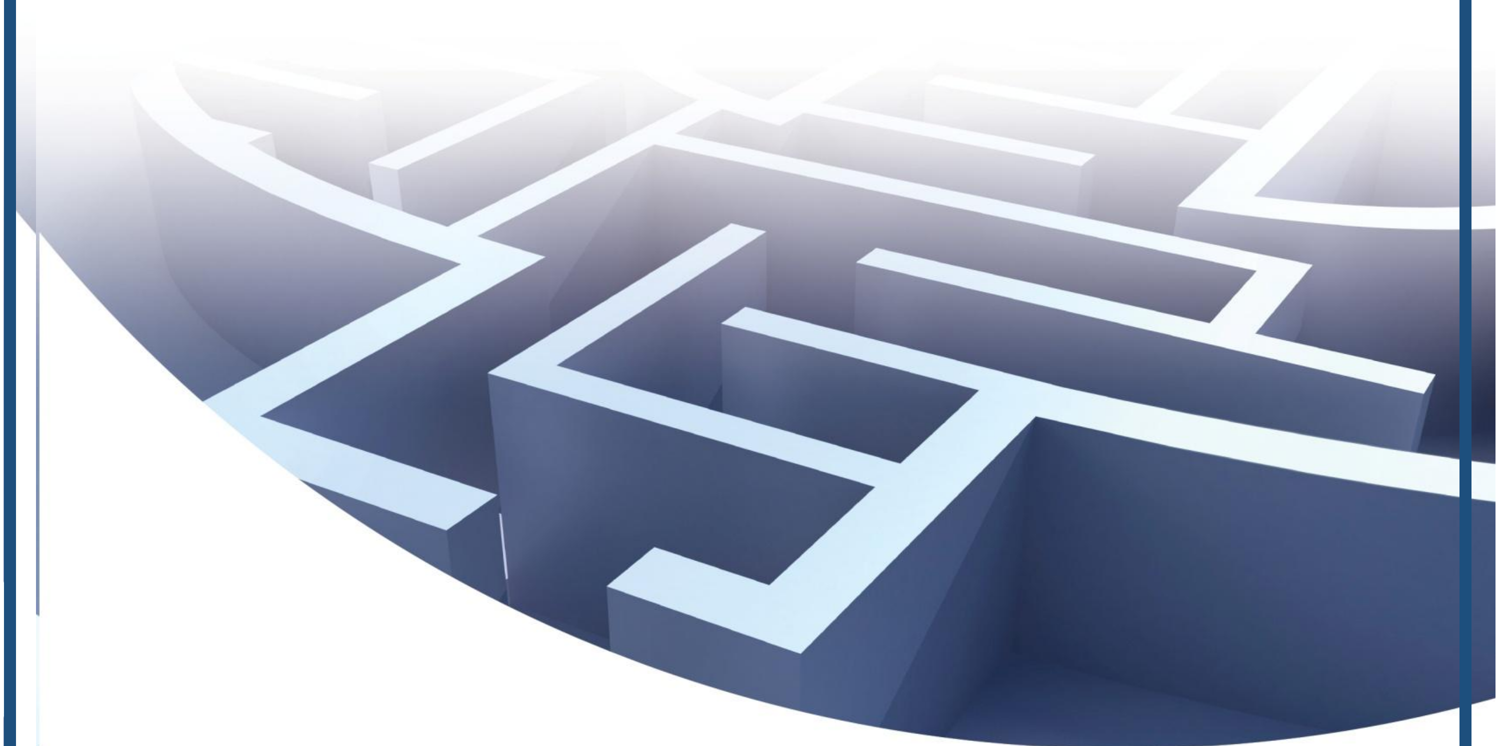
Vocera Communications, Inc.

