Zebra Technologies Corporation

Non-Proprietary FIPS 140-3 Security Policy For

Zebra 8887 Cryptographic Module

Firmware-Hybrid Module

HW ID:9134

Firmware Versions:

FIPS Driver Firmware Version 2.1 and NXP Firmware Version 15.68.19.p59

Documentation Version 1.1

Last Update: June 18, 2024

Table of Contents

List of Figures

List of Tables

1. General

This document defines the Security Policy for Zebra 8887 Cryptographic Module from Zebra Technologies Corporation; hereinafter referred to as the Module. The module resides in the wireless LAN (WLAN) data plane of several Zebra Technologies devices. The Module meets FIPS 140-3 overall Level 1 requirements. The module is intended for use by US Federal agencies and other markets that require FIPS 140-3 validated Zebra devices.

The below table indicates the individual cause levels and over levels.

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Titles	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Ports and Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical Security	1
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-Tests	1
11	Life-cycle assurance	1
12	Mitigation of Other Attacks	N/A
Overall Level	**Security Level 1**	

Table 1 - Security Levels

The module has an overall security level of 1.

2. Cryptographic Module Specification

The module is a multi-chip standalone Firmware-hybrid module. The module's cryptographic boundary includes the NXP 88W8887 CPU and the driver firmware providing the interface to the 88W8887 CPU. The module's cryptographic boundary includes the following components:

Component	Type	FW/HW Version
Module's Firmware Component: Zebra WLAN Library running FIPS driver firmware binary file: devnp-mv8887-fips.so	Firmware	FW: FIPS driver Firmware Version 2.1
Module's Firmware Component: Zebra WLAN Core running NXP firmware binary file: sd8887_uapsta.bin	Firmware	FW: NXP Firmware Version 15.68.19.p59
Module's Hardware Component: Zebra WLAN Core	Hardware	HW ID: 9134

Table 2 – Module's HW/FW Components

The module has been tested on the following platforms:

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	QNX 7.0.4	Zebra ZQ521 Printer	NXP i.MX 6ULL ARM Cortex-A7 and NXP ARMv5TE	None

Table 3 – Tested Operational Environments

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Modes of Operation

By design, the module can only support approved mode of operation and does not implement any Non-Approved Security Functions. The module does not claim the implementation of a degraded mode of operation.

The table below lists all approved security functions of the module, including specific key size(s) -in bits unless otherwise noted- employed for approved services, and implemented modes of operation. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

CAVP	Algorithm and Standard	Mode/Method	Description/Key Size(s) / Key Strenth(s)	Use/Function
A1146	AES [FIPS 197; SP800-38A]	AES-ECB	128 bits	Prerequisite algorithms for AES-CCM
A1146	AES [FIPS 197; SP 800-38C]	AES-CCM	128 bits	Authenticated Symmetric Encryption/Decryption
A2718	HMAC [FIPS 198-1]	HMAC-SHA-1	160 bits	Keyed Hash. Used in Firmware Integrity Check
A2718	SHS [FIPS 180-4]	SHA-1	N/A	Prerequisite algorithm of HMAC-SHA-1

Table 4 – Approved Algorithms

As the module can only be operated in the Approved mode of operation, and any algorithms not listed in table 4 above will be rejected by the module while in the approved mode, the tables defined in SP800-140B for the following categories are missing from this document.

- Non-Approved Algorithms Allowed in Approved Mode of Operation
- Non-Approved Algorithms Allowed in Approved Mode of Operation with No Security Claimed
- Non-Approved Algorithms Not Allowed in Approved Mode of Operation

Cryptographic Boundary

The module is defined as a multi-chip standalone Firmware-hybrid module (thin red line area), with the boundary of the Tested Operational Environment's Physical Perimeter (TOEPP) being defined as the physical perimeter of the tested platform enclosure around which everything runs.

Figure 1 - Module's Hardware Component (Zebra WLAN Core)

