Code Corporation

CodeXML® FIPS Bluetooth® Modem Security Policy

C005585

02/24/2011

Reviewed By	Role	Signature	Date
Tim Jackson	COGE		/ /
Mark Ashby	Engineering		/ /
Kerri Humpherys	Marketing		/ /
Ryan Hoobler	Application Engineering		/ /
Mark Gray	VPI Engineering		/ /

CHANGE RECORD

Revision	*Date*	*Author*	*Description of Change*
00AA	7/30/2010	Tim Jackson	Initial Work
00AB	8/5/2010	Tim Jackson	Added sections 11 & 12; added clarifications
00AC	8/8/2010	Tim Jackson	Fixed zeroize to unauthenticated, minor errors in logical diagrams, standardized firmware placeholder
00AD	8/10/2010	Tim Jackson	Updated status LED blink modes
00AE	8/11/2010	Tim Jackson	Added firmware version; added per role authentication status
00AF	8/11/2010	Tim Jackson	Added per role authentication status in 3.1
00AG	8/12/2010	Tim Jackson	Updated Sections 3.2, 13
00AH	8/18/2010	Tim Jackson	Updated photos throughout
00AI	8/24/2010	Tim Jackson	Updated part names, etc.
00AJ	8/24/2010	Tim Jackson	Update registered trademarks
00AK	8/24/2010	Tim Jackson	Updated TEK to CTR mode
00AL	9/3/2010	Tim Jackson	Updated typographical errors
00AM	2/24/2011	Tim Jackson	Approved minor changes made on our behalf by InfoGard in response to CMVP inquiries

Contents

Tables

Figures

1 Module Overview

The Code Corporation CodeXML® FIPS Bluetooth® Modem (MFG#: BTHDFIPS-M2_01) Cryptographic Module (hereafter referred to as the module) is a Multi-Chip Standalone module used as an external PC accessory designed to be connected to a computer via a USB or Serial cable for use with a Code Reader 2500 FIPS or Code Reader 3500 FIPS (CR2500 FIPS or CR3500 FIPS). The modem enables a Code reader to wirelessly transmit encrypted data to the computer.

The boundary of the module is the outer case of the physical device.

No components are excluded from the cryptographic boundary.

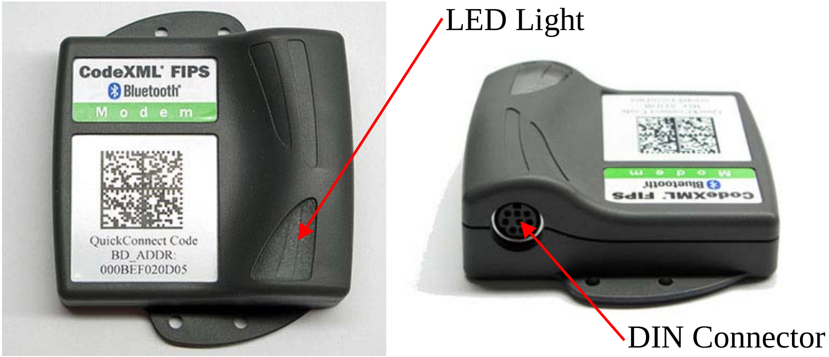

Figure 1 – Image of the Cryptographic Module

The configuration of hardware and firmware for this validation is:

Hardware: CodeXML® FIPS Bluetooth® Modem, Version: BTHDFIPS-M2_01

Firmware: 0187

Figure 2 depicts a block diagram of the CodeXML® FIPS Bluetooth® Modem hardware components, with the cryptographic boundary shown in red. The major blocks of the module hardware are:

- Memory: RAM and EEPROM
- CPU: Texas Instruments MSP430F149IPM/RG4
- One LED
- DIN Interface
- Wireless Bluetooth® Interface

