Vocera Communications, Inc.

Vocera Cryptographic Module v3.0

Hardware Part Number: 88W8787; Software Version: 3.0; Firmware Version: 3.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.7

Prepared for:

Vocera Communications, Inc.
525 Race Street

San Jose, CA 95126
United States of America

Phone: +1 408 882 5100
www.vocera.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Vocera Cryptographic Module v3.0 from Vocera Communications, Inc. (Vocera). This Security Policy describes how the Vocera Cryptographic Module v3.0 meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which 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) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Vocera Cryptographic Module v3.0 is referred to in this document as the VCM 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 (www.vocera.com) contains information on the full line of products from Vocera.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

2. Vocera Cryptographic Module v3.0

2.1 Overview

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

- The Vocera Server System Software, which runs on a standard Windows server, controls and manages call activity.
- The Vocera B3000n Communications Badge allows users to converse over a Wireless Local Area Network (WLAN).

A typical Vocera system deployment is shown in Figure 1 below. The following acronyms that are previously undefined appear in Figure 1:

- LAN – Local Area Network
- PBX – Private Branch Exchange

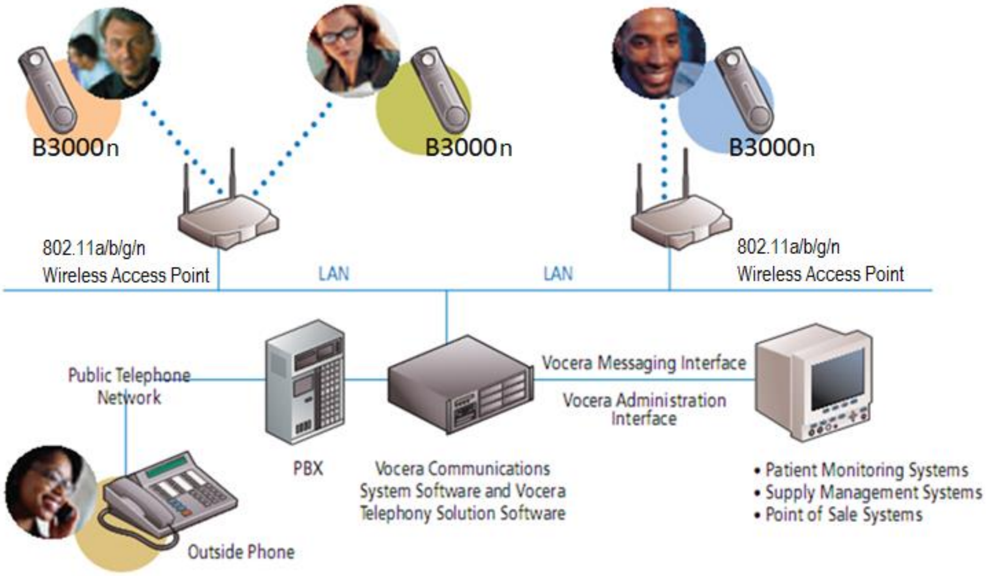

B3000n
B3000n
B3000n
802.11a/b/g/n
Wireless Access Point
LAN
LAN
802.11a/b/g/n
Wireless Access Point
Public Telephone Network
PBX
Vocera Messaging Interface
Vocera Administration Interface
Vocera Communications System Software and Vocera Telephony Solution Software
• Patient Monitoring Systems
• Supply Management Systems
• Point of Sale Systems
Outside Phone

Figure 1 – Typical Vocera Communications System Deployment

The Vocera B3000n 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 Server System Software (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 PBX. The badge employs a high-performance antenna for improved transmit and receive sensitivity.

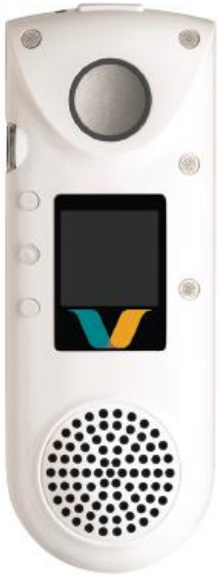


Figure 2 – Vocera B3000n Communications Badge

Communications are protected via industry-standard secure wireless communications protocols. The security functionality is provided by the VCM embedded in the badge. Various applications on the Vocera B3000n Communications 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.

The VCM is validated at the FIPS 140-2 Section levels shown in Table 1.