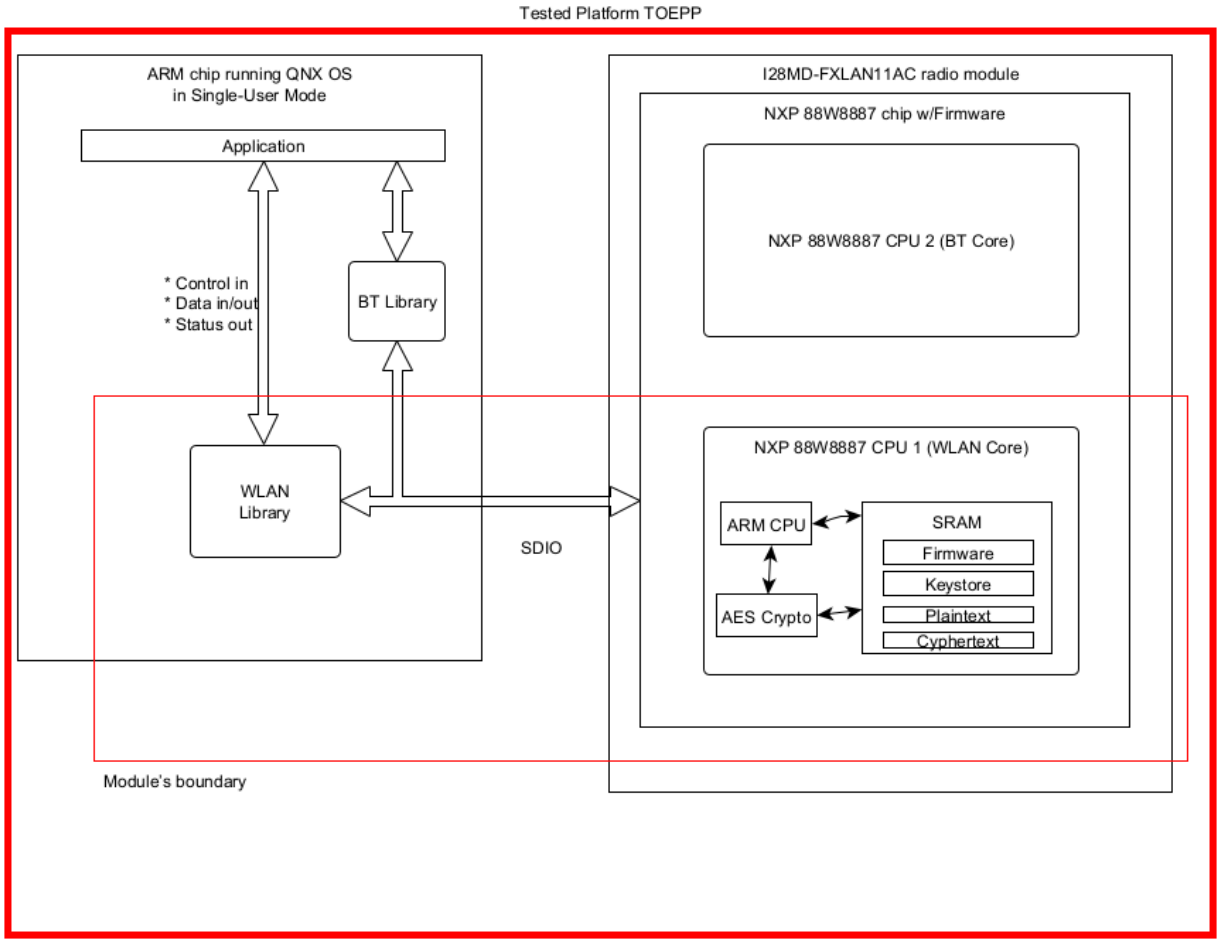

Figure 2 – Block Diagram

3. Cryptographic Module Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Table 2. The module provides its logical interfaces via Application Programming Interface (API) calls. The logical interfaces provided by the module are mapped onto the FIPS 140-3 interfaces (data input, data output, control input, control output and status output) as follows.

Physical Port	Logical Interface	Data that passes over port/interface
SDIO Interface	Data Input	Arguments for an API call that provide the data to be used of processed by the module.
SDIO Interface	Data Output	Arguments output from an API call.
SDIO Interface	Control Input	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.
SDIO Interface	Status Output	Returns values from firmware API commands used to obtain information on the status of the module. The status output interface also includes the log files where the module messages are output.
N/A	Control Output	N/A
Power Interface	N/A	Module's hardware component power supply.

Table 5 – Ports and Interfaces

4. Roles, Services, and Authentication

The module supports Crypto Officer (CO) role. The cryptographic module does not provide any authentication methods. The module does not allow concurrent operators. The Crypto Officer is implicitly assumed based on the service requested. The module provides the following services to the Crypto Officer role.

Role	Service	Input	Output
Cryptographic Officer (CO)	Self-tests	Command to conduct self-tests	Status of self-tests
Cryptographic Officer (CO)	Show Status	Command to check status	Module's current status
Cryptographic Officer (CO)	Show Version	Command to read module's version	Module's name/ID and versioning information
Cryptographic Officer (CO)	Load Key	Command to set key	Updated key message
Cryptographic Officer (CO)	Encrypt/Decrypt	Command to conduct the encryption and decryption operation	Encrypted or Decrypted message
Cryptographic Officer (CO)	Zeroize	Command to zeroize all SSPs	Key zeroize message

Table 6 – Roles, Service Commands, Input and Output

The table below lists all approved services that can be used in the approved mode of operation. The abbreviations of the access rights to keys and SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module.