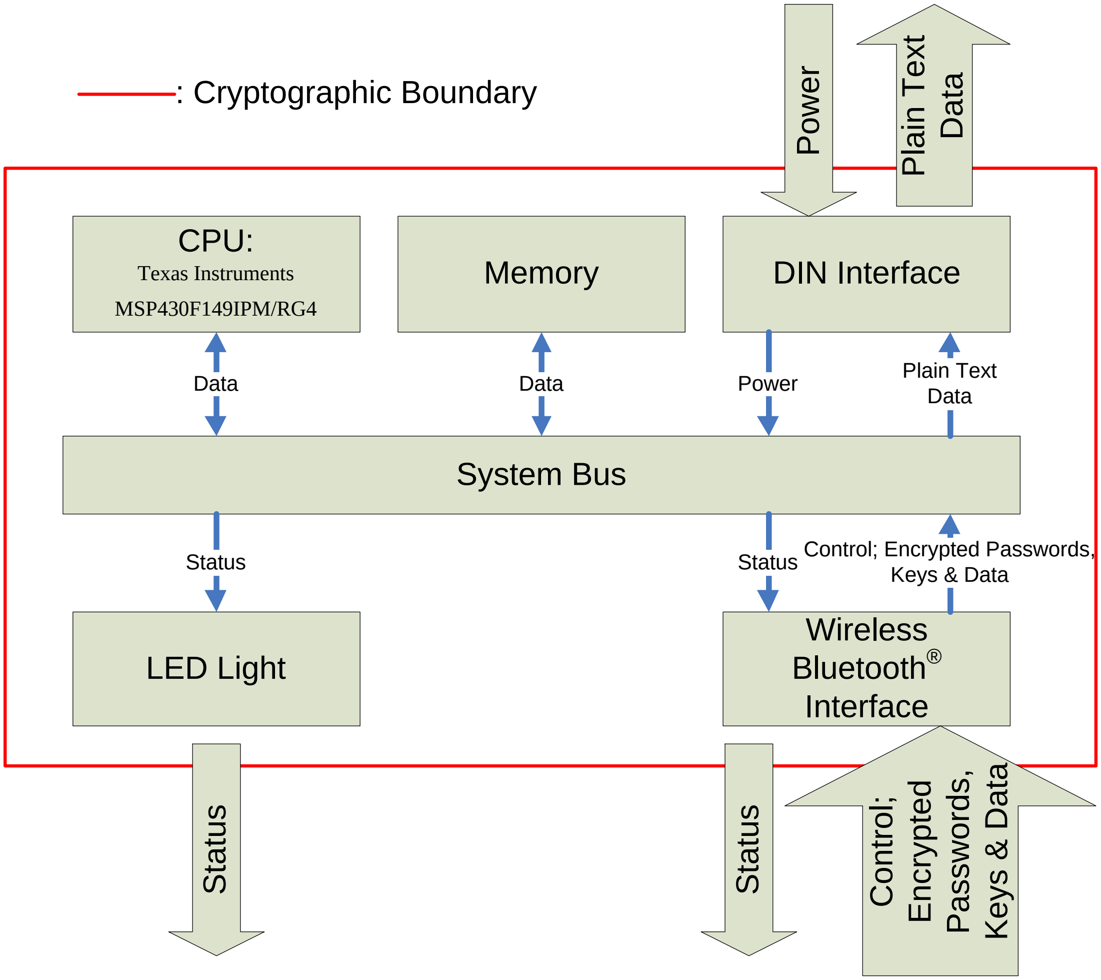

Figure 2 – Code FIPS Modem Block Diagram

Figure 3 depicts the logical block diagram for Initializing the CodeXML® FIPS Bluetooth® Modem. This process replaces the default Cryptographic Officer Password, Reader (User) Password, and Key Encryption Key with new values chosen by the Cryptographic Officer. This command is only available to the Cryptographic Officer. The readers are the interface to the modem, so the Initialization data is input to the modem having been encrypted using the KEK.