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[1]/EMC[2]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A[3]

[1] EMI – Electromagnetic Interference

[2] EMC –Electromagnetic Compatibility

[3] N/A – Not Applicable

2.2 Module Specification

The VCM is a software-hybrid cryptographic module with an overall security level of 1, supporting both an Approved mode of operation and non-Approved mode of operation. Please refer to Section 3.4 of this Security Policy for details regarding the non-Approved mode of operation.

The module consists of four software libraries and a high-performance Marvell chip.

- The four software libraries are fips_libbadgecrypto.so, fips_rsa_sig_verify.so, mlan.ko, and sd8787.ko (collectively versioned as version 3.0). The software libraries are stored in Flash and execute on a Texas Instruments applications processor (part number OMAPL138). The fips_libbadgecrypto.so and fips_rsa_sig_verify.so libraries provide AES, HMAC SHA-1, HMAC SHA-256, CMAC, DRBG, and RSA signature verification services, whereas mlan.ko and sd8787.ko provide the API to the Marvell chip.

- The Marvell Avastar WLAN SoC[4] (part number 88W8787) holds and executes its associated firmware (sd8787_uapsta.bin). The chip firmware is version 3.0.

The logical cryptographic boundary surrounds all of the components listed above. Physically, the module takes on the characteristics of the host device, the Vocera B3000n Communications Badge. Thus, the physical cryptographic boundary is the hard plastic badge enclosure, and the module is defined as having a multiple-chip standalone embodiment. See Figure 3 below for an illustration of the module components and boundaries.

[4] SoC – System on a Chip

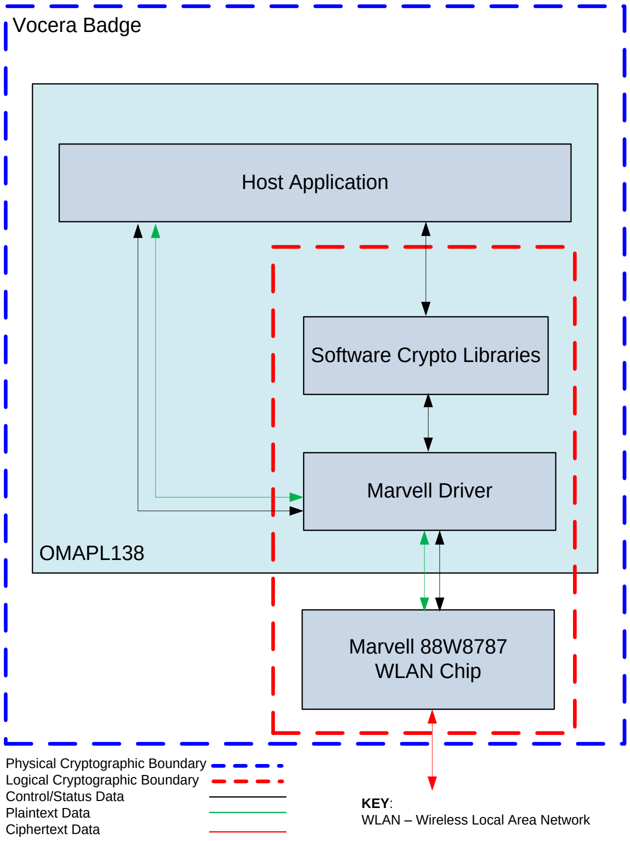


Figure 3 – Module Cryptographic Boundaries

The module implements the FIPS-Approved algorithms listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Algorithm	Standard	Certificate Number	
		Software Libraries	Marvell Chip Firmware
AES[5] in CBC[6] encryption/decryption with 128-bit keys	FIPS 197	#3532	-
AES in ECB[7] and CCM[8] encryption/decryption with 128-bit keys	FIPS 197	-	#3531
RSA[9] Signature Verification (PKCS[10] #1 v1.5) with 1024, 1536, 2048, 3072, and 4096-bit keys	FIPS 186-2	#1815	-
RSA Signature Verification (PKCS[11] #1 v1.5) with 1024, 2048, and 3072-bit keys	FIPS 186-4	#1815	-
SHA[12]-1 and SHA-256	FIPS 180-4	#2912	-

