Zebra Technologies Corporation

Zebra 9098 Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 6
2.3 Excluded Components 7
2.4 Modes of Operation 7
2.5 Algorithms 8
2.6 Security Function Implementations 9
2.7 Algorithm Specific Information 9
2.8 RBG and Entropy 9
2.9 Key Generation 9
2.10 Key Establishment 9
2.11 Industry Protocols 9
3 Cryptographic Module Interfaces 9
3.1 Ports and Interfaces 9
4 Roles, Services, and Authentication 10
4.1 Authentication Methods 10
4.2 Roles 10
4.3 Approved Services 10
4.4 Non-Approved Services 12
4.5 External Software/Firmware Loaded 12
5 Software/Firmware Security 12
5.1 Integrity Techniques 12
5.2 Initiate on Demand 12
6 Operational Environment 12
6.1 Operational Environment Type and Requirements 12
7 Physical Security 13
7.1 Mechanisms and Actions Required 13
8 Non-Invasive Security 13
9 Sensitive Security Parameters Management 13
9.1 Storage Areas 13
9.2 SSP Input-Output Methods 13
9.3 SSP Zeroization Methods 14

9.4 SSPs 14
9.5 Transitions 14
10 Self-Tests 14
10.1 Pre-Operational Self-Tests 14
10.2 Conditional Self-Tests 15
10.3 Periodic Self-Test Information 15
10.4 Error States 16
10.5 Operator Initiation of Self-Tests 16
11 Life-Cycle Assurance 16
11.1 Installation, Initialization, and Startup Procedures 16
11.2 Administrator Guidance 17
11.3 Non-Administrator Guidance 17
12 Mitigation of Other Attacks 18

List of Tables

Table 1: Security Levels....5
Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)....7
Table 3: Tested Module Identification – Hybrid Disjoint Hardware....7
Table 4: Tested Operational Environments - Software, Firmware, Hybrid....7
Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid....7
Table 6: Modes List and Description....8
Table 7: Approved Algorithms....8
Table 8: Security Function Implementations....9
Table 9: Ports and Interfaces....10
Table 10: Roles....10
Table 11: Approved Services....11
Table 12: Mechanisms and Actions Required....13
Table 13: Storage Areas....13
Table 14: SSP Input-Output Methods....13
Table 15: SSP Zeroization Methods....14
Table 16: SSP Table 1....14
Table 17: SSP Table 2....14
Table 18: Pre-Operational Self-Tests....15
Table 19: Conditional Self-Tests....15
Table 20: Pre-Operational Periodic Information....15
Table 21: Conditional Periodic Information....16
Table 22: Error States....16

List of Figures

Figure 1: Module’s Hardware Component....6
Figure 2: Block Diagram....6

1 General

1.1 Overview

This document defines the Security Policy for Zebra 9098 Cryptographic Module from Zebra Technologies Corporation, hereinafter referred to as the Module. The module resides in the 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.

1.2 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module 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	1

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is a multi-chip standalone Hybrid Firmware module, and is used by Zebra Technologies devices.

Module Type: Firmware-hybrid

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The module's cryptographic boundary includes all firmware and disjoint hardware components utilized by the module. Please refer to Figure 2 below for details. In addition, Figure 1 below show the module's disjoint hardware component (NXP 88W9098 with hardware version 914C).

Figure 1: Module's Hardware Component

Please note that Model number WYSBHVDXP appeared in Figure 1 above is referenced to Module's hardware component NXP 88W9098. The disjoint hardware component versioning information (914C) can be retrieved via command: ! U1 getvar "card.cardid".