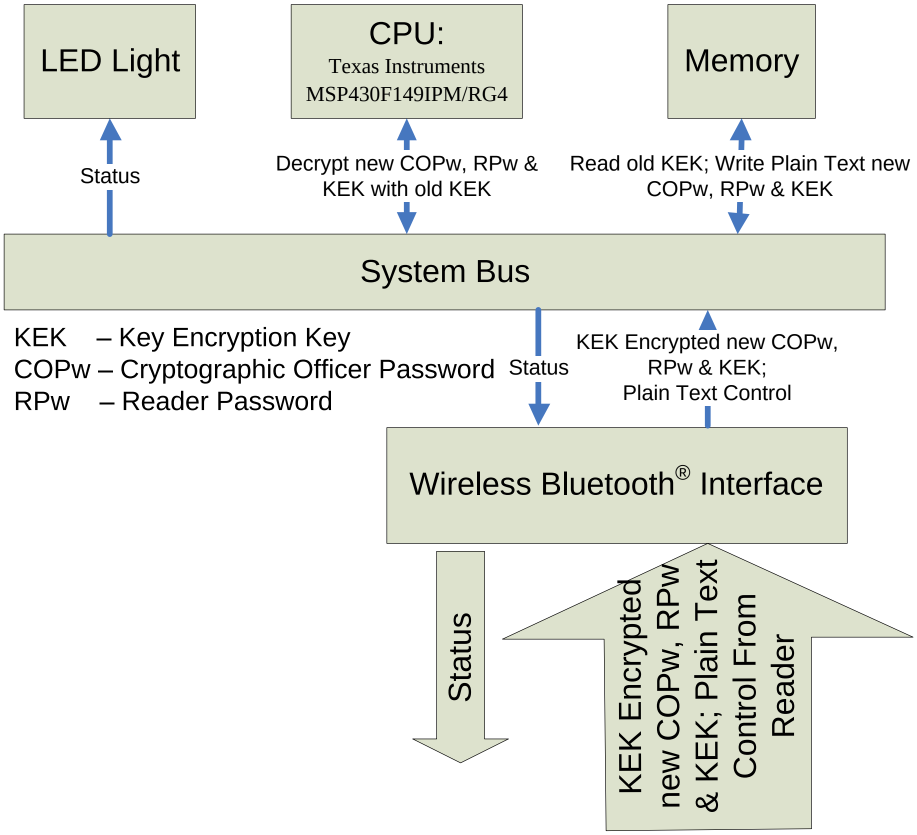
LED Light
CPU:
Texas Instruments
MSP430F149IPM/RG4
Memory
Status
Decrypt new COPw, RPw & KEK with old KEK
Read old KEK; Write Plain Text new COPw, RPw & KEK
System Bus
KEK – Key Encryption Key
COPw – Cryptographic Officer Password
RPw – Reader Password
Status
KEK Encrypted new COPw, RPw & KEK; Plain Text Control
Wireless Bluetooth® Interface
Status
KEK Encrypted new COPw, RPw & KEK; Plain Text Control From Reader

Figure 3 – Initialization Logical Block Diagram

Figure 4 depicts the logical block diagram for Authenticating to the CodeXML® FIPS Bluetooth® Modem. The Authentication process compares a supplied password with a password stored in memory and allows or disallows firmware paths based on the results.