[5] AES – Advanced Encryption Standard
[6] CBC – Cipher Block Chaining
[7] ECB – Electronic Code Book
[8] CCM – Counter with CBC-MAC
[9] RSA – Rivest, Shamir, Adleman
[10] PKCS – Public Key Cryptography Standard
[11] PKCS – Public Key Cryptography Standard
[12] SHA – Secure Hash Algorithm

Algorithm	Standard	Certificate Number	
		Software Libraries	Marvell Chip Firmware
HMAC[13] with SHA-1 and SHA-256	FIPS 198	#2257	-
CMAC[14] generation and verification with 128-bit AES keys	NIST SP[15] 800-38B	#3532	-
Hash-based DRBG[16]	NIST SP 800-90A	#888	-
Components Validation List: Section 4.2, TLS[17]-KDF[18]	NIST SP 800-135	#586	-

Note: The TLS protocol has not been reviewed or tested by the CAVP or CMVP.

The module implements the following non-Approved security functions. These algorithms and protocols are allowed for use in a FIPS-Approved mode of operation:

- Non-Deterministic Random Number Generator (NDRNG)
  - Used as an entropy input source for the module's Approved DRBG. Each call to the entropy source requests 256 bits for entropy input or 128 bits for the DRBG's nonce.
- RSA key transport (allowed for use in the FIPS-Approved mode of operation)
  - **Caveat:** RSA (key transport; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- Message Digest 5 (MD5)
  - Used only as an underlying algorithm within the module's key transport schemes (TLS, EAP[19]-TLS, and PEAP[20]) and, as such, are allowed for use per FIPS Implementation Guidance D.9
- HMAC MD5
  - Used only as an underlying algorithm within the module's key transport schemes (TLS, EAP-TLS, and PEAP), and as such, are allowed for use per FIPS Implementation Guidance D.9

2.3 Module Interfaces

The module interfaces exist at the module's logical cryptographic boundary. Thus, while included here for completeness, the Vocera B3000n Communications Badge is not within the logical boundary of the cryptographic module, and the module's interfaces are not implemented at this boundary. Only the components within the logical boundary illustrated in Figure 3 above comprise the module, and it is at this boundary where the module's interfaces are implemented. However, at the physical boundary, the badge features the physical ports shown in Figure 4 below.

[13] HMAC – Hash-based Message Authentication Code
[14] CMAC – Cipher-based Message Authentication Code
[15] SP – Special Publication
[16] DRBG – Deterministic Random Bit Generator
[17] TLS – Transport Layer Security
[18] KDF – Key Derivation Function
[19] EAP – Extensible Authentication Protocol
[20] PEAP – Protected Extensible Authentication Protocol

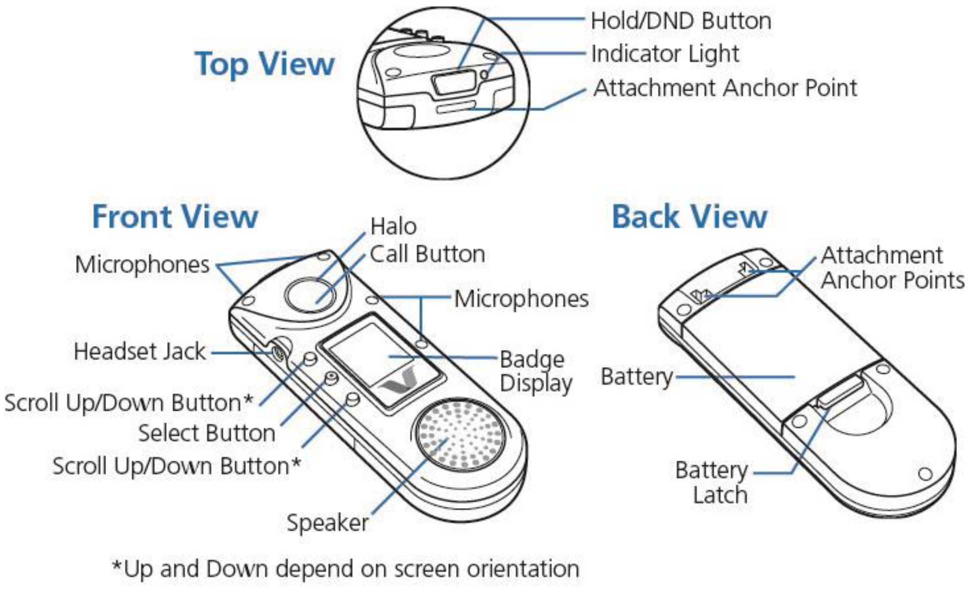


Figure 4 – Physical Features of the Vocera B3000n Communications Badge

The following is a list of the badge's physical interfaces:

