Zebra Technologies Corp.

ZBR-88W8787-WLAN

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Version: 0.11

Date: April 27, 2016

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the Zebra Technologies ZBR-88W8787-WLAN cryptographic module; hereafter denoted the Module. The Module resides in the wireless LAN (WLAN) data plane of several Zebra Technologies devices. The Module meets FIPS 140-2 overall Level 1 requirements.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated Zebra devices.

The Module is a multi-chip standalone embodiment, and is defined as a Firmware-Hybrid. The cryptographic boundary includes the Marvell Avastar 88W8787 SoC and the embedded operating system (QNX) upon which the driver firmware resides providing the interface to the 88W8787 SoC. The physical boundary of the module is drawn at the casing of the general operating platform (printer).

The cryptographic module under validation is:

- HW P/N: Marvel Avastar 88W8787 (Version 1.0)
- Marvell Firmware version 14.66.35.p51
- Zebra Driver Firmware Version: 1.2

The module was tested on the following operational environment:

- Zebra QLn320 Printer running QNX 6.5.0

The cryptographic module is also supported on the following operating environments using identical hardware listed above, for which operational testing was not performed:

- QNX 6.4.x
- QNX 6.5.x
- QNX 6.6.x

The FIPS 140-2 security levels for the Module are as follows:

Table 1 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1

Security Requirement	Security Level
Mitigation of Other Attacks	N/A

1.1 Ports and Interfaces

The module includes both physical and logical interfaces. The firmware APIs constitute the module's logical interfaces, and the physical interfaces are defined by the 88W8787 chip and the generic ports of the operating platform. The interfaces are as follows:

- Control Input Interface: firmware API commands and command parameters used to control and configure module operation. The Control Input Interface also includes the registry values used to control module behavior.
- Status Output Interface: return values from firmware API commands used to obtain information on the status of the module. The Status Output Interface also includes the log file where the module messages are output.
- Data Input Interface: data inputs to the firmware API commands
- Data Output Interface: data outputs of the firmware API commands
- Data output interface: 88W8787 radio MAC
- Power: Power input port of 88W8787 chip and the power input port of the operating platform.
- Physical Ports of Generic Operating Platform (Printer): USB, Serial, and Ethernet (via external cradle)

All module interfaces, inputs and outputs are provided by the firmware component, the 88W8787 radio MAC, and the generic ports of the operating platform.

1.2 Logical Cryptographic Boundary

Figure 1 depicts the Module operational environment.

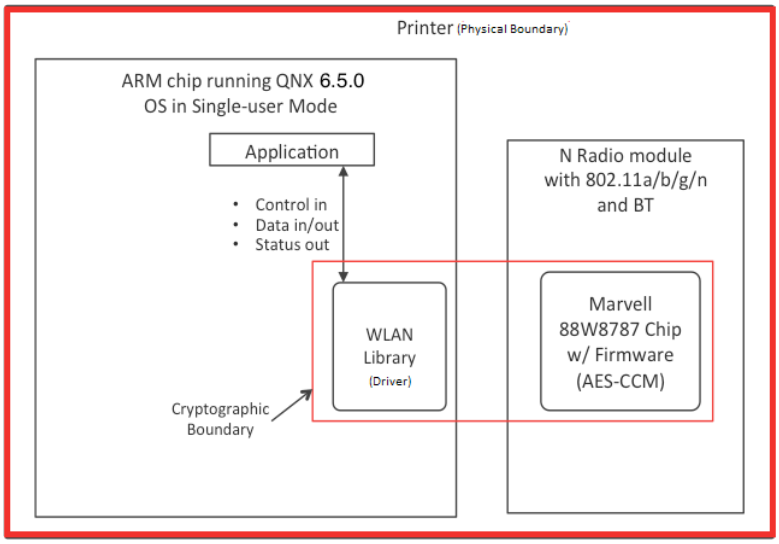

Figure 1: Module Block Diagram

1.3 Hardware Component of Module

Figure 2 depicts the external packaging of the hardware component of the module (N Radio Module containing Marvell 88W8787 Chip).

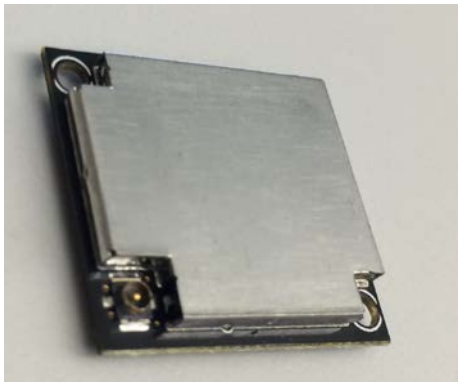

Figure 2: Hardware Component of Module

1.4 Physical Security

The module embodiment is multi-chip standalone, and the physical boundary is drawn at the casing of the general purpose platform (printer). The physical components that comprise the module are production grade. All IC's are coated with industry standard passivation.

