KlasRouter
Security Policy

Version: 1.3

Revision Date: Oct 10, 2011

Klas Ltd.

CHANGE RECORD

Revision	*Date*	*Author*	*Description of Change*
0.1	12 Jan 11	C. Masterson	Initial Release
0.2	28 Jan 11	C. Daly	
0.3	2 Mar 11	C. Masterson	Updated to add more detail after initial review.
0.4	18 Apr 11	C. Masterson	Updated following second review.
0.5	9 May 11	C. Masterson	Minor changes to services.
0.6	12 May 11	C. Masterson	Added photos of tamper labels.
1.0	17 June 2011	C. Masterson	Updated following final review.
1.1	17 June 2011	C. Masterson	Updated following final review.
1.2	23 Sept 2011	C. Masterson	Updated following submission to NIST
1.3	10 Oct 2011	C. Masterson	Updated following submission to NIST

Contents

Tables

Figures

Module Overview

KlasRouter is a fully-functional compact router that offers deployable, converged network communications over satellite. With its embedded 8-port FastEthernet Switch and 4-port VoIP package, KlasRouter has everything a team needs to utilize their voice, data, and video resources to their full potential. Additionally, KlasRouter was designed to combine ease-of-use with the smallest possible form factor for maximum portability. Built upon a standards-based platform, KlasRouter is interoperable with IT infrastructures and the perfect solution for establishing a remote office in a secure environment.

KlasRouter utilizes FIPS 140-2 cryptographic algorithms, including AES-256 and Suite-B algorithms.

Figure 1 – Front of the Cryptographic Module

The Klas Ltd. KlasRouter (hereafter referred to as the module) is a multi-chip standalone module, as defined by FIPS 140-2. The boundary of the module is the outer metal enclosure. There are some components which have been excluded from the requirements of FIPS 140-2. None of these components are security relevant that could lead to a compromise of the module.

Figure 2 – Rear of the Cryptographic Module

The configuration of hardware and firmware for this validation is:

Hardware: KlasRouter, Version 3.02 and Version 3.03;

- The two different versions have different ROM chips.

Firmware: KlasOS 3, Version 3.1.0 rc0

Figure 3 depicts the logical block diagram for the module, with the cryptographic boundary shown in red. The entire KlasRouter is within the cryptographic boundary.