- Badge display
- Buttons (call button, hold/DND[21] button, and menu buttons)
- Speaker
- Microphone
- Badge indicator light
- Call button halo
- Headset jack
- Contact pins
- WLAN unit

The badge's physical interfaces (manual controls, physical indicators, and physical ports) map to logical interfaces supported by the module. The module's logical interfaces exist at a low level in the software as APIs[22]. The APIs are grouped into four logically distinct categories:

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

Per FIPS 140-2 Implementation Guidance, a hybrid module's control input and status output interfaces are provided only via the software/firmware component of the module. Thus, the module's interfaces consist solely of the available APIs for the software libraries. The data and control inputs made via the badge microphone and buttons are translated into the logical data and control inputs made via the API calls to the software-hybrid

[21] DND – Do Not Disturb
[22] API – Application Programming Interface

module. Likewise, the data and status outputs made via API call returns from the software-hybrid module are translated into the data and status outputs made to the badge display, speaker, and status lights.

Table 3 below provides a mapping of the physical (i.e. badge) and logical (i.e. module) interfaces to the appropriate interface category.

Table 3 – Interface Mappings

Interface Category	Physical Interface	Logical Interfaces
Data Input	WLAN Unit, Microphone, Headset Jack	Function calls that accept, as their arguments, data to be used or processed by the module.
Data Output	WLAN Unit, Headset Jack, Speaker	Arguments for a function that specify where the result of the function is stored or returned as a return value.
Control Input	WLAN Unit, Call Button, Hold/DND Button (Hold to power-off), Menu Buttons	Function calls utilized to initiate the module and the function calls used to control the operation of the module.
Status Output	Badge Display, Badge Indicator Light, Call Button Halo	Return values for function calls
Power Input	Contact Pins	N/A

2.4 Roles and Services

There are two roles supported the module (as required by FIPS 140-2) that operators may assume: a Crypto-Officer (CO) role and a User role. Operators assume their desired role implicitly, based on the module service selected for execution. Please note that the keys and CSPs[23] listed in the tables below indicate the type of access required using the following notation:

- Read: The CSP is read.
- Write: The CSP is established, generated, modified, or zeroized.
- Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto-Officer Role

The CO role has the ability to manage the module and monitor the status. Descriptions of the services available to the CO role are provided in Table 4 below.

Table 4 – Crypto-Officer Services

Service	Description	Input	Output	CSP and Type of Access
Self-Test execution	Run power-up self-tests on demand	API call or cycling power	Status output	None
Status monitoring	Monitor status	Command	Status output	None

[23] CSP – Critical Security Parameter

2.4.2 User Role

The User role is used to secure communication services. Descriptions of the services available to the User role are provided in Table 5 below.

Table 5 – User Services

Service	Description	Input	Output	CSP And Type Of Access
Crypto operation initiation	Creates an environment to carry out cryptographic operation	API call	Encrypted or decrypted data	None
Random number generation	Generate random number based on SP 800-90A Hash-based DRBG	API call	Random bits	DRBG Seed – Read, Write, Execute DRBG C Value – Read, Execute
EAPOL[24]-Key Message operations	Format EAPOL-Key message	API call	Status output	802.11i/r/w Pair-Wise Master Key (PMK) – Read, Execute
EAPOL operation	Transmit and receive EAP messages using EAPOL	API call	Status output	802.11i/r/w PMK – Read, Write, Execute
OKC[25] operation	Performs Opportunistic Key Caching operation	API call	Status output	802.11i/r/w PMK – Read, Execute
Four-way handshake processing	Process four-way handshake	API call	Status output	802.11i/r/w PMK – Read, Execute 802.11i/r/w Temporal Key – Write, Execute
HMAC operation	Generate HMAC value	API call with data input	HMAC value and status output	HMAC Key – Read, Execute
PEAP operation	Perform PEAP operation	API call with data	Secure tunnel establishment	RSA Server Public Key – Read, Execute RSA Client Private Key – Read, Execute TLS Authentication Key – Execute TLS Session Key – Execute 802.11i/r/w PMK – Read, Write, Execute DRBG Seed – Execute DRBG C Value – Read, Execute
EAP-TLS operation	Perform EAP-TLS operation	API call with data	Secure tunnel establishment	RSA Server Public Key – Read, Execute RSA Client Private Key – Read, Execute TLS Authentication Key – Execute TLS Session Key – Execute 802.11i/r/w PMK – Read, Write, Execute DRBG Seed – Execute DRBG C Value – Read, Execute
Hashing operation	Generate SHA-1 digest	API call with data input	Digest value and status output	None
TLS operation	Perform TLS operation	API call with data	Secure tunnel establishment	TLS Authentication Key – Write, Execute TLS Session Key – Write, Execute