Vocera Cryptographic Module

Hardware Version: 88W8688; Firmware Version: 2.0; Software Version: 2.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.5



Prepared for:

Vocera Communications, Inc.
525 Race Street
San Jose, CA 95126
United States of America

Phone: +1 (408) 882-5100
http://www.vocera.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

1 INTRODUCTION 3
 1.1 PURPOSE 3
 1.2 REFERENCES 3
 1.3 DOCUMENT ORGANIZATION 3
2 VOCERA CRYPTOGRAPHIC MODULE 4
 2.1 OVERVIEW 4
 2.2 MODULE SPECIFICATION 6
 2.3 MODULE INTERFACES 7
 2.4 ROLES AND SERVICES 8
  2.4.1 Crypto Officer Role 8
  2.4.2 User Role 8
 2.5 PHYSICAL SECURITY 10
 2.6 OPERATIONAL ENVIRONMENT 10
 2.7 CRYPTOGRAPHIC KEY MANAGEMENT 10
 2.8 SELF-TESTS 14
 2.9 EMI/EMC 14
 2.10 MITIGATION OF OTHER ATTACKS 14
3 SECURE OPERATION 15
 3.1 INITIAL SETUP 15
 3.2 CRYPTO-OFFICER GUIDANCE 16
  3.2.1 Management 17
  3.2.2 Zeroization 17
 3.3 USER GUIDANCE 17
4 ACRONYMS 18

Table of Figures

FIGURE 1 – TYPICAL VOCERA COMMUNICATIONS SYSTEM DEPLOYMENT 4
FIGURE 2 – VOCERA B3000 COMMUNICATIONS BADGE 5
FIGURE 3 – LOGICAL CRYPTOGRAPHIC BOUNDARY 6
FIGURE 4 – PHYSICAL FEATURES OF THE VOCERA B3000 BADGE 7
FIGURE 5 – PHYSICAL BLOCK DIAGRAM OF THE MODULE'S TARGET DEVICE 10
FIGURE 6 – CONFIGURING THE BADGE PROPERTY FILE FOR FIPS SUPPORT 16

List of Tables

TABLE 1 – SECURITY LEVEL PER FIPS 140-2 SECTION 5
TABLE 2 – FIPS 140-2 LOGICAL INTERFACE MAPPINGS 8
TABLE 3 – CRYPTO OFFICER SERVICES 8
TABLE 4 – USER SERVICES 9
TABLE 5 – FIPS-APPROVED ALGORITHM IMPLEMENTATIONS 11
TABLE 6 – CRYPTOGRAPHIC KEYS, CRYPTOGRAPHIC KEY COMPONENTS, AND CSPS 12
TABLE 7 – ACRONYMS 18

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 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 Canada (CSEC) 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 is referred to in this document as the cryptographic module, crypto-module, 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 (http://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.

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 Model document
- 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 Submission Package 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 Server System Software, which runs on a standard Windows server, controls and manages call activity.
- The Vocera B3000 Communications Badge allows users to converse over a Wireless Local Area Network (WLAN).

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

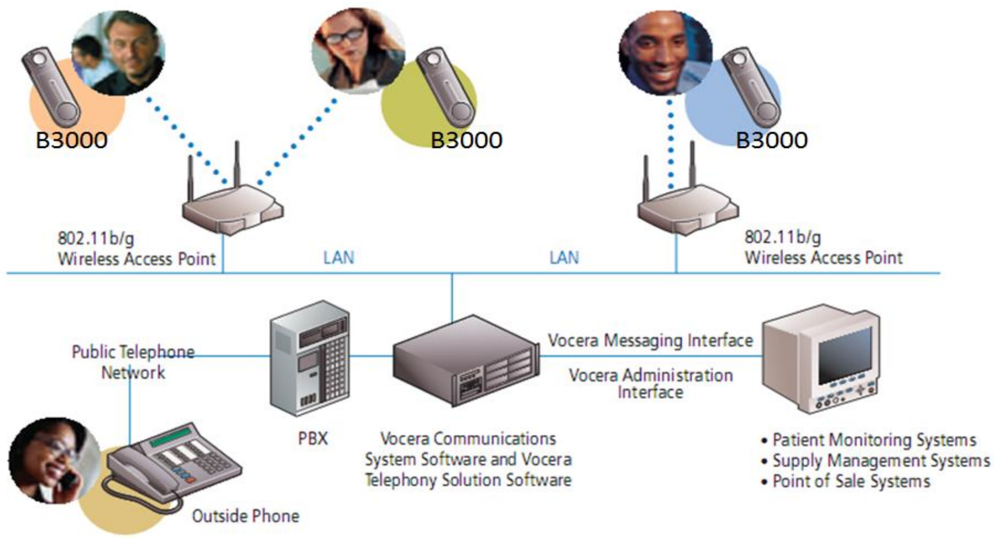


Figure 1 – Typical Vocera Communications System Deployment

The Vocera B3000 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 private branch exchange (PBX). The badge employs a high-performance antenna for improved transmit and receive sensitivity.