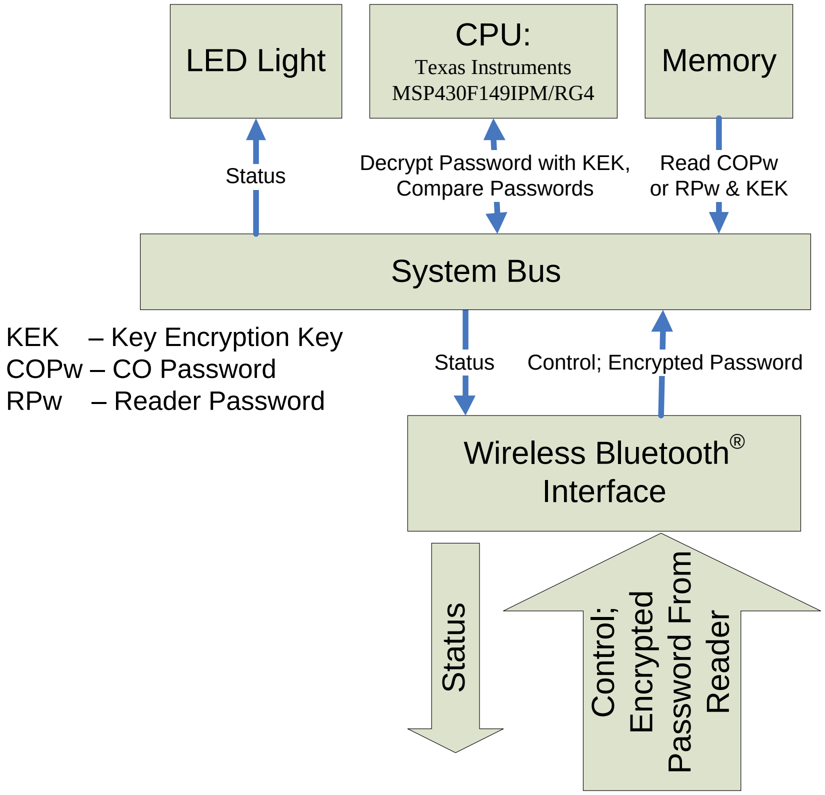

Figure 4 – Authentication Logical Block Diagram

Figure 5 depicts the logical block diagram for receiving encrypted data from the CR2500 FIPS and CR3500 FIPS bar code reader.

