From Web Cryptik

From Web Cryptik

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

[1 General 7](#_Toc164700004)

[1.1 Overview 7](#_Toc164700005)

[1.2 Security Levels 7](#_Toc164700006)

[1.3 Additional Information [O] 7](#_Toc164700007)

[2 Cryptographic Module Specification 7](#_Toc164700008)

[2.1 Description 7](#_Toc164700009)

[2.2 Tested and Vendor Affirmed Module Version and Identification 7](#_Toc164700010)

[2.3 Excluded Components 8](#_Toc164700011)

[2.4 Modes of Operation 8](#_Toc164700012)

[2.5 Algorithms 8](#_Toc164700013)

[2.6 Security Function Implementations 9](#_Toc164700014)

[2.7 Algorithm Specific Information 9](#_Toc164700015)

[2.8 RBG and Entropy 9](#_Toc164700016)

[2.9 Key Generation 9](#_Toc164700017)

[2.10 Key Establishment 10](#_Toc164700018)

[2.11 Industry Protocols 10](#_Toc164700019)

[2.12 Additional Information [O] 10](#_Toc164700020)

[3 Cryptographic Module Interfaces 10](#_Toc164700021)

[3.1 Ports and Interfaces 10](#_Toc164700022)

[3.2 Trusted Channel Specification [O] 10](#_Toc164700023)

[3.3 Control Interface Not Inhibited [O] 10](#_Toc164700024)

[3.4 Additional Information [O] 10](#_Toc164700025)

[4 Roles, Services, and Authentication 10](#_Toc164700026)

[4.1 Authentication Methods 10](#_Toc164700027)

[4.2 Roles 10](#_Toc164700028)

[4.3 Approved Services 11](#_Toc164700029)

[4.4 Non-Approved Services 11](#_Toc164700030)

[4.5 External Software/Firmware Loaded 11](#_Toc164700031)

[4.6 Bypass Actions and Status [O] 11](#_Toc164700032)

[4.7 Cryptographic Output Actions and Status [O] 11](#_Toc164700033)

[4.8 Additional Information [O] 11](#_Toc164700034)

[5 Software/Firmware Security 11](#_Toc164700035)

[5.1 Integrity Techniques 11](#_Toc164700036)

[5.2 Initiate on Demand 11](#_Toc164700037)

[5.3 Open-Source Parameters [O] 11](#_Toc164700038)

[5.4 Additional Information [O] 12](#_Toc164700039)

[6 Operational Environment 12](#_Toc164700040)

[6.1 Operational Environment Type and Requirements 12](#_Toc164700041)

[6.2 Configuration Settings and Restrictions [O] 12](#_Toc164700042)

[6.3 Additional Information [O] 12](#_Toc164700043)

[7 Physical Security 12](#_Toc164700044)

[7.1 Mechanisms and Actions Required [O] 12](#_Toc164700045)

[7.2 User Placed Tamper Seals [O] 12](#_Toc164700046)

[7.3 Filler Panels [O] 12](#_Toc164700047)

[7.4 Fault Induction Mitigation [O] 13](#_Toc164700048)

[7.5 EFP/EFT Information [O] 13](#_Toc164700049)

[7.6 Hardness Testing Temperature Ranges [O] 13](#_Toc164700050)

[7.7 Additional Information [O] 13](#_Toc164700051)

[8 Non-Invasive Security 13](#_Toc164700052)

[8.1 Mitigation Techniques [O] 13](#_Toc164700053)

[8.2 Effectiveness [O] 13](#_Toc164700054)

[8.3 Additional Information [O] 13](#_Toc164700055)

[9 Sensitive Security Parameters Management 13](#_Toc164700056)

[9.1 Storage Areas 13](#_Toc164700057)

[9.2 SSP Input-Output Methods 13](#_Toc164700058)

[9.3 SSP Zeroization Methods 14](#_Toc164700059)

[9.4 SSPs 14](#_Toc164700060)

[9.5 Transitions [O] 14](#_Toc164700061)

[9.6 Additional Information [O] 14](#_Toc164700062)

[10 Self-Tests 14](#_Toc164700063)

[10.1 Pre-Operational Self-Tests 14](#_Toc164700064)

[10.2 Conditional Self-Tests 14](#_Toc164700065)

[10.3 Periodic Self-Test Information 14](#_Toc164700066)

[10.4 Error States 15](#_Toc164700067)

[10.5 Operator Initiation of Self-Tests [O] 15](#_Toc164700068)

