



SCHWEITZER ENGINEERING LABORATORIES, INC.

2350 NE Hopkins Court • Pullman, WA 99163-5603 USA

Tel: +1.509.332.1890 • Fax: +1.509.332.7990

www.selinc.com • info@selinc.com

SEL-3044

Security Policy

Schweitzer Engineering Laboratories, Inc.

Version: 0.11

Copyright 2009-2010 Schweitzer Engineering Laboratories, Inc.

May be reproduced only in its original entirety [without revision].



Contents

1	Definitions and Acronyms	4
2	References	4
3	Module Overview	4
3.1	SEP.....	6
3.2	SEAP.....	6
3.3	Security Level.....	6
4	Modes of Operation	7
4.1	FIPS Approved Mode of Operation	7
4.2	Approved and Allowed Algorithms.....	7
5	Ports and Interfaces	8
5.1	Physical Ports	8
5.2	Logical Ports	9
6	Identification and Authentication Policy	12
6.1	Assumption of Roles	12
7	Access Control Policy	14
7.1	Roles and Services	14
7.2	Definition of Critical Security Parameters (CSPs).....	15
7.3	Definition of Public Keys.....	16
7.4	Definition of CSPs Modes of Access.....	16
8	Operational Environment.....	18
9	Security Rules	18
10	Physical Security Policy.....	19
10.1	Physical Security Mechanisms	19
10.2	Operator Required Actions	20
11	Mitigation of Other Attacks Policy	20



Tables

Table 1: Module Security Level Specification.....	6
Table 2: FIPS Approved Algorithms Used in Current Module	7
Table 3: FIPS Allowed Algorithms Used in Current Module.....	8
Table 4: Non-Callable Functions Present in Current Module	8
Table 5: Physical Ports.....	9
Table 6: Logical Ports	9
Table 7: Gemini Pins and FIPS 140-2 Ports and Interfaces.....	10
Table 8: Roles	12
Table 9: Identity Authentication Mechanism	13
Table 10: Roles and Service Matrix	14
Table 11: CSPs	15
Table 12: Public Keys.....	16
Table 13: CSP Access Rights within Roles & Services	16

Figures

Figure 1: Image of the Cryptographic Module	5
Figure 2: Point to Point