Zebra Technologies Corporation

ZBR-88W8887-WLAN

FIPS 140-2 Cryptographic Module Non-Proprietary Security Policy

Documentation Version: 1.3

Last Update: March 23, 2022

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the ZBR-88W8887-WLAN cryptographic module from Zebra Technologies Corporation; 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 defined as a Firmware-Hybrid. The module's cryptographic boundary includes the NXP 88W8887 SoC and the embedded operating system (QNX) upon which the driver firmware resides providing the interface to the 88W8887 SoC. The physical boundary of the module is drawn at the casing of the tested operational platform (Zebra ZQ521 printer).

Figure 1: ZQ521 Printer

The hardware version and firmware versions running on the cryptographic module under validation are listed as below.

- **Hardware Version**: P/N: NXP 88W8887 (Version 1.0)
- **Firmware Versions**: NXP Firmware Version 15.68.19.p59 and Zebra 8887 FIPS Driver Firmware Version 2.0

Tested Configuration

The module was tested on the following operational environment:

- QNX 7.0 running on Zebra ZQ521 printer with NXP i.MX6ULL (ARM Cortex-A7) and NXP ARMv5TE

Vendor Affirmed Tested Platforms

The following platforms have not been tested as part of the FIPS 140-2 Level 1 certification however the vendor (Zebra Technologies Corporation) "vendor affirms" that these platforms are equivalent to the tested and validated platforms. Additionally, Vendor affirms that the Module will function the same way and provide the same security services on any of the operating systems listed below.

- NXP i.MX25 running QNX 6.5.x
- NXP i.MX6SoloX running QNX 6.6.x
- NXP i.MX7 running QNX 7.0

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
Mitigation of Other Attacks	N/A
Overall Level	**1**

1.1 Ports and Interfaces

The module is a multi-chip standalone embodiment for FIPS 140-2 purposes. The module's physical boundary encompasses the 88W8887 chip Radio MAC[1] interface on the module's hardware component and the generic ports (USB, Serial, and Ethernet ports) on the tested platform (Zebra ZQ521 printer).

The module provides its logical interfaces via Application Programming Interface (API) calls. The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

Table 2 – Module Interfaces

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	Arguments for an API call that provide the data to be used or processed by the module.
Data Output Interface	Arguments output from an API call.
Control Input Interface	Arguments for an API call 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.
N/A	Power input port.

[1] The Radio MAC is referenced to the radio transmitter/receiver.

1.2 Logical Cryptographic Boundary

Figure 2 depicts the module's Block Diagram. Please note that the bold RED rectangle in Figure 2 below represents the module's physical boundary; thin RED rectangle is for the logical boundary/cryptographic boundary.