Figure 2 – Vocera B3000 Communications Badge

Communications are protected via industry-standard secure wireless communications protocols. The security functionality is provided by the Vocera Cryptographic Module 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 validated as a hybrid cryptographic module. A hybrid module is a special type of software or 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) and firmware running on a high-performance Marvell WLAN chip (part number 88W8688), and all of the required components are contained within the Vocera badge. The hybrid module software was tested on a Vocera B3000 badge using Vocera Embedded Linux Version 1.1 running on a Texas Instruments OMAP5912 (single-user mode).

Versioning for the module's components is as follows:

- Hardware Version: 88W8688
- Firmware Version: 2.0
- Software Version: 2.1

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

Section	Section Title	Level
7	Cryptographic Key Management	1
8	EMI/EMC[1]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

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 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.

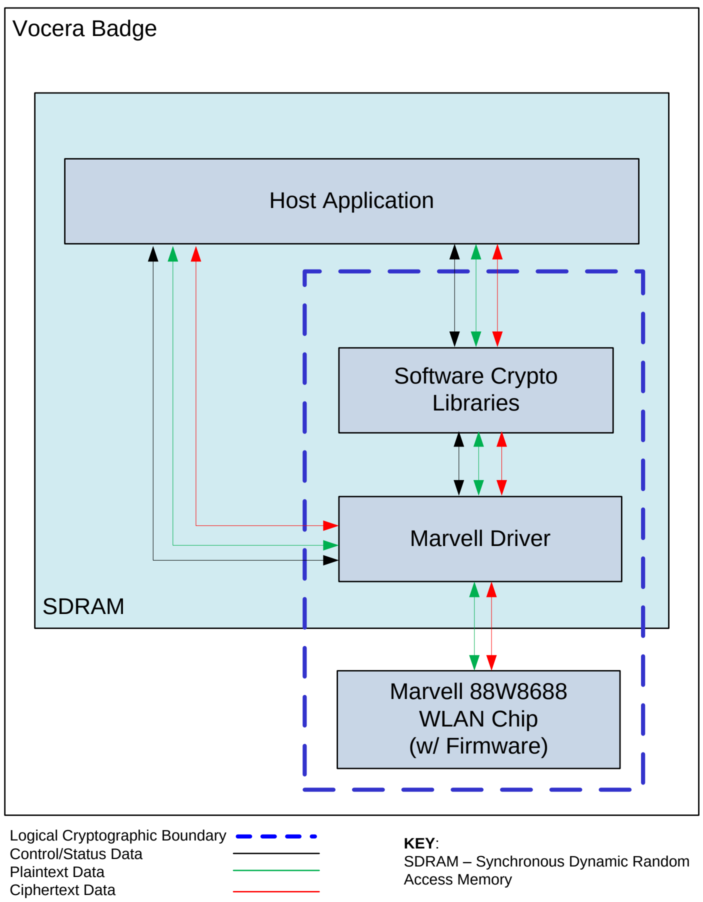


Figure 3 – Logical Cryptographic Boundary

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

2.3 Module Interfaces

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 B3000 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[2] button, and menu buttons)
- 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 B3000 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.