[24] EAPOL – Extensible Authentication Protocol over Local Area Network

[25] OKC – Opportunistic Key Caching

Service	Description	Input	Output	CSP And Type Of Access
Zeroization	Zeroize keys utilized by the module	CSP to be zeroized, CSP type	Zeroization status	RSA Server Public Key – Write RSA Client Private Key – Write TLS Authentication Key – Write TLS Session Key – Write 802.11i/r/w PMK – Write 802.11i/r/w Temporal Key – Write HMAC Key – Write DRBG Seed – Write DRBG C Value – Read

2.5 Physical Security

The VCM is a software-hybrid module, which FIPS defines as a multiple-chip standalone embodiment. The module consists of production-grade components that include standard passivation techniques, meeting level 1 requirements.

2.6 Operational Environment

The module is intended for use on a Vocera B3000n Communications Badge running Vocera Embedded Linux Version 3.0. The software libraries run on the OMAP-L138 processor, while the Marvell WLAN chip runs its own special-purpose firmware.

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 communications badge (which hosts the module) at any given time. The module is not intended to operate on any platform other than the Vocera B3000n Communications 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 (OS) uses its native memory management mechanisms to ensure that outside processes cannot access the process space used by the module.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6.

Table 6 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
RSA Server Public Key	1024, 1536, 2048, 3072, 4096-bit RSA public key	Externally generated; automatically downloaded to the module	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Used for signature verification; key transport during TLS handshake for PEAP and EAP-TLS phase 1
RSA Client Private Key	2048, 4096-bit RSA private key	Externally generated; automatically downloaded to the module	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Used with client-side certificates for authentication in EAP-TLS
TLS Authentication Key	160-bit HMAC SHA-1 key	Internally generated OR Externally generated; input in ciphertext	Encrypted during TLS handshake	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Used for data authentication for TLS sessions for PEAP Phase 2 and EAP-TLS
TLS Session Key	128-bit AES key	Internally generated OR Externally generated; input in ciphertext	Encrypted during TLS handshake	Reside on volatile memory only in plaintext	Power cycle or after the TLS session is closed	Used for encryption and decryption of TLS session authentication-related messages in PEAP Phase 2 and EAP-TLS
802.11i/r/w Pairwise Master Key	256-bit shared secret	For Pre-shared: externally generated; enters the module in plaintext For PEAP and EAP-TLS: internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the 802.11i/r/w session is closed	Used as partial input to construct the Temporal Key used in the 802.11i/r/w protocol
802.11i/r/w Temporal Key	128-bit AES key	Internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or after the 802.11i/r/w session is closed	Used to create secure tunnel for wireless data transmission.

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
HMAC Key	128, 160, 256-bit HMAC SHA-1 key 256-bit HMAC SHA-256 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
AES CMAC Key	128-bit AES CMAC 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
802.11w Integrity Group Temporal Key	128-bit AES CMAC 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 data integrity check for group addressed Management frame
DRBG Seed	440 bits of seed value	Internally generated using nonce along with entropy input	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or reboot	Used for the DRBG
DRBG C Value	Internal Hash_DRBG state value	Internally generated	Never exits the module	Reside on volatile memory only in plaintext	Power cycle or reboot	Used for the DRBG

2.8 EMI / EMC

The module is a software-hybrid module and depends on the target platform for its physical characteristics. The VCM is not a radio device. However, the module's target platform is a Vocera B3000n Communications Badge, which is considered a radio device. The Vocera B3000n Communications Badge has been tested and found compliant with Subparts B, C, and E of Part 15 of the Federation Communications Commission (FCC) rules (CFR[26] title 47) for Class A digital devices.

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and loaded into memory as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and error resolutions.