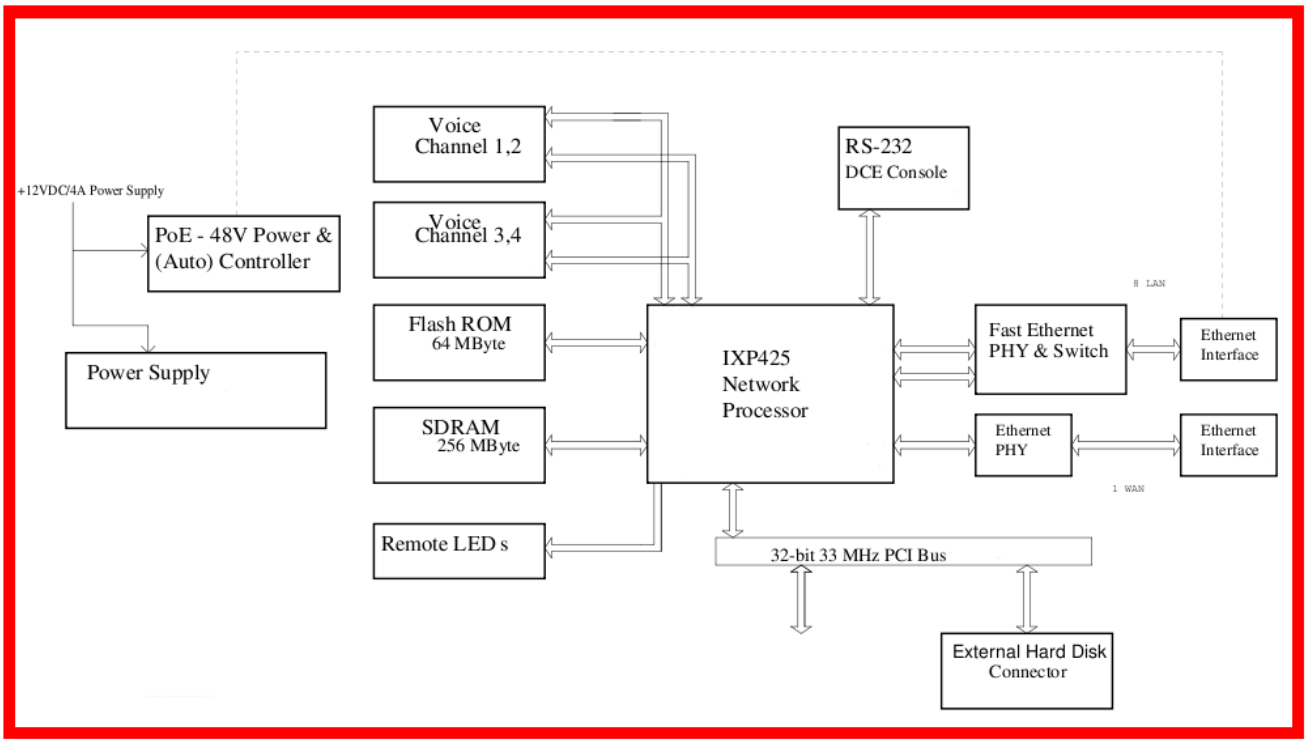

Figure 3 - Logical Block Diagram

Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Modes of Operation

The module can be configured in both FIPS and non-FIPS modes. By default the module boots into non-FIPS mode.

The module provides a command-line interface (CLI) to allow an operator to initially configure it through the Console port or a Network port using SSH. The user 'klas' will be assigned the Crypto-Officer role.

1.1 FIPS Approved Mode of Operation

After initialization, the operator must confirm that the firmware version has been FIPS Approved before enabling FIPS mode.

To enable FIPS mode the user must do the following steps:

- Connect a serial cable to the console port and use a terminal emulator to log into the module as user 'klas' (default password is 'klas').
- From the Menu Displayed select option 7, “Advanced Configuration”
- From the Advanced Configuration sub-menu select option 5, “VPN Configuration”
- From the VPN Configuration sub-menu select option 1, “IPSec”
- From the IPSec sub-menu select option 9, “FIPS Mode”
- From the FIPS Mode sub-menu select option 1, “Enable FIPS Mode”.

Upon confirmation of switching to FIPS mode, the operator will then be prompted to enter a new login password that must be a minimum of 8 characters in length. Once this has been completed the module will be zeroized and reset to factory defaults, storing the updated password for use after the power cycle. The module will then reboot and will subsequently enter FIPS mode once the Power-Up Self Tests have been completed successfully. The operator can then verify that the device is operating in FIPS mode through the IPSec sub-menu in the CLI after login.

The device will impose the following restrictions when operating in FIPS mode:

- SSH access will be disabled.
- The ability to transfer KlasRouter configuration files to and from a PC via TFTP is disabled.
- CLI configuration will only be accessible through the console port.
- MD5 will be disabled in IPSec.
- Only Diffie-Hellman Groups 14 to 21 and Group 26 are allowed in FIPS mode.

1.2 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms:

Table 2 - FIPS Approved Algorithms Used in Current Module

Approved Algorithm	CAVP Cert. #
AES (ECB, CBC, CTR, CCM, CMAC, GCM, 128, 192, 256 modes; E/D; 128, 192 and 256)	1599
Triple-DES (3-key; TCBC mode; E/D)	1045
HMAC-SHA-1, SHA-256, SHA-384, SHA-512	936
SHA-1, SHA-256, SHA-384, SHA-512	1411
ECDSA key generation, signature generation and verification (CURVES P; 192, 224, 256, 384, 521)	197
FIPS 186-2 RNG	856

The cryptographic module supports the following non-FIPS Approved algorithms which are allowed for use in FIPS mode:

Table 3 – FIPS Allowed Algorithms Used in Current Module

FIPS Allowed Algorithm
Diffie-Hellman (for key agreement; 2048 bits which provides 112 bits of security)
ECDH (for key agreement; 224 bits which provides 112 bits of security, 256 bits, which provides 128 bits of security, 384 bits which provides 192 bits of security, 512 bits, which provides 256 bits of security)
NDRNG (used to seed the FIPS-approved RNG)

1.3 Non-Approved, Non-Allowed Algorithms

The cryptographic module supports the following non-Approved algorithms only if the module is not in FIPS mode. No security claim is made in the current module for any of the following non-Approved algorithms.