1.5 Mode of Operation

The module supports both an Approved and non-Approved mode of operation. To configure the module in the Approved mode of operation, the operator initializes the module using the io-pkt-v4-t 1 –d mv8787 no_bt command. This command disables the Bluetooth connection, and enables only the WiFi connection. The operator can obtain confirmation of the Approved mode of operation by viewing the value of the file "is_fips_mode". A return value of YES indicates the module is operating in the Approved mode. To configure the module in the non-Approved mode of operation, the operator initializes the module using the io-pkt-v4 –t 1 –d mv8787 command, which enables both the Bluetooth and WiFi connection options. The operator can obtain confirmation of the non-Approved mode of operation by viewing the value of the file "is_fips_mode". A return value of NO indicates the module is operating in non-Approved mode. The Bluetooth connection does not utilize the implemented AES algorithm or the AES key.

2. Cryptographic Functionality

The Module implements only the FIPS Approved cryptographic functions listed in the table below.

Table 2 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES-CCM	[SP 800-38C] Functions: Generation/Encryption, Verification/Decryption Key sizes: 128, 192 and 256	3003
HMAC	[198-1] HMAC –SHA-1 Functions: Firmware Integrity Check on Load Key sizes: 160 bits, 512 bits	2248
SHA	[180-4] SHA-1 Functions: Support firmware Integrity Check	2902

The Module implements the following non-approved cryptographic functions listed in the table below.

Table 3 – Non-Approved Cryptographic Functions

Algorithm	Description
SAFER+	Used for key derivation and MAC creation over the non-approved Bluetooth connection.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 4 – Critical Security Parameters

CSP	Description / Usage
AES Key	Used to encrypt wireless data. Generated externally during the establishment of the wireless session. Stored temporarily in volatile RAM. Entry in plaintext, output is N/A. An application program that uses the API may destroy the key. The zeroization service zeroizes the CSP. AES key sizes (128, 192 or 256)

3. Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module does not provide any identification or authentication methods of its own. The Cryptographic Officer and the User roles are implicitly assumed based on the service requested.

Table 5 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer	N/A	N/A
User	User	N/A	N/A

3.2 Services

All services implemented by the Module are listed in the table below. Each service description also describes all usage of CSPs by the service. All services, with the exception of Encrypt / Decrypt and Serial Port Profile, are available in both the approved and non-approved mode. The non-approved mode enables Bluetooth for use as a communication option, and does not utilize the Encrypt / Decrypt service.

The cryptographic module supports the following service that does not require an operator to assume an authorized role:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. It is invoked by reloading the library into executable memory.

Table 6 – Authorized Services

Service	Description	CO	U
Self-tests	Perform cryptographic algorithm self-tests via power cycle	X	X
Show status	Show cryptographic module status (see section 4)	X	X
Read version	Read cryptographic module version	X	X
Loads key	Install cryptographic key	X	X
Encrypt / Decrypt	Perform AES-CCM generation/verification (Approved Mode Only)	X	X
Serial Port Profile	Bluetooth flow control emulation (Non-Approved mode only)	X	X
Zeroize	Zeroize all CSP's contained in memory	X	X

Table 7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

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

Table 7 – CSP Access Rights within Services

Service	CSPs
	AES Key
Self-Tests	-
Load Key	W
Encrypt (generation) / Decrypt (Verification)	R,E
Read Version	-
Show Status	-
Serial Port Profile	-
Zeroize	Z

4. Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 7 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the SOFT ERROR state. The SOFT ERROR state is indicated by the inoperability of the module (enters infinite loop). The module must be reloaded (power cycled) to clear the error state and return to normal operation.

Contents of the POST file can be accessed to confirm the successful passing of all module power-on self-tests. A return message of "OK" will be returned to confirm all power-on self-tests have completed successfully.

Table 8 – Power Up Self-tests

Test Target	Description
Firmware Integrity	HMAC-SHA1 driver firmware integrity check. (*Note: Marvell firmware included in integrity check)*
AES-CCM	KATs: Generation and Verification Key sizes: 128, 192, 256 bits

5. Operational Environment

The module operates QNX 6.5.0, which is an embedded non-modifiable operational environment installed on a generic operating platform (e.g., printer). The firmware driver component of the module is loaded onto the embedded OS prior to deployment to the end user. The QNX 6.5.0 embedded operating system runs in single operator mode only. The module has been tested on QNX 6.5.0 running on a Zebra QLn320 printer ; however, as stated in section 1, is capable of running on other versions of the QNX OS and various operating platforms.

6. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2 requirements.

7. Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides no authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

4. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
5. Power-up self-tests do not require any operator action.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support concurrent operators.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.
14. The module does not output intermediate key values.

8. References and Definitions

The following standards are referred to in this Security Policy.

Table 9 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[FIPS IG]	*Implementation Guidance, April 25th 2014.*
[FIPS 197]	*Announcing the Advanced Encryption Standard*
[SP800-38A]	*Recommendation for Block Cipher Mode of Operation*
[SP800-38C]	*Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*
[198-1]	*The Keyed-Hash Message Authentication Code (HMAC)*
[180-4]	*Secure Hash Standard (SHS)*

Table 10 – Acronyms and Definitions

Acronym	Definition
WLAN	Wireless LAN using 802.11x
SoC	System on Chip