2.9.1 Power-Up Self-Tests

The module performs a series of FIPS-required self-tests at power-up. These tests are performed automatically, without the need for operator intervention. The module is capable of performing the power-up self-tests on-demand via power cycle, which restarts the module.

The VCM 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 KAT for encrypt and decrypt
    - AES CCM KAT for encrypt and decrypt
    - AES CBC KAT for encrypt and decrypt
    - AES CMAC KAT for encrypt and decrypt
    - SHA-1 KAT (performed as part of Software Integrity Check)
    - SHA-256 KAT
    - HMAC SHA-1 KAT (performed as part of Software Integrity Check)
    - HMAC SHA-256 KAT
    - Hash-based DRBG KAT
    - RSA Signature Verification KAT

The module also performs the following critical function self-test at power-up:

- TLS-KDF KAT

2.9.2 Conditional Self-Tests

The module performs a series of FIPS-required self-tests operationally when the module generates a random value. These tests are performed automatically, without the need for operator intervention. The VCM performs the following conditional self-tests:

[26] CFR – Code of Federal Regulations

- CRNGT for the non-Approved NDRNG
- CRNGT for the FIPS-Approved DRBG

2.9.3 Self-Test Failure Handling

Failure of any power-up self-test or the conditional CRNGT for the non-Approved NDRNG will result in the module entering a critical error state immediately. For the conditional CRNGT for the Approved DRBG, a newly-produced set of random bits is compared to the previously-produced set of random bits. If they are equal, then the test is failed and the module will enter a soft error state. The module will then generate a new set of random bits and perform the comparison again. If the test is failed a second time, the module will enter a critical error state.

Upon reaching the critical error state, the module outputs a failure message over the module's status output interface. The module will then immediately terminate the host application and either (1) restart the host application or (2) reboot the badge. See Table 7 below for a list of self-test failure actions and messages.

Table 7 – Self-Test Failure Actions and Messages

Self-Test	Failure Action		Failure Message
	Restart Host Application	Reboot Badge	
Firmware Integrity Check using HMAC SHA-1		X	"Integrity check of [module file name] Power On Self Test failed. Rebooting system in <n>* seconds."
Software Integrity Check using HMAC SHA-1		X	"Integrity check of [module file name] Power On Self Test failed. Rebooting system in <n> seconds."
AES ECB KAT		X	"AES ECB Decryption Power On Self Test failed. Rebooting system in <n> seconds."
		X	"AES ECB Encryption Power On Self Test failed. Rebooting system in <n> seconds."
AES CCM KAT		X	"AES CCM Encryption Power On Self Test failed. Rebooting system in <n> seconds."
		X	"AES CCM Decryption Power On Self Test failed. Rebooting system in <n> seconds."
AES CBC KAT		X	"AES CBC Encryption Power On Self Test failed. Rebooting system in <n> seconds."
		X	"AES CBC Decryption Power On Self Test failed. Rebooting system in <n> seconds."
AES CMAC KAT		X	"AES CMAC Power On Self Test failed. Rebooting system in <n> seconds."
SHA-1 KAT		X	[refer to Software Integrity Check using HMAC SHA-1]
SHA-256 KAT		X	"SHA256 Power On Self Test failed. Rebooting system in <n> seconds."
HMAC SHA-1 KAT		X	[refer to Software Integrity Check using HMAC SHA-1]
HMAC SHA-256 KAT		X	"HMAC SHA256 Power On Self Test failed. Rebooting system in <n> seconds."

Self-Test	Failure Action		Failure Message
	Restart Host Application	Reboot Badge	
Hash-based DRBG KAT		X	"DRBG Power On Self Test failed. Rebooting system in <n> seconds."
	x		"RBG[27] KAT for Instantiate failed. Restarting. Restarting application in <n> seconds."
	x		"RBG Invalid parameter specified for Instantiate. Restarting. Restarting application in <n> seconds."
	x		"RBG KAT for Reseed failed. Restarting. Restarting application in <n> seconds."
	x		"RBG Invalid parameter specified for Reseed. Restarting. Restarting application in <n> seconds."
	x		"RBG KAT for Generate failed. Restarting. Restarting application in <n> seconds."
	x		"RBG Invalid parameter specified for Generate. Restarting. Restarting application in <n> seconds."
	x		"RBG KAT for Uninstantiate failed. Restarting. Restarting application in <n> seconds."
RSA Signature Verification KAT		X	"RSA Sigver Power On Self Test failed. Rebooting system in <n> seconds."
CRNGT for DRBG	x		"RBG Continuous Test failed. Restarting. Restarting application in <n> seconds."
CRNGT for NDRBG		X	"RBG Entropy input continuous test failed. Rebooting. Rebooting system in <n> seconds."
	x		"Unable to process RBG entropy source. Restarting. Restarting application in <n> seconds."
		X	"Unable to open RBG entropy source. Rebooting. Rebooting System in <n> seconds."
		X	"Unable to get requested RBG entropy. Rebooting. Rebooting System in <n> seconds."
	x		"Unknown entropy source specified. Rebooting. Restarting application in <n> seconds."
TLS-KDF KAT		X	"TLS KDF Power On Self Test failed. Rebooting system in <n> seconds."