Table 4 - Non-Approved, Non-Allowed Algorithms Used in Current Module

Non-FIPS Allowed Algorithm
MD5
HMAC-MD5
Diffie-Hellman Groups 1,2, and 5
DSA key generation, signature generation and verification (used only in non-FIPS mode within SSH)

Ports and Interfaces

The module is a multi-chip standalone with ports and interfaces as shown below.

Table 5 - Module FIPS 140-2 Ports and Interfaces

Interface	FIPS 140-2 Designation	Name and Description
Power	Power input	12V DC
Ethernet (8)	Data input, Data output, Control input, Status output	10/100 FastEthernet RJ45 interfaces.
Power over Ethernet (1)	Power output	10/100 FastEthernet RJ45 interface. There is 1 designated PoE port within the 8 FastEthernet ports.
Voice (4)	Data input, Data output, Control input	POTS, RJ11 interface
Status Interface	Status Output	Non-standard pinout for LED status board. LED board shows Power, Ethernet Activity, Voice over IP activity, Power over Ethernet status.
External Hard Disk Connector (2)	Data input, Data output	Non-standard pinout. Provides connection for Klas-provided USB Hard Disk.
Console	Data input, Control input, Status output	RS232 interface used for configuration via a directly connected cable.

Identification and Authentication Policy

1.4 Assumption of Roles

The module supports two distinct operator roles, Crypto Officer (CO) and User. Authentication for the CO is based on Username and Password and authentication for the User is based on the IPSec handshake.

The module does not provide a bypass capability.

Table 6 - Roles and Required Identification and Authentication

Role	Description	Authentication Type	Authentication Data
CO	This role has access to services for configuring and monitoring the module.	Identity-based operator authentication	Username and password (minimum 8 characters, standard ASCII)
User	This role accesses the VPN services offered by the module. (peer router)	Identity-based operator authentication	IP Address and 160-bit HMAC key used in IPSec Handshake

Table 7 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
CO login via console	The probability that a random attempt will succeed or a false acceptance will occur is $1/(2.18 \times 10^{14})$ which is less than 1/1,000,000. The maximum login attempts that can be made in a minute via the console port in FIPS mode is 14. The probability of successfully authenticating to the module within one minute is hence $1/(1.45 \times 10^{13})$ which is less than 1/100,000.
User validation via IPSec	KlasRouter uses a minimum HMAC key length of 160-bits.This means the probability that a random attempt will succeed is $1/(2^{160})$ which is less than 1/1,000,000. The maximum number of connection attempts that can be made on KlasRouter per minute is 10,000 which results in a total probability of randomly authenticating to the module within a minute of $600,000/(2^{160})$ which is less than 1/1,000,000.

Access Control Policy

1.5 Roles and Services

Table 8 – Authenticated Services

Service	Used By	Description
View Configuration	CO	Ability to view configuration parameters via the CLI
Configure Switch	CO	Configuring the layer 2 switching capabilities of the module
Configure Routing	CO	Configuring the layer 3 routing capabilities of the module
Configure VoIP	CO	Configuring the parameters for transmitting voice over IP
VPN Configuration	CO	Configuring the VPN policies. Enable/Disable FIPS
Configure WAN Acceleration	CO	Configuring acceleration for the WAN link (might include TLS, HTTPS acceleration, SCPS and Caching)
Show Status	CO	Viewing status via the CLI
Profiles	CO	Create and save profiles
Configure ACLs	CO	Configuring the Access Control Lists
Configure QoS	CO	Configuring Quality of Service
Configure PAT	CO	Configuring Port Address Translation
Configure SNMP	CO	Configuring SNMP
IPSec VPN Connectivity	User	Connect to a peer router via IPSec session
Zeroize	CO	Erase all CSPs and reset the router to factory default configuration

1.6 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 9 - Unauthenticated Services

Service	Description
Perform Self-tests	Causing the module to perform self-tests on demand by power-cycling the module
Show Status	Collect status from the module LED status interfaces
Reset to Factory Defaults	Reset the router to factory default configuration at prompt during boot up

1.7 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 10 - Private Keys and CSPs