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

N/A = The service does not access any SSP during its operation.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Self-tests	Perform cryptographic algorithm self-tests via power cycle or API command	AES-ECB; AES-CCM; HMAC-SHA-1; SHA-1;	Firmware Integrity Test Key (non-SSP)	CO	N/A	Self-Tests completion status log message
Show status	Show cryptographic module status	N/A	N/A	CO	N/A	N/A
Show version	Show module's name/ID and versioning information	N/A	N/A	CO	N/A	N/A
Load key	Load cryptographic key	N/A	AES Key	CO	W	Key Load completion log message
Encrypt / Decrypt	Perform AES-CCM generation/verification	AES-ECB; AES-CCM;	AES Key	CO	R, E	Encryption or Decryption completion message
Zeroize	Zeroize all CSP's contained in memory	N/A	All SSPs	CO	Z	Zeroization completion message

Table 7 – Approved Services

5. Software/Firmware security

Integrity Techniques

The module is provided in the form of binary executable code. To ensure the firmware security, the module is protected by HMAC-SHA-1 (HMAC Cert. #A2718) algorithm. The firmware integrity test key (non-SSP) was preloaded to the module's binary at the factory and used for firmware integrity test only at

the pre-operational self-test. At module initialization, the HMAC value is recalculated and compared to the hardcoded build-time generated MAC value. If at load time the signature does not match, the crypto module library exits with error. If at any point the integrity checks or known answer test fails, the module will go into an error state and will not be useable until the module is power cycled, and the integrity checks and known answer tests are run again.

Integrity Test On-Demand

While the integrity test is performed as part of the Pre-Operational Self Tests, the operator can also run the on-demand tests at any time using the API or by power cycling the device.

6. Operational Environment

The module operates QNX 7.0.4, which is a 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.

7. 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.

8. Non-Invasive Security

The module does not claim any non-invasive security.

9. Sensitive Security Parameters Management

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Key / SSP Name / Type	Strength	Security Function and Cert. #	Generation	Import / Export	Establish-ment	Storage	Zeroization	Use & related keys
AES Key	128 bits	AES-ECB; AES-CCM; Cert. # A1146	N/A	Import: This key is entered into the module via API within GPC's INT pathways in plaintext Export: No	N/A	Module Hardware Component's RAM	API Zeroization function	Used to protect module's wireless radio data

Table 8 – SSPs

10. Self-Tests

When the module is loaded or instantiated (after being powered off, rebooted, etc.), the module runs pre-operational self-tests. The operating system is responsible for the initialization process and loading of the library. The module is designed with a default entry point (DEP) which ensures that the self-tests are initiated automatically when the module is loaded. Prior to the module providing any data output via the data output interface, the module performs and passes the pre-operational self-tests. Following the successful pre-operational self-tests, the module executes the Conditional Cryptographic Algorithm Self-tests (CASTs).

The self-test success or failure results are an output of the return value of the library load API call, which is functioning as the self-test status indicator. If any one of the self-tests fails, the module transitions into an error state and outputs the error message via the module's status output interface. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module. All self-tests must be completed successfully before the module transitions to the operational state.

Below are the details of the self-tests conducted by the module.

1. Pre-Operational Self-Tests:
    - Pre-operational Firmware Integrity Test
        - HMAC-SHA-1 KAT
        - SHA-1 KAT
        - Firmware Integrity Test (HMA-SHA-1)

2. Conditional Self-Test:
    - Conditional Cryptographic Algorithm Self-Tests (CASTs)
        - AES-ECB 128 bits Encrypt KAT
        - AES-ECB 128 bits Decrypt KAT
        - AES-CCM 128 bits Authenticated Encrypt KAT
        - AES-CCM 128 bits Authenticated Decrypt KAT
        - HMAC-SHA-1 KAT
        - SHA-1 KAT

11. Life-Cycle Assurance

Secure Operation

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.

The module is enabled by default (and hence used automatically) as part of the device without any user configuration. The module always runs in the Approved Mode of Operation and does not implement any Non-Approved Security Functions. When the module is instantiated (after being powered off, rebooted, etc.), the module runs pre-operational self-tests without any operator intervention. The Module will be operated in an approved mode of operation when pre-operational self-tests have completed successfully.

The module is provided directly to solution developers and is not intended for direct download by the general public.

The module supports a Crypto Officer role only.

The module provides no authentication.

When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.

Power-up self-tests do not require any operator action.

Data output shall be inhibited during self-tests, zeroization, and error states.

Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

There are no restrictions on which keys or CSPs are zeroized by the zeroization service.

The module does not support concurrent operators.

The module does not support a maintenance interface or role.

The module does not support manual key entry.

The module does not have any external input/output devices used for entry/output of data.

The module does not output plaintext CSPs. The module does not output intermediate key values.

12. Mitigation of Other Attacks

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-3 requirements.