*<n> is a countdown from 10 to 1

If the error state persists through the automatic restart/reboot, an operator may attempt to manually clear the 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.

[27] RBG – Random Bit Generation

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3. Secure Operation

The VCM meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The module operates on the Vocera B3000n Communications 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 communications badge hosting the module at any given time.

The Vocera B3000n Communications Badge must be configured to support the use of the module in its FIPS-Approved mode. The CO is responsible for configuring the communications badge to make proper use of the module.

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

Vocera B3000n Communications Badges are configured to make use of the VCM 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:

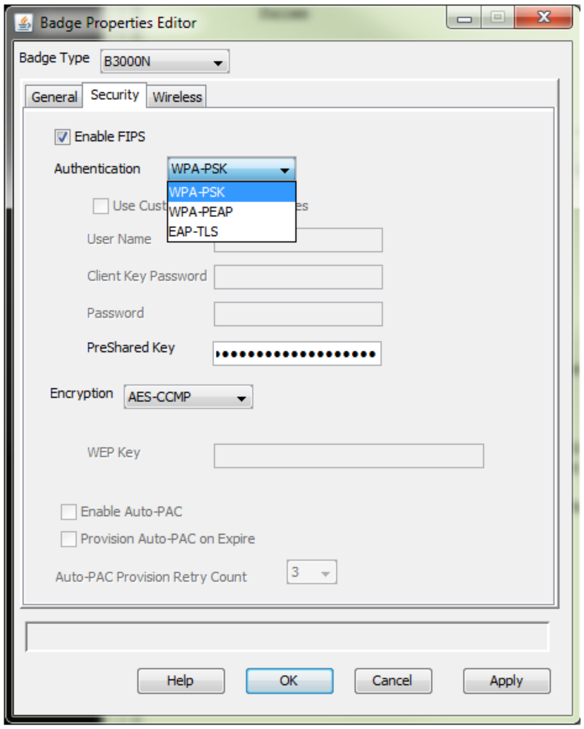
1. From the Windows **Start** menu, choose Start > All Programs > Vocera > Badge Properties Editor. The Badge Properties Editor will appear.
2. From the **Badge Type** drop-down menu, choose "B3000n".
3. Select the **Security** tab (shown in Figure 5 below) and do the following:

   - Check the "Enable FIPS" checkbox.
   - From the **Authentication** drop-down menu, select "WPA[28]-PSK[29]", "WPA-PEAP", or "EAP-TLS".
   - From the **Encryption** drop-down menu, select "AES-CCMP[30]"

[28] WPA – Wi-Fi Protected Access

[29] PSK – Pre-Shared Key

[28] CCMP – Counter with CBC-MAC Protocol



Badge Type: B3000N

☑ Enable FIPS

Authentication: WPA-PSK

PreShared Key: ••••••••••••••••••••

Encryption: AES-CCMP

Figure 5 – Configuring the Badge Property File for FIPS Support

4. Press "Apply" and then "OK" 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). 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 home screen 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 "VERSION: 3.0".

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

3.2 Secure Management

The following sections provide guidance to ensure that the module is operating in its FIPS-Approved configuration. The CO is responsible for making sure the module is running in FIPS-Approved mode of operation using the steps provided in Section 3.1 above.