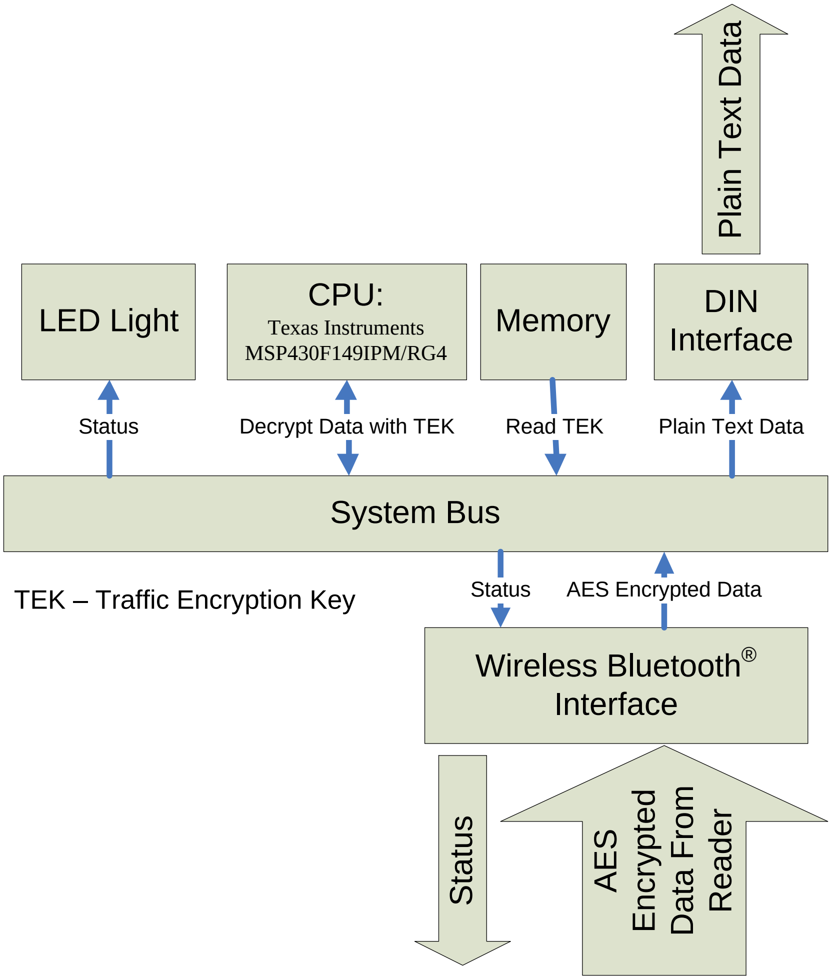

Figure 5 – Receiving Encrypted Data Logical Block Diagram

Figure 6 depicts the logical block diagram for Zeroizing the CodeXML® FIPS Bluetooth® Modem. All four CSP are reset back to defaults in this procedure – Cryptographic Officer Password, Reader (User) Password, Key Encryption Key and Traffic Encryption Key.

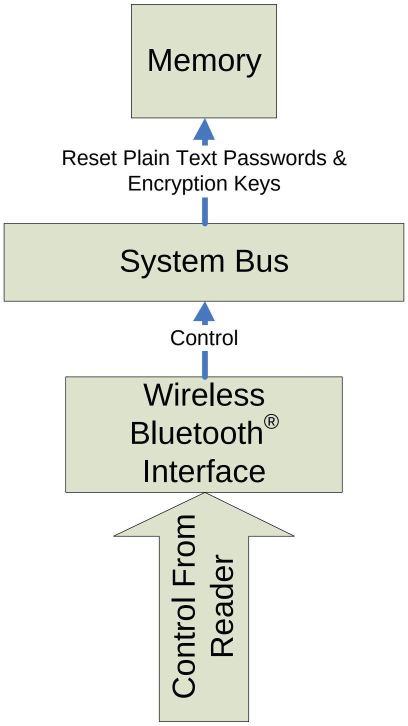
Memory
Reset Plain Text Passwords & Encryption Keys
System Bus
Control
Wireless Bluetooth® Interface
Control From Reader

Figure 6 – Zeroization Logical Block Diagram

Module services are described in Section 6 below.

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 FIPS Approved Mode of Operation

The module provides a FIPS Approved mode of operation, comprising all services described in Section 6 below and a non-FIPS mode where the modules respond in the same manner as non-FIPS Code devices. The module will enter FIPS Approved mode following successful power up self tests and authentication.

- CO Authenticated – the module will indicate this mode of operation by blinking the blue LED light in a 1 second on, 1 second off pattern.
- Un-Authenticated – the module will indicate this mode of operation by blinking the blue LED light in a 2 seconds on, 1 second off pattern.
- Reader (User) Authenticated – the module will indicate this mode of operation by blinking the blue LED light in a Morse Code 'F' pattern. The Morse Code 'F' is comprised of two short dots, a long dash and a short dot (••—•) followed by a 3.5 second delay.

3.2 Non-FIPS Mode of Operation

If the Power-on Initialization determines that the module has not been Initialized, the module does not provide access to any Cryptographic functions. In this state, the module will function as a non-FIPS Code modem would function – the modules will pass plain text data. This is the non-FIPS mode of operation for the module.

3.3 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2 – FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	CAVP Cert. #
AES: ECB; 128 and 256 bit	Cert. #1456
AES: CTR; 256 bit; External Counter	Cert. #1456

The cryptographic module contains no non-FIPS Approved algorithms.

4 Ports and Interfaces

The CodeXML® FIPS Bluetooth® Modem is a multi-chip standalone cryptographic module with ports and interfaces as shown below.