Key Name	Description
Pre-shared Key (PSK)	Pre-shared key used in the IPSec handshake (IKE) to authenticate the User
CO Password	CO Password
DH Private Components	Used to derive the secret session key during DH key agreement protocol
ECDH Private Components	Used to derive the secret session key during DH key agreement protocol
DRNG Seed Key	Used to seed the RNG for key generation
DRNG Seed	Used to seed the RNG for key generation
TDES Session Key	For TDES encryption/decryption of data
AES Session Key	For AES encryption/decryption of data
HMAC Key	Used in HMAC SHA-1, 256, 384 and 512
XAUTH Password	Xauth password used in IPSec

1.8 Definition of Public Keys

The module contains the following public keys:

Table 11 - Public Keys

Key Name	Description
DH Public Component	Receive Client Public Component during DH exchange. Transmit Host Public Component during DH exchange
ECDH Public Components	Receive Client Public Component during DH exchange. Transmit Host Public Component during DH exchange

1.9 Definition of CSPs Modes of Access

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

G = Generate: The module generates the CSP.

R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.

W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, or the module generates a CSP, or the module overwrites an existing CSP.

Z = Zeroize: The module zeroizes the CSP.

Table 12 - CSP Access Rights within Roles & Services

Role	Authorized Service	Mode	Cryptographic key or CSP
CO	VPN Configuration	GR	Generate DH Key pair.
		GR	Use DH parameters.
		GR	Use DH private component.
		GR	Generate DH shared secret.
		GR	Use ECDH private component.
		GR	Generate ECDH shared secret.
		GR	Use AES key.
		GR	Use TDES key.
		GR	Generate SHA-1 output.
		GR	Generate SHA-256 output.
		GR	Generate SHA-384 output.
		GR	Generate SHA-512 output.
		GR	Use HMAC-SHA-1 key.

		GR GR GR GR GR GR GR GR GWR	Generate HMAC-SHA-1 output. Use HMAC-SHA-256 key. Generate HMAC-SHA-256 output. Use HMAC-SHA-384 key. Generate HMAC-SHA-384 output. Use HMAC-SHA-512 key. Generate HMAC-SHA-512 output. Use seed key to generate random number. Destroy Seed Key after use. Input and read Pre-Shared Keys.
CO	View Configuration	R	View Pre-Shared key over direct connection
CO	Profiles	GWR	Input and read Pre-Shared Keys.
User	IPSec VPN Connectivity	GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR GR	Generate DH Key pair. Use DH parameters. Use DH private component. Generate DH shared secret. Use ECDH private component. Generate ECDH shared secret. Use AES key. Use TDES key. Generate SHA-1 output. Generate SHA-256 output. Generate SHA-384 output. Generate SHA-512 output. Use HMAC-SHA-1 key. Generate HMAC-SHA-1 output. Use HMAC-SHA-256 key. Generate HMAC-SHA-256 output. Use HMAC-SHA-384 key. Generate HMAC-SHA-384 output. Use HMAC-SHA-512 key. Generate HMAC-SHA-512 output. Use seed key to generate random number. Destroy Seed Key after use.
CO	Zeroize	Z	Destroy all CSPs.

Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Module does not contain a modifiable operational environment.

Security Rules

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

The cryptographic module shall provide two distinct operator roles. These are the Cryptographic Officer and the User role.

The cryptographic module shall provide identity-based authentication.

The cryptographic module shall clear previous authentications on power cycle.

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

The cryptographic module shall perform the following tests:

A. Power up Self-Tests
    1. Cryptographic algorithm tests
        a) AES-ECB, CBC, CCM, CMAC, CTR, GCM Known Answer Test
        b) Triple-DES Known Answer Test
        c) SHA-1 Known Answer Test
        d) SHA-256 Known Answer Test
        e) SHA-384 Known Answer Test
        f) SHA-512 Known Answer Test
        g) HMAC-SHA-1 Known Answer Test
        h) HMAC-SHA-256 Known Answer Test
        i) HMAC-SHA-384 Known Answer Test
        j) HMAC-SHA-512 Known Answer Test
        k) ECDH Pairwise Consistency Test
        l) ECDSA Pairwise Consistency Test
        m) DH Pairwise Consistency Test
        n) FIPS 186-2 RNG Known Answer Test
    2. Firmware Integrity Test
        a) The firmware integrity test is a 32-bit CRC calculated on the firmware image by the bootloader at power-on. If the CRC check fails, the module will not boot.