Tested Operational Environment's Physical Perimeter (TOEPP):

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

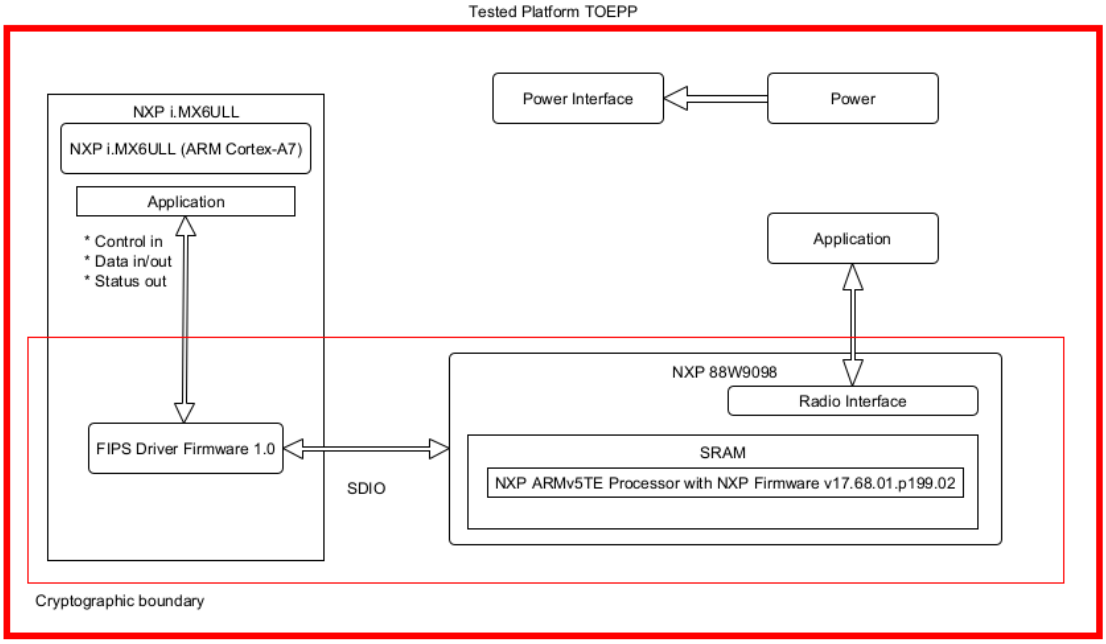

Figure 2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
devnp-mv9098-fips.so	FIPS Driver Firmware Version 1.0		HMAC-SHA-1

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
NXP 88W9098	914C	NXP Firmware v17.68.01.p199.02	NXP ARMv5TE	

Table 3: Tested Module Identification – Hybrid Disjoint Hardware

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
QNX 7.0.4	Zebra ZQ620 Plus Printer	NXP i.MX6ULL (ARM Cortex-A7)	No		FIPS Driver Firmware Version 1.0

Table 4: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
QNX 7.0.4	ZQ600 Plus series Zebra printers
QNX 7.0.4	ZD421D, ZD621D, ZD421T, ZD411D, ZD411T, ZD611D, ZD611T series Zebra printer with option kit P1134555-017A
QNX 7.0.4	ZD421D, ZD621D, ZD421T, ZD411D, ZD411T, ZD611D, ZD611T series Zebra printer with option kit P1130666-017A
QNX 7.0.4	ZD421C, ZD621T, ZD621R series Zebra printers with option kit P1134555-239A
QNX 7.0.4	ZD421C, ZD621T, ZD621R series Zebra printers with option kit P1130666-239A
QNX 7.0.4	ZT411/ZT411R, ZT421/ZT421R, ZT610/ZT610R, and ZT620/ZT620R series Zebra printers with option kit P1131216-01A

Table 5: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

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

2.3 Excluded Components

Not Applicable as the module doesn’t exclude components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
General Operation	The Module always operates in an Approved manner/mode	Approved	Normal mode operation status (as the module is always operated in approved mode)

Table 6: Modes List and Description

By design, the module only implements 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.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CCM	A6540	Key Length - 128 Tag Length - 64 IV Length - IV Length: 104 Payload Length - Payload Length: 8-256 Increment 8 AAD Length - AAD Length: 120-240 Increment 8	SP 800-38C
AES-ECB	A6540	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
HMAC-SHA-1	A5388	MAC - MAC: 160 Key Length - Key Length: 112-512 Increment 8	FIPS 198-1
SHA-1	A5388	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 7: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Encryption/Decryption	BC-Auth	AES-CCM encryption/decryption		AES-ECB: (A6540) AES-CCM: (A6540)
Firmware Integrity Test	MAC	Firmware Integrity Test by using HMAC-SHA-1		HMAC-SHA-1: (A5388) SHA-1: (A5388)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

Not applicable for this module.