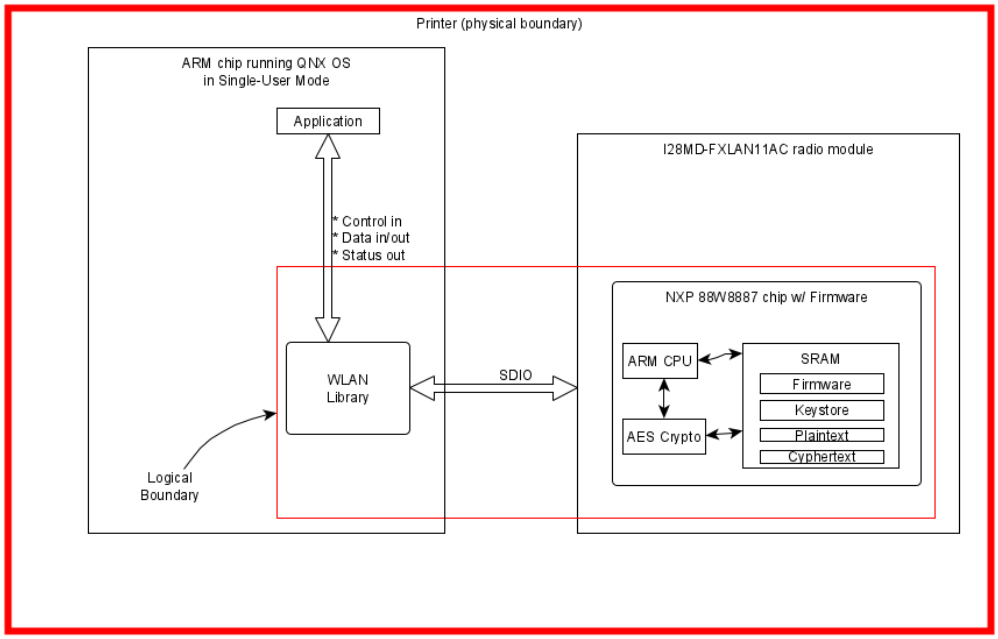

Figure 2: Module Block Diagram

1.3 Hardware Component of Module

Figure 3 depicts the external packaging of the 88W8887 Radio hardware component of the module, which contains the NXP 88W8887 Chip.

Figure 3: Module's Hardware Component

1.4 Physical Security

The module's physical boundary is drawn at the casing of the tested operational platform (Zebra ZQ521 printer). The physical components that comprise the module are production grade. All ICs are coated with industry standard passivation.

1.5 Mode of Operation

The module only can be operated in FIPS mode.

2. Cryptographic Functionality

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

Table 3 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
Algorithm Implementation - 8887 AES Module		
AES-ECB, AES-CCM	[SP 800-38C] Functions: Generation-Encryption; Decryption-Verification Key sizes: 128-bit	A1146
Algorithm Implementation - 8887 FIPS driver		
HMAC	[198-1] HMAC –SHA-1 Functions: Firmware Integrity Check on Load Key size: 160 bits	A1145
SHA	[180-4] SHA-1 Functions: Support firmware Integrity Check	A1145

Note:
There are key sizes that have been CAVP tested but are not used by the module. Only the key lengths/curves/moduli shown in this table are used by the module.

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 3.2.

Table 4 – Critical Security Parameters and Keys

CSP/Keys	Description / Usage
AES Key	This AES-CCM (128 bits) key is used to protect the module's wireless Radio data. It is generated outside the module's logical boundary, but still in the module's physical boundary. Enter into the module is in plaintext as an API parameter, and output is N/A. It is stored temporarily in volatile RAM, and can be zeroized via an API zeroization call.
HMAC Key	This HMAC-SHA-1 key is only used to perform the Firmware Integrity Test. It is stored in the firmware. This key is not considered as a CSP and therefore does not need to meet the FIPS 140-2 Section 4.7.6 zeroization requirements.

3. Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two operator roles, User and Cryptographic Officer (CO). The cryptographic module does not provide any identification or authentication methods of its own. The module does not allow concurrent operators. 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. 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 or API command	X	X
Show status	Show cryptographic module status	X	X
Read version	Read cryptographic module version	X	X
Loads key	Load cryptographic key (AES Key)	X	X
Encrypt / Decrypt	Perform AES-CCM generation/verification	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	-

Service	CSPs
	AES Key
Show Status	-
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 8 below. All Known Answer Tests (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
Algorithm Implementation - 8887 FIPS driver	
Firmware Integrity Test	HMAC-SHA-1 Firmware Integrity Check Note: the firmware integrity test covers both NXP Firmware (version: 15.68.19.p59) and Zebra 8887 FIPS Driver Firmware (version: 2.0)
Algorithm Implementation - 8887 AES Module	
AES-ECB	KATs: Encryption and Decryption Key size: 128-bit
AES-CCM	KATs: Encryption and Decryption Key size: 128-bit

5. Operational Environment

The module operates QNX 7.0, 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 7.0 embedded operating system runs in single operator mode only. The module has been tested on QNX 7.0 running on a Zebra ZQ521 printer with i.MX6ULL CPU; however, as stated in section 1, is capable of running on other versions of the operating systems.

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 validated firmware binary files, including the Zebra 8887 FIPS driver firmware binary file: devnp-mv8887-fips.so, and the NXP firmware binary file: sd8887_uapsta.bin, were loaded/installed into the module while being manufactured, and cannot be updated by the operator.
2. The module provides two distinct operator roles: User and Cryptographic Officer.
3. The module provides no authentication.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
6. Power-up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not output the plaintext CSPs.
15. 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
SoC	System on Chip