B. Conditional Self-Tests

1. Continuous Random Number Generator (RNG) test – performed on NDRNG and RNG, 64 bits

On successful completion of the self-tests, the following text is printed on the console:

Performing FIPS Crypto Module Selftests ... OK.

Performing FIPS Crypto Library Selftests ... OK.

The operator shall be capable of commanding the module to perform the power up self-test by cycling power, resetting the module, or by selecting “Perform Self-tests” from the FIPS menu.

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

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

Zeroization will be invoked when the operator exits FIPS mode, or explicitly requests zeroization from the CLI. Zeroization completely overwrites all CSPs and no services are available while zeroization is taking place. The operator must be in control of the module during the entire zeroization procedure to ensure that it has successfully completed.

The module allows plaintext keys and CSPs to be output over the console after the module performs two internal actions.

The module only allows firmware to be loaded when it is in a pre-initialization state. In order to get into the pre-initialization state, the operator must exit FIPS mode, which causes all CSPs to be zeroized. When the module is reinitialized, it will only enter FIPS mode if the loaded firmware is the FIPS Approved version.

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

The module ensures that the seed and seed key inputs to the Approved RNG are not equal.

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

The module supports concurrent operators and ensures their separation by means of authentication.

The module does not support a maintenance interface or role.

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

The module does not output intermediate key values.

The following documents the security rules imposed by the vendor.

1. Presently, the module will support a maximum of 1 Crypto Officer login at a time when in FIPS mode.
2. If the Crypto Officer's login remains inactive for more than 10 minutes, the module automatically logs out the operator. This timeout period is configurable by the Crypto Officer.
3. SSH access to the module is disabled when in FIPS mode.

4. To prevent transfer of passwords via Ethernet the module cannot be put into FIPS mode via SSH.

Physical Security Policy

1.10 Physical Security Mechanisms

The KlasRouter module is a PCB assembly contained in a clear-chromated aluminum enclosure. The enclosure is screwed together and the screw heads are covered by a total of seven tamper-proof labels, applied during manufacturing. These labels have unique serial numbers etched below the surface, and attempts to remove them will result in highly noticeable markings left on the case. The enclosure itself is designed to be opaque so no components are visible through any of the ports.

1.11 Operator Required Actions

Table 13 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	12 months. If there is any evidence of tampering on the security labels stop using the module and contact Klas Technical Support immediately.	There are 7 tamper seals on the module, covering all 8 assembly screws.

1.12 Tamper Evident Seal Placement

The labels were placed in locations that would prevent the module's cover from being removed without leaving tamper evidence. There are a total of seven tamper evident labels placed around the module. These are shown in Figures 4 through 7 below.

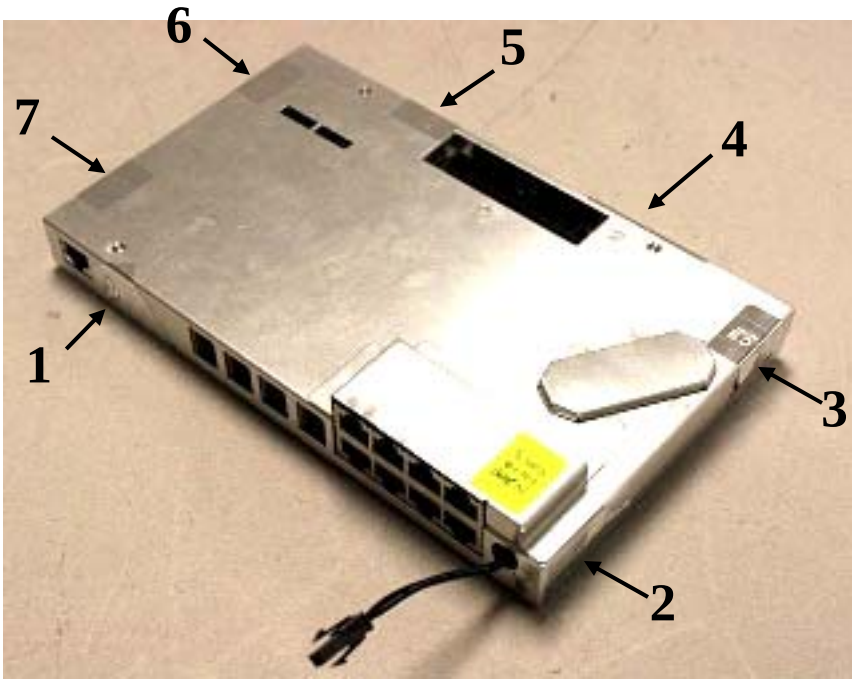

Figure 4 – Label Placement (Top/Front/Right)