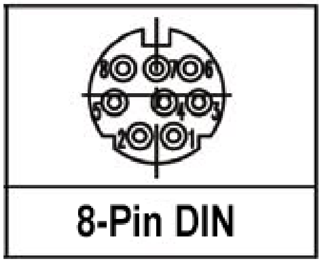

Figure 7 – 8-Pin DIN Connector Pin-Out

Table 3 – Code FIPS Modem Pins and FIPS 140-2 Ports and Interfaces

Pin	FIPS 140-2 Designation	Name and Description
LED Light	Status Output	Displays FIPS status
Wireless Bluetooth® Radio	Encrypted Data Input/Control Input	Receives Encrypted Data from Reader, sends responses to Reader
8-Pin DIN Connector Pin 1 (DIN1)	Power Port	VIN - Input Voltage to the voltage regulators/batter charging IC
DIN2	Data Output	RS232_TX - RS-232 level serial transmit signal
DIN3	Data Output	RS232_RX - RS-232 level serial receive signal
DIN4	Data Output	PS2_DATA_UART_RX_USB_DP - UART transmit signal/ USB Data plus signal
DIN5	Data Output	PS2_DATA_UART_RX_USB_DM - UART receive signal/ USB Data minus signal
DIN6	N/A	This pin is disabled via firmware while in FIPS Mode.
DIN7	N/A	This pin is disabled via firmware while in FIPS Mode.
DIN8	Power Port	Ground

5 Identification and Authentication Policy

5.1 Assumption of Roles

The module supports two distinct operator roles, Reader (User) and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles using re-authentication when changing roles. The Reader role is not allowed to change passwords on the device and the CO role is not allowed to receive encrypted data.

Authentication is based on eight-character passwords using any Extended ASCII character value in the range 0x20 - 0xFF.

The module provides neither a maintenance role or bypass capability.

Table 4 – Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CRYPTOGRAPHIC OFFICER	This role has access to the Initialize service. The CO is not allowed to transmit data.	Role-based operator authentication	Password is fixed at eight characters from the Extended ASCII set 0x20 through 0xFF. Password must be received from the CR2500 FIPS & CR3500 FIPS reader module, encrypted with the KEK.
READER (USER)	This role has access to the Receive Encrypted Data service. The Reader is not allowed to initialize.	Role-based operator authentication	Password is fixed at eight characters from the Extended ASCII set 0x20 through 0xFF. Password must be received from CR2500 FIPS & CR3500 FIPS reader module, encrypted with the KEK.

Table 5 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Passwords (Fixed-length, eight characters; 0x20-0xFF Extended ASCII character set)	The probability that a random attempt will succeed or a false acceptance will occur is a minimum of 1/ 2^{3*225} or $1/2^{675}$ or 1/ $1.5676426594103495798233121284485\text{x}10^{203}$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute through random attempts is a minimum of $1/2^{(3*225)-12.55}$ or $1/2^{662.45}$ or 1/ $2.6140905529297575030401884034\text{1x}10^{199}$ which is less than 1/100,000. The calculations are based on eight character (2^3) passwords built from a 225 character set. Code readers can read 6000 (or ~ $2^{12.55}$) bar codes per minute under ideal conditions.

6 Access Control Policy

6.1 Roles and Services

Table 6 – Authenticated Services

Service	CO	Reader	Description
Authenticate	X	X	Ensures the operator assuming role is authorized and limits the services available to a role.
Initialize	X		Receives and sets Encrypted Cryptographic Officer Password, Reader Password, and Key Encryption Key.
Receive Encrypted Data		X	Transfer data from the Reader to the Modem using the Traffic Encryption Key.
Receive Encrypted TEK		X	Receives and sets Encrypted Traffic Encryption Key.

6.2 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 7 – Unauthenticated Services

Service	Description
Self Test	Re-runs Power-On Self Test
Zeroize	Clears Encryption Keys and Passwords. Requires the Initialize Command to be run to return to FIPS functionality.

6.3 Specification of Service Input and Output

Table 8 – Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Self-Test	N/A	N/A	N/A	On FAIL – LED Light flashes blue .5 sec on, .5 sec off On Success – LED Light flashes blue 2 second on, 1 second off.
Initialize	Plain Text Initialize command via Bluetooth®	KEK Encrypted Data - Initialize command, two eight character passwords and a 256 bit Key	N/A	LED Light flashes repeating 1 second on, 1 second off; Acknowledgement via

