	Pairwise Master Key
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, and Adleman
RTC	Real-Time Clock
SDRAM	Synchronous Dynamic Random Access Memory
TI	Texas Instruments

Acronym	Definition
TLS	Transport Layer Security
VCM	Vocera Cryptographic Module
WLAN	Wireless Local Area Network