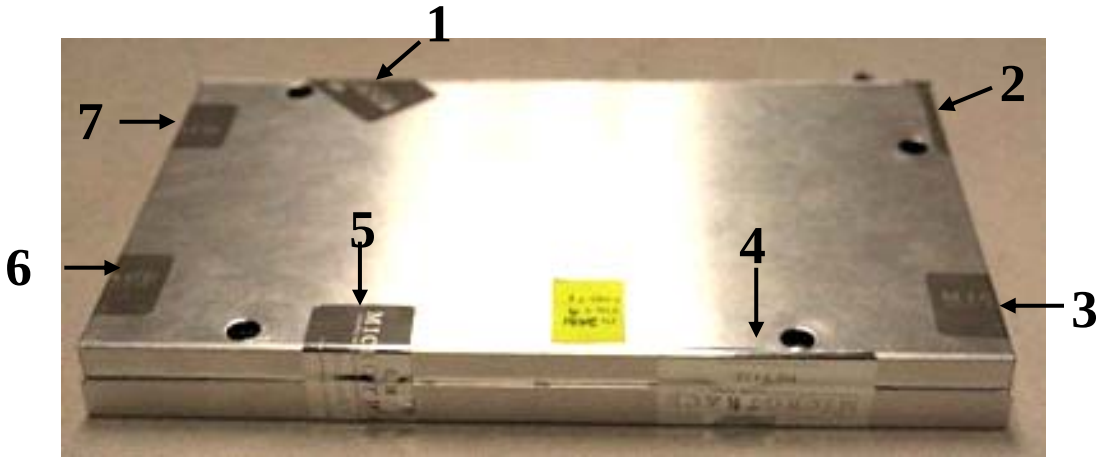

Figure 5 – Label Placement (Bottom/Back)

Figure 6 – Label Placement (Left)

Figure 7 – Label Placement (Right)

Mitigation of Other Attacks Policy

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

References

[FIPS 140-2] FIPS Publication 140-2 *Security Requirements for Cryptographic Modules*

<References>

Definitions and Acronyms

ACL – Access Control List
AES – Advanced Encryption Standard
ASCII – American Standard Code for Information Interchange
CBC – Cipher Block Chaining
CCM – Counter with CBC MAC
CLI – Command Line Interface
CMAC – Cipher based Message Authentication Code
CO – Crypto Officer
CSP – Critical Security Parameter
CTR – Counter
DC – Direct Current
DES – Data Encryption Standard
DH – Diffie-Hellman
DRNG – Deterministic Random Number Generator
ECDH – Elliptic Curve Diffie-Hellman
ECDSA – Elliptic Curve Digital Signature Algorithm
EMC – Electromagnetic Compatibility
EMI – Electromagnetic Interference
FIPS – Federal Information Processing Standard
GCM – Galois/Counter Mode
HMAC – Hashed Message Authentication Code
HTTP – Hyper Text Transfer Protocol
HTTPS – Hyper Text Transfer Protocol Secure
IKE – Internet Key Exchange
IT – Information Technology
IPSec – Internet Protocol Security
LED – Light Emitting Diode
MD5 – Message Digest 5 Algorithm
NDRNG – Non Deterministic Random Number Generator
PAT – Port Address Translation

PCB – Printed Circuit Board
POTS – Plain Old Telephone System
QoS – Quality Of Service
RNG – Random Number Generator
RS232 – Recommended Standard 232
SCPS – Space Communications Protocol Standards
SHA – Secure Hash Algorithm
SNMP – Simple Network Management Protocol
SSH – Secure Shell
TDES – Triple Data Encryption Standard
TFTP – Trivial File Transfer Protocol
TLS – Transport Layer Security
USB – Universal Serial Bus
VoIP – Voice Over Internet Protocol
VPN – Virtual Private Network
WAN – Wide Area Network