	Wireless from Reader	Encryption Key decoded from a Data Matrix bar code via Bluetooth® Wireless from Reader		Bluetooth® Wireless to Reader
Receive Encrypted TEK	Plain Text Control via Bluetooth® Wireless from Reader	KEK Encrypted Data - one 256 bit Traffic Encryption Key generated by the reader and sent via Bluetooth® Wireless from Reader	N/A	LED Light flashes blue repeating Morse Code ‘F’ (••–•); Acknowledgement via Bluetooth® Wireless to Reader
Authenticate	Plain Text Authenticate command via Bluetooth® Wireless from Reader	KEK Encrypted Data - one eight-character password via Bluetooth® Wireless from Reader	N/A	Authenticate CO - LED Light flashes repeating 1 second on, 1 second off; Acknowledgement via Bluetooth® Wireless to Reader
				Authenticate READER - LED Light flashes blue repeating Morse Code ‘F’ (••–•); Acknowledgement via Bluetooth® Wireless to Reader
Zeroize	Plain Text Zeroize command via Bluetooth® Wireless from Reader	N/A	N/A	LED Light solid on; Acknowledgement via Bluetooth® Wireless to Reader
Receive Encrypted Data	Plain Text Control via Bluetooth® Wireless from Reader	TEK Encrypted Data - via Bluetooth® Wireless from Reader	Plain Text Data via DIN Connector to PC	LED Light flashes blue repeating Morse Code ‘F’ (••–•); Acknowledgement via Bluetooth® Wireless to Reader

6.4 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 9 – Private Keys and CSPs

Key Name	Type	Description
Key Encryption Key	AES-256: ECB	Key used to decrypt session-based Traffic Encryption Key as well as other CSPs from the Reader. Set in Initialization procedure.
Traffic Encryption Key	AES-256: CTR	Key used to encrypt data sent from Reader to Modem. This key is received encrypted with the KEK from the reader for each session to provide a higher level of confidentiality.
Reader (User) Password	Eight characters; 0x20-0xFF Extended ASCII character set	Password used to authenticate the Reader (User) role
Cryptographic Officer Password	Eight characters; 0x20-0xFF Extended ASCII character set	Password used to authenticate the Cryptographic Officer role

6.5 Definition of CSPs Modes of Access

Table 13 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 10 – CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic Key or CSP
CO	Authenticate	R R	Cryptographic Officer Password Key Encryption Key
	Initialize	W W W R	New Key Encryption Key New Reader Password New Cryptographic Officer Password Existing Key Encryption Key

Reader (User)	Authenticate	R R	Reader Password Key Encryption Key
	Receive Encrypted Data	R	Traffic Encryption Key
	Receive Encrypted TEK	R W	Key Encryption Key Traffic Encryption Key
Un-Authenticated or Any Role	Zeroize	Z Z Z Z	Key Encryption Key Traffic Encryption Key Reader Password Cryptographic Officer Password
	Self-Test	N/A	N/A

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the FIPS Modem does not contain a modifiable operational environment.

8 Security Rules

The module design corresponds to the CodeXML® FIPS Bluetooth® Modem security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide role-based authentication.
2. The cryptographic module shall provide two distinct operator roles. These are the Reader (User) role, and the Cryptographic Officer role.
3. The cryptographic module shall clear previous authentications on power cycle
4. The cryptographic module shall clear Traffic Encryption Keys on power cycle
5. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
6. The cryptographic module shall perform the following tests
   A. Critical Function Tests
         a. Electronic board initialization
   B. Power up Self-Tests
      1. Cryptographic algorithm tests
         a. AES Encrypt and Decrypt Known Answer Test
      2. Firmware Integrity Test – CRC16 check against known value at firmware load (power on)
7. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power by removing and replacing the DIN cable to the module.
8. Power-up self tests do not require any operator action.
9. Data output shall be inhibited during self-tests, zeroization, and error states.
10. The module does not generate keys.
11. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
12. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
13. The module does not support concurrent operators.
14. The module does not support a maintenance interface or role.
15. The module does not support manual key entry.
16. The module only accepts plain text commands, encrypted passwords, keys and data from the Wireless Bluetooth® Interface from the Code Corporation Code Reader 2500 FIPS & Code Reader 3500 FIPS module.
17. The module does not enter or output plaintext CSPs.
18. The module does not support the update of the firmware.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The outer casing of the module is production quality opaque material. Two of the six screws are covered with blue tamper evident compound. The tamper evident compound is applied to the module by Code Corporation in manufacturing before distribution to the end user.