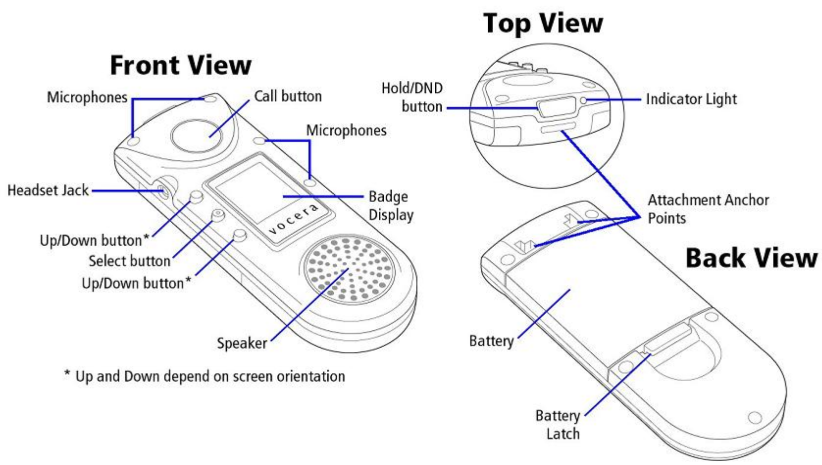


Figure 4 – Physical Features of the Vocera B3000 Badge

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 indicator light.

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

[2] DND – Do Not Disturb

Table 2 – FIPS 140-2 Logical 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.
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, Badge Indicator Light	Return values for function calls
Power Input	Power Interface	N/A

2.4 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.

2.4.1 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 Table 3 below. Please note that the keys and CSPs listed in the table indicate the type of access required using the following notation:

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

Table 3 – Crypto Officer Services

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

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 4 below.

Table 4 – User Services

Service	Description	Input	Output	CSP and Type of Access
Initiate crypto operation	Creates an environment to carry out cryptographic operation	API call	Encryption or decryption of data	None
Generate random number	Generate random number based on SP 800-90A Hash-based DRBG	API call	Random bits generation	DRBG Seed – R, W, X DRBG C Value – R, W, X
EAPOL[3]-Key Message operations	Format EAPOL-Key message	API call	Status output	802.11i Pairwise Master Key (PMK) – R, X
EAPOL operation	Transmit and receive EAP[4] messages using EAPOL	API call	Status output	802.11i PMK – R, W, X
OKC[5] operation	Performs Opportunistic Key Caching operation	API call	Status output	802.11i PMK – R, X
Four-way handshake	Process four-way handshake	API call	Status output	802.11i PMK – R, X 802.11i Temporal Key – W, X
HMAC operation	Generate HMAC value	API call with data input	HMAC generation and status output	HMAC key – R, X
Protected EAP (PEAP) operation ** (1024 and 1536 bit keys non-compliant)*	Perform PEAP operation	API call with data	Secured tunnel establishment	RSA public key – R, X TLS[6] Authentication Key – X TLS Session Key – X 802.11i PMK – R, W, X DRBG Seed – X DRBG C Value – R, W, X
EAP-TLS operation ** (1024 and 1536 bit keys non-compliant)*	Perform EAP-TLS operation	API call with data	Secure tunnel establishment	RSA public key – R, X TLS Authentication Key – X TLS Session Key – X 802.11i PMK – R, W, X DRBG Seed – X DRBG C Value – R, W, X
Hashing operation	Generate SHA-1 digest	API call with data input	Digest generation and status output	None
TLS operation	Perform TLS operation	API call with data	Secured tunnel establishment	TLS Authentication Key – W, X TLS Session Key –W, X
Zeroization	Zeroize keys utilized by the module	CSP to be zeroized, CSP type	Zeroization status	RSA Public Key – W TLS Authentication Key – W TLS Session Key – W 802.11i PMK – W 802.11i Temporal Key – W HMAC Key – W DRBG Seed – W DRBG C Value – R, W, X

[3] EAPOL –Extensible Authentication Protocol over Local Area Network
[4] EAP – Extensible Authentication Protocol
[5] OKC – Opportunistic Key Caching
[6] TLS – Transport Layer Security

2.5 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 B3000 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.