2.8 RBG and Entropy

Not applicable as the module doesn't implement RBG and Entropy.

2.9 Key Generation

Not applicable as the module doesn't support key generation.

2.10 Key Establishment

Not applicable as the module doesn't implement key establishment.

2.11 Industry Protocols

Not applicable as the module doesn't implement industry protocols.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The module's physical perimeter encompasses the case of the tested platform mentioned in Section 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).

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Input	Arguments for an API call that provide the data to be used or processed by the module

Physical Port	Logical Interface(s)	Data That Passes
N/A	Data Output	Arguments output from Module to respond to an API call
N/A	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
N/A	Status Output	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	Control Output	N/A
Radio Interface	Data Input	Plaintext/Ciphertext that passes into the module
Radio Interface	Data Output	Plaintext/Ciphertext that outputs from the module
Power Interface	Power	Power supply

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A as the module doesn't implement authentication methods.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	Crypto Officer	None

Table 10: Roles

The Crypto Officer is implicitly assumed based on the service requested. The module does not allow concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show version	Show module's name/ID and versioning information	N/A	Command to read module's version	Module's name/ID and versioning	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				information		
Show status	Show module's status	N/A	Command to read module's status	Module's current status	None	Crypto Officer
Perform self-tests	Perform cryptographic algorithm self-tests on demand	N/A	Command to conduct self-tests	Self-tests status	Firmware Integrity Test	Crypto Officer
Load key	Load AES-CCM key into the module from an APP within Module's TOEPP	N/A	Command to set AES-CCM key	Updated AES-CCM key status	None	Crypto Officer - AES Key: G,W,E,Z
Encrypt/Decrypt operation	Perform AES-CCM generation/verification	AES-CCM encryption or decryption successful completion message	Command to conduct the encryption and decryption operation	Encrypted or Decrypted message	Encryption/Decryption	Crypto Officer
Perform zeroization	Zeroize all SSPs stored within the module	N/A	Command to zeroize all SSPs	Key zeroization status	None	Crypto Officer

Table 11: Approved Services

The following API function can be used for 'show version' service to retrieve module's firmware versions.

1. API function call 'cat /dev/wlan0/FIPS/module_version' to retrieve firmware version v1.0 on Module's FIPS Driver.

2. API function call 'cat /dev/wlan0/status/firmware_version' to retrieve firmware version v17.68.01.p199.02 on NXP 88W9098 (disjoint hardware component)

4.4 Non-Approved Services

N/A as the module doesn't support non-approved services.

4.5 External Software/Firmware Loaded

Not Applicable as the module doesn't support external firmware load function.

5 Software/Firmware Security

5.1 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. #A5388) 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 MAC value 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.

5.2 Initiate 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

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The module operates QNX 7.0.4, which is an embedded non-modifiable operational environment installed on a generic tested platform (e.g., printer). The firmware driver component of the module is loaded into the embedded OS by the manufacture prior to deployment to the end user. The QNX 7.0.4 embedded operating system runs in single operator mode only. The module has been tested on QNX 7.0.4 running on a Zebra ZQ620 Plus printer with i.MX6ULL CPU.

- The module has control over its own SSPs
- The module separates individual application processes from each other to prevent uncontrolled access to CSPs and uncontrolled modification of SSPs. This ensures direct access to CSPs and SSPs is restricted to the cryptographic module and the trusted parts of the operational environment

- Processes spawned by the module are owned by the module and not by the external processes/operators

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Production grade components	N/A	N/A

Table 12: Mechanisms and Actions Required

The module is a multi-chip standalone Hybrid Firmware cryptographic module. The module meets the FIPS 140-3 Level 1 security requirements as production grade equipment.

8 Non-Invasive Security

Not Applicable as the module doesn’t implement non-invasive security techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Disjoint hardware component's RAM	RAM memory provided by Module's disjoint hardware component for the temporary storage	Dynamic
Tested platform's RAM	RAM memory provided by Tested platform (in addition to disjoint hardware component's RAM) for the temporary storage	Dynamic

Table 13: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Load key	The application outside the module's boundary, but still within Module's TOEPP	Module	Plaintext	Manual	Electronic	

Table 14: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Command	CO invokes zeroization service	The zeroization command will erase all SSPs stored within the module	CO issues command 'cat zeroize_key'
Power Off	Power off the tested platform	Powering off the tested platform will erase all SSPs stored within the module	Power off

Table 15: SSP Zeroization Methods

The zeroized SSPs cannot be retrieved or reused. Once the command is initiated, the SSPs are overwritten with 0s.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES Key	AES-CCM key used to encrypt/decrypt the traffic	128 bits - 128 bits	CSP - CSP			Encryption/Decryption

Table 16: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	Load key	Disjoint hardware component's RAM:Plaintext Tested platform's RAM:Plaintext	Until reboot	Zeroization Command Power Off	

Table 17: SSP Table 2

9.5 Transitions

SHA-1: The module includes an implementation of SHA-1 for hashing. This implementation will be non-Approved for all uses starting January 1, 2031.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA-1 (A5388)	HMAC-SHA-1	KAT	SW/FW Integrity	Module is in normal state	HMAC-SHA-1

Table 18: Pre-Operational Self-Tests

When the module is 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 into the memory. 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).

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM Authenticated Encrypt KAT (A6540)	128 bits	KAT	CAST	Module is in normal state	Authenticated Encryption	Power Up
AES-CCM Authenticated Decrypt KAT (A6540)	128 bits	KAT	CAST	Module is in normal state	Authenticated Decryption	Power up
HMAC-SHA-1 KAT (A5388)	SHA-1	KAT	CAST	Module is in normal state	HMAC-SHA-1	Power up

Table 19: Conditional 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).

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA-1 (A5388)	KAT	SW/FW Integrity	Recommend 60 Days	Reboot the tested platform

Table 20: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM Authenticated Encrypt KAT (A6540)	KAT	CAST	Recommend every 60 Days	Reboot the tested platform
AES-CCM Authenticated Decrypt KAT (A6540)	KAT	CAST	Recommend every 60 Days	Reboot the tested platform
HMAC-SHA-1 KAT (A5388)	KAT	CAST	Recommend every 60 Days	Reboot the tested platform

Table 21: Conditional Periodic Information

The module performs on-demand self-tests initiated by the operator, by power cycling to the module. The full suite of self-tests is then executed. The same procedure may be employed by the operator to perform periodic self-tests.

In addition, the Crypto Officer shall perform the periodic test on demand no less than every 90 days to ensure all components are functioning correctly.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error State	If self-test tests fail, the module enters error state	Self-test failure	Reboot the tested platform	Error message "FIPS KAT failed!" is logged; System halt

Table 22: Error States

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.

10.5 Operator Initiation of Self-Tests

The operator can initiate the self-test by power cycling or rebooting the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The validated firmware versions listed in Tables 2 and 2a 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 loaded or 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 is capable of commanding the module to perform the cryptogamic algorithms self-tests by cycling power or resetting the module.

Cryptogamic algorithms self-tests (CASTs) do not require any operator action.

Data output is 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.

11.2 Administrator Guidance

No specific Administrator guidance.

11.3 Non-Administrator Guidance

No specific non-Administrator guidance.

12 Mitigation of Other Attacks

Not Applicable as the module does not claim mitigation of other attacks.