[10.6 Additional Information [O] 15](#_Toc164700069)

[11 Life-Cycle Assurance 15](#_Toc164700070)

[11.1 Installation, Initialization, and Startup Procedures 15](#_Toc164700071)

[11.2 Administrator Guidance 15](#_Toc164700072)

[11.3 Non-Administrator Guidance 15](#_Toc164700073)

[11.4 Design and Rules [O] 15](#_Toc164700074)

[11.5 Maintenance Requirements [O] 15](#_Toc164700075)

[11.6 End of Life [O] 15](#_Toc164700076)

[11.7 Additional Information [O] 15](#_Toc164700077)

[12 Mitigation of Other Attacks 16](#_Toc164700078)

[12.1 Attack List [O] 16](#_Toc164700079)

[12.2 Mitigation Effectiveness [O] 16](#_Toc164700080)

[12.3 Guidance and Constraints [O] 16](#_Toc164700081)

[12.4 Additional Information [O] 16](#_Toc164700082)

List of Tables

Table 1: Security Levels 7

Table 2: Tested Module Identification – Hardware 8

Table 3: Tested Module Identification – Software/Firmware/Hybrid (Executable Code Sets) 8

Table 4: Tested Module Identification – Hybrid Disjoint Hardware 8

Table 5: Tested Operational Environments - Software, Firmware, Hybrid 8

Table 6: Vendor Affirmed Operational Environments - Software, Firmware, Hybrid 8

Table 7: Modes List and Description 8

Table 8: Approved Algorithms 9

Table 9: Vendor Affirmed Algorithms 9

Table 10: Non-Approved, Allowed Algorithms 9

Table 11: Non-Approved, Allowed Algorithms with No Security Claimed 9

Table 12: Non-Approved, Not Allowed Algorithms 9

Table 13: Security Function Implementations 10

Table 14: Entropy Certificates 10

Table 15: Entropy Sources 10

Table 16: Key Generation 10

Table 17: Key Agreement 10

Table 18: Key Transport 10

Table 19: Ports and Interfaces 11

Table 20: Authentication Methods 11

Table 21: Roles 11

Table 22: Approved Services 11

Table 23: Non-Approved Services 12

Table 24: Mechanisms and Actions Required 13

Table 25: EFP/EFT Information 13

Table 26: Hardness Testing Temperatures 14

Table 27: Storage Areas 14

Table 28: SSP Input-Output 14

Table 29: SSP Zeroization Methods 14

Table 30: SSP Information First 15

Table 31: SSP Information Second 15

Table 32: Pre-Operational Self-Tests 15

Table 33: Conditional Self-Tests 15

Table 34: Pre-Operational Periodic Information 15

Table 35: Conditional Periodic Information 15

Table 36: Error States 15

List of Figures

[Figure 1: Block Diagram 6](#_Toc135467278)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

# 1 General

## 1.1 Overview

<Text>

## 1.2 Security Levels

From Web Cryptik

## 1.3 Additional Information [O]

<Text>

# 2 Cryptographic Module Specification

## 2.1 Description

**Purpose and Use:**

<Text>

**Module Type**: From Web Cryptik

**Module Embodiment**: From Web Cryptik

**Module Characteristics**: From Web Cryptik

**Cryptographic Boundary:**

<Text>

**Tested Operational Environment’s Physical Perimeter (TOEPP) [O]:**

<Text>

<Other Diagrams, Photographs and Descriptive Text>

<Picture or Block Diagram>

Figure 1: Block Diagram

## 2.2 Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Hardware:**

From Web Cryptik [O]

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

From Web Cryptik [O]

**Tested Module Identification – Hybrid Disjoint Hardware:**

From Web Cryptik [O]

**Tested Operational Environments - Software, Firmware, Hybrid:**

From Web Cryptik [O]

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

From Web Cryptik [O]