3.2.1 Initialization

While there is no means to configure the module directly, the communications badge must be configured to use the module in its FIPS-Approved mode of operation. Thus, with the proper badge configuration, the module runs the power-up self-tests automatically when it is powered up, it. 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."
```

3.2.2 Management

The CO is also responsible for monitoring that the Vocera B3000n Communications Badge's FIPS configuration is maintained by using only FIPS-Approved functions. To maintain the FIPS configuration, the CO must ensure that that only those algorithms mentioned in Section 2.7 (Cryptographic Key Management) of this document are in use. Cisco Centralized Key Management (CCKM) is also disabled in the Vocera B3000n Communications Badge by default. The CO must confirm that CCKM is disabled when running the badge in its FIPS configuration by verifying that the CCKM checkbox remains unchecked under the **Wireless** tab of the Badge Properties Editor.

3.2.3 Zeroization

The module does not provide a facility to persistently store its cryptographic keys. Any keys in SDRAM can be zeroized by simply powering off the communications badge. Additionally, the HMAC Integrity Key is used only in the performance of a power-up self-test, and thus is not subject to FIPS zeroization requirements as per FIPS Implementation Guidance 7.4.

3.3 User Guidance

Users are not responsible for the badge's configuration; this is the responsibility of the CO. Users employ the secure communications services provided by the module (listed in Table 5). For guidance on using the Vocera B3000n Communications Badge, please refer to the *Vocera Badge User Guide*. The document can be found in Vocera's website (http://vocera.com).

3.4 Non-Approved Mode

If the Vocera badge is not properly configured, the host application may invoke non-Approved algorithms. When operated in this fashion, the module can switch between an Approved mode of operation and a non-Approved mode of operation on a service-by-service basis. The module will transition to the non-Approved mode of operation when the "PEAP operation" or "EAP-TLS operation" service is invoked using RSA key transport with RSA that provides less than 112 bits of encryption strength. The module transitions back to the Approved mode of operation upon the utilization of an Approved security function.

3.4.1 Roles and Services

The module supports the Crypto Officer and User roles while in the non-Approved mode of operation.

In the Approved mode of operation, the module supports the WPA-PSK, WPA-PEAP and EAP-TLS network port authentication protocols. In the non-Approved mode of operation, the module supports the following authentication protocols:

- WPA-PSK
    - AES-CCMP (non-compliant)
    - TKIP[31]-WPA
- WPA-PEAP

[31] TKIP – Temporal Key Integrity Protocol

  - AES-CCMP (non-compliant)
  - TKIP-WPA
- LEAP (including the use of CCKM)
  - AES-CCMP (non-compliant)
  - TKIP-WPA
  - WEP[32]64
  - WEP128
- EAP-FAST
  - AES-CCMP (non-compliant)
  - TKIP-WPA

Table 8 below lists the services available in the non-Approved mode of operation.

Table 8 – Non-Approved Services

Service	Operator		Description
	CO	User	
PEAP operation (non-compliant)		✓	Perform PEAP operation
EAP-TLS operation (non-compliant)		✓	Perform EAP-TLS operation
WPA-PSK (non-compliant)		✓	Perform WPA-PSK operation
LEAP operation		✓	Perform LEAP operation
EAP-FAST operation		✓	Perform EAP-FAST operation

3.4.2 Security Functions

The module employs the following non-Approved algorithms to support WEP (40-bit and 104-bit) and TKIP, as well as to support RC4[33]-based TLS cipher suites:

- RC4
- MD5
- HMAC MD5
- AES-CCMP (non-compliant)

[32] WEP – Wired Equivalent Protocol
[33] RC4 – Rivest Cipher 4

4. Acronyms

Table 9 provides definitions for the acronyms used in this document.

Table 9 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CCKM	Cisco Centralized Key Management
CCM	Counter with CBC-Message Authentication Code
CCMP	Counter with CBC-Message Authentication Code Protocol
CFR	Code of Federal Regulations
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DND	Do Not Disturb
DRBG	Deterministic Random Bit Generator
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over Local Area Network
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MD5	Message Digest 5
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology

Acronym	Definition
OKC	Opportunistic Key Caching
OS	Operating System
PBX	Private Branch Exchange
PEAP	Protected Extensible Authentication Protocol
PKCS	Public Key Cryptography Standard
PMK	Pairwise Master Key
PSK	Pre-Shared Key
RC4	Rivest Cipher 4
RSA	Rivest, Shamir, Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SoC	System on a Chip
SP	Special Publication
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
VCM	Vocera Cryptographic Module
WEP	Wired Equivalent Protocol
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Prepared by:
Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com