9.2 Operator Required Actions

Examine the tamper evident seals monthly.

Table 11 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	1 month	There are two tamper-evident seals on the module. Two (of six) of the screw holes in the bottom of the case will be filled with blue tamper evident compound. (see Figure 8, below) The compound dries into a hard, brittle substance. Inspect the screw holes for any signs of scratching or broken compound. If any tampering is suspected, return the module to Code for testing and replacement of the tamper evident compound.

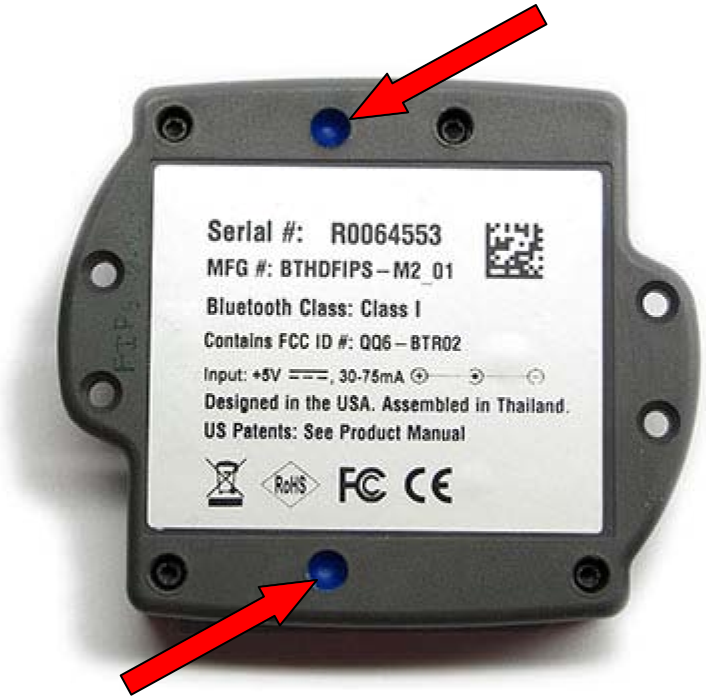
Serial #: R0064553
MFG #: BTHDFIPS–M2_01
Bluetooth Class: Class I
Contains FCC ID #: Q06–BTR02
Input: +5V ⎓, 30-75mA
Designed in the USA. Assembled in Thailand.
US Patents: See Product Manual
RoHS
FC
CE

Figure 8 – Image of the Cryptographic Module showing the placement of tamper-evident seals

10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks that are outside of the scope of FIPS 140-2.

11 Pre-Initialization Mode

The module employs a Pre-Initialization mode that employs default values for the Cryptographic Officer role password, the Reader (User) role password and the Key Encryption Key. The only service that is available in pre-initialization mode is Authentication of the CO role. Once Authenticated the CO is required to Initialize the module before the Reader role can be Authenticated.

The module returns to the Pre-Initialization state after it receives the Zeroization command. The passwords and KEK are returned to default and the TEK is overwritten with zeroes.

12 Delivery Security

The modules will be packed by Code Corporation representatives, sealed with packing tape, and then delivered via common carrier using a tracking code to the end user or their delegate. If the package is damaged in shipping, inspect the Tamper Evident seals to determine if the modules have been compromised.

13 References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

[FIPS 197] FIPS Publication 197 *ADVANCED ENCRYPTION STANDARD (AES)*

14 Definitions and Acronyms

KEK – Key Encryption Key; Encrypts passwords and keys exchanged between Reader and Modem

TEK – Traffic Encryption Key; Encrypts data exchanged between Reader and Modem