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

<Excluded components statements or table>

## 2.4 Modes of Operation

**Modes List and Description:**

From Web Cryptik

<Text>

**Mode Change Instructions and Status [O]:**

<Text>

**Degraded Mode Description [O]:**

<Text>

## 2.5 Algorithms

**Approved Algorithms:**

From Web Cryptik

<Text>

**Vendor-Affirmed Algorithms:**

From Web Cryptik

<Text>

**Non-Approved, Allowed Algorithms:**

From Web Cryptik

<Text>

**Non-Approved, Allowed Algorithms with No Security Claimed:**

From Web Cryptik

<Text>

**Non-Approved, Not Allowed Algorithms:**

From Web Cryptik

<Text>

## 2.6 Security Function Implementations

From Web Cryptik

<Text>

## 2.7 Algorithm Specific Information

<Text>

## 2.8 RBG and Entropy

From Web Cryptik

From Web Cryptik

<Text>

## 2.9 Key Generation

<Text>

## 2.10 Key Establishment

<Text>

## 2.11 Industry Protocols

<Text>

## 2.12 Additional Information [O]

<Text>

# 3 Cryptographic Module Interfaces

## 3.1 Ports and Interfaces

From Web Cryptik

<Text>

## 3.2 Trusted Channel Specification [O]

<Text>

## 3.3 Control Interface Not Inhibited [O]

<Text>

## 3.4 Additional Information [O]

<Text>

# 4 Roles, Services, and Authentication

## 4.1 Authentication Methods

From Web Cryptik

<Text>

## 4.2 Roles

From Web Cryptik

<Text>

## 4.3 Approved Services

From Web Cryptik

<Text>

## 4.4 Non-Approved Services

From Web Cryptik

<Text>

## 4.5 External Software/Firmware Loaded

<Text>

## 4.6 Bypass Actions and Status [O]

<Text>

## 4.7 Cryptographic Output Actions and Status [O]

<Text>

## 4.8 Additional Information [O]

<Text>

# 5 Software/Firmware Security

## 5.1 Integrity Techniques

<Text>

## 5.2 Initiate on Demand

<Text>

## 5.3 Open-Source Parameters [O]

<Text>

## 5.4 Additional Information [O]

<Text>

# 6 Operational Environment

## 6.1 Operational Environment Type and Requirements

**Type of Operational Environment**: From Web Cryptik

**How Requirements are Satisfied** [O]:

<Text>

## 6.2 Configuration Settings and Restrictions [O]

<Text>

## 6.3 Additional Information [O]

<Text>

# 7 Physical Security

## 7.1 Mechanisms and Actions Required [O]

From Web Cryptik

<Text and Photos>

## 7.2 User Placed Tamper Seals [O]

**Number:**

**Placement:**

**Surface Preparation:**

**Operator Responsible for Securing Unused Seals:**

**Part Numbers:**

<Text and Pictures>

## 7.3 Filler Panels [O]

<Text and Pictures>

## 7.4 Fault Induction Mitigation [O]

<Text>

## 7.5 EFP/EFT Information [O]

From Web Cryptik

<Text>

## 7.6 Hardness Testing Temperature Ranges [O]

From Web Cryptik

<Text>

## 7.7 Additional Information [O]

<Text>

# 8 Non-Invasive Security

## 8.1 Mitigation Techniques [O]

<Text>

## 8.2 Effectiveness [O]

<Text>

## 8.3 Additional Information [O]

<Text>

# 9 Sensitive Security Parameters Management

## 9.1 Storage Areas

From Web Cryptik

<Text>

## 9.2 SSP Input-Output Methods

From Web Cryptik

<Text>

## 9.3 SSP Zeroization Methods

From Web Cryptik

<Text>

## 9.4 SSPs

From Web Cryptik

From Web Cryptik

<Text>

## 9.5 Transitions [O]

<Text>

## 9.6 Additional Information [O]

<Text>

# 10 Self-Tests

## 10.1 Pre-Operational Self-Tests

From Web Cryptik

<Text>

## 10.2 Conditional Self-Tests

From Web Cryptik

<Text>

## 10.3 Periodic Self-Test Information

From Web Cryptik

From Web Cryptik

<Text>

## 10.4 Error States

From Web Cryptik

<Text>

## 10.5 Operator Initiation of Self-Tests [O]

<Text>

## 10.6 Additional Information [O]

<Text>

# 11 Life-Cycle Assurance

## 11.1 Installation, Initialization, and Startup Procedures

<Text>

## 11.2 Administrator Guidance

<Text>

## 11.3 Non-Administrator Guidance

<Text>

## 11.4 Design and Rules [O]

<Text>

## 11.5 Maintenance Requirements [O]

<Text>

## 11.6 End of Life [O]

<Text>

## 11.7 Additional Information [O]

<Text>

# 12 Mitigation of Other Attacks

## 12.1 Attack List [O]

<Text>

## 12.2 Mitigation Effectiveness [O]

<Text>

## 12.3 Guidance and Constraints [O]

<Text>

## 12.4 Additional Information [O]

<Text>