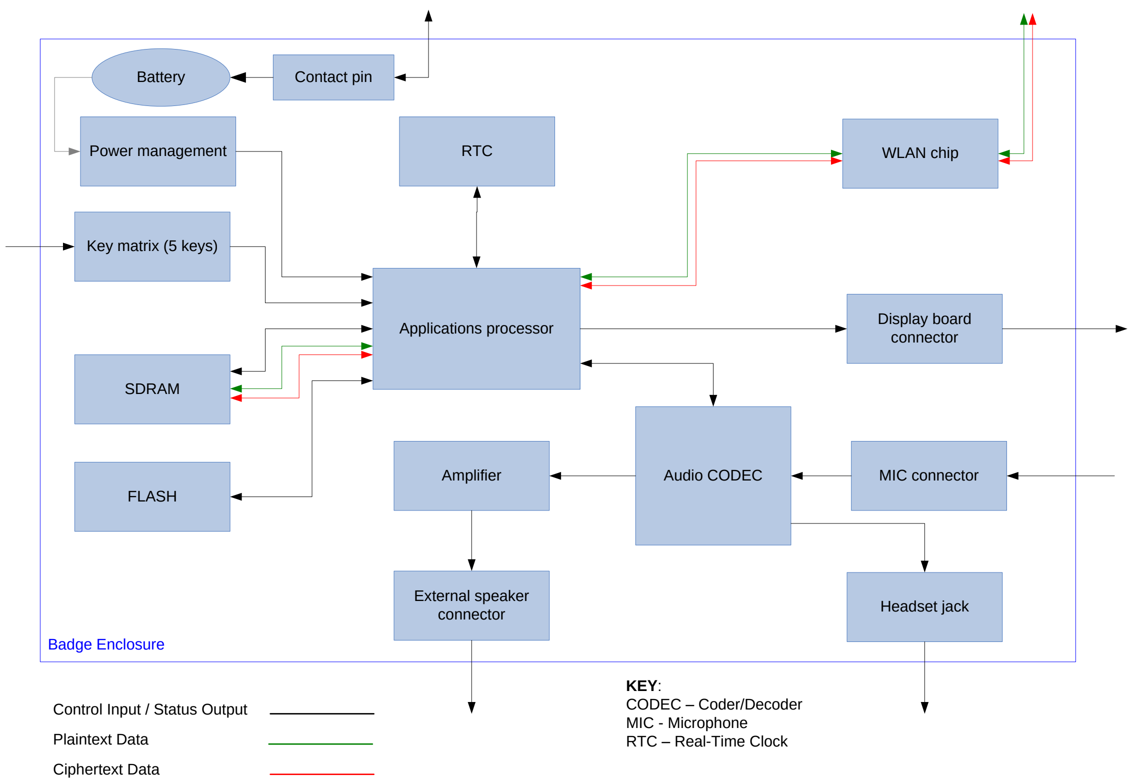


Figure 5 – Physical Block Diagram of the Module's Target Device

2.6 Operational Environment

The module is intended for use on a Vocera B3000 badge using Vocera Embedded Linux Version 1.1 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.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES 128-bit in CBC[7] mode	2225
AES 128-bit in ECB[8] and CCM[9] modes	2224
SHA-1	1914
HMAC using SHA-1	1353
RSA (PKCS[10] #1 v1.5) signature verification (1024/1536/2048/3072/4096 bits) ** (1024 and 1536 bit keys non-compliant)*	1139
Hash-based SP 800-90A DRBG	261

The module also implements the following non-FIPS-Approved algorithms:

- RSA key wrap[11] (allowed for use in the FIPS-Approved mode of operation)
- MD5[12]
- HMAC-MD5

Note that MD5 and HMAC-MD5 are used only as underlying algorithms 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.

[7] CBC – Cipher-Block Chaining
[8] ECB – Electronic Code Book
[9] CCM – Counter with Cipher Block Chaining-Message Authentication Code
[10] PKCS – Public-Key Cryptography Standards
[11] Caveat: RSA (key wrapping; key establishment methodology provides 112 to 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
[12] MD5 – Message Digest 5

The module supports the critical security parameters (CSPs) listed below in Table 6.

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

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
RSA Public Key	RSA 1024/1536/2048/3072/4096-bit public key ** (1024 and 1536 bit keys non-compliant)*	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	Signature verification; Key transport during TLS handshake for PEAP and EAP-TLS 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 and EAP-TLS
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 and EAP-TLS
802.11i 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 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.

.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
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
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 SP 800-90 Hash_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 SP 800-90 Hash_DRBG

2.8 Self-Tests

The module performs a series of FIPS-required self-tests both at power-up and operationally as certain conditions dictate. 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 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 KATs
    - AES CBC mode KAT
    - Hash-based DRBG KAT
    - HMAC-SHA-1 KAT (performed as part of power-up integrity test)
    - SHA-1 KAT (performed as part of power-up integrity test)
    - RSA Signature Verification KAT

Additionally, the module performs the following conditional self-test:

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

If any power-up or conditional self-test fails, the module enters a critical error state and outputs the error over the module’s status output interface before terminating the host application (thus shutting down the module). An operator may attempt to 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.

2.9 EMI/EMC

The module is a software module, and depends on the target platform for its physical characteristics. However, the module’s target platform is a Vocera B3000 Communications Badge, which is considered a radio device. This device has been tested and found compliant with FCC 47 Code of Federal Regulations Part 15C and 15B, Class B requirements.

2.10 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 FIPS-approved mode of operation.

3.1 Initial Setup

The module operates on a Vocera B3000 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 Server Software System. Instructions to manage the Vocera badge via the Vocera Server Software System are provided in the *Vocera Badge Configuration Guide* document available to the Crypto-Officer via Vocera's website (http://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 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 "B3000".

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", "WPA-PEAP", or "EAP-TLS".

   - From the **Encryption** drop-down menu, select "AES-CCMP"

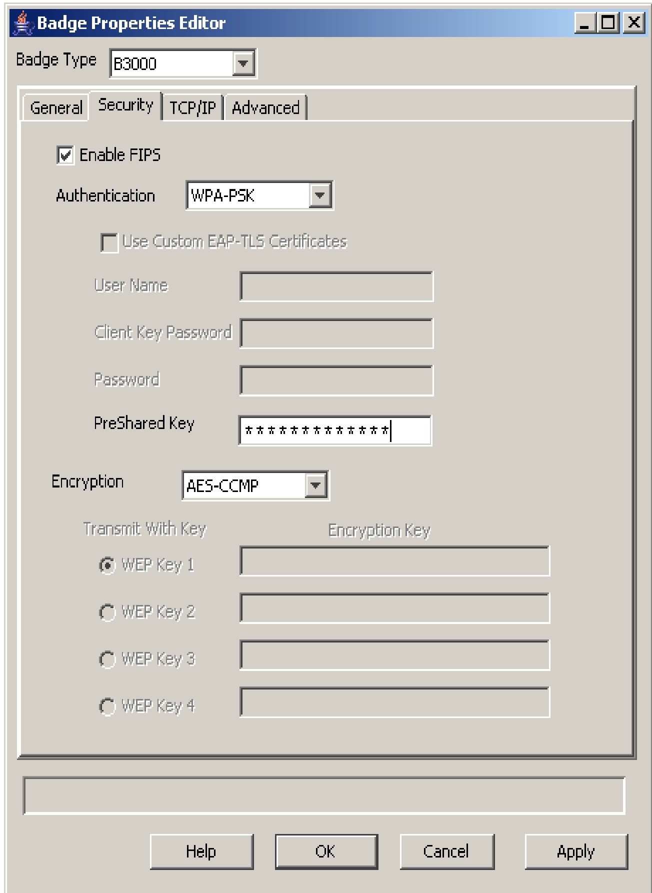


Figure 6 – Configuring the Badge Property File for FIPS Support

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).

   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 “2.1”.

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

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 2.7 (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.

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. 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 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

The Table 7 below describes the acronyms used in this document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
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
DRBG	Deterministic Random Bit Generator
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
OKC	Opportunistic Key Caching
OS	Operating System
PBX	Private Branch Exchange
PEAP	Protected Extensible Authentication Protocol

.

Acronym	Definition
PKCS	Public-Key Cryptography Standards
PMK	Pairwise Master Key
RSA	Rivest, Shamir, and Adleman
RTC	Real-Time Clock
SDRAM	Synchronous Dynamic Random Access Memory
SP	Special Publication
TI	Texas Instruments
TLS	Transport Layer Security
VCM	Vocera Cryptographic Module
WLAN	Wireless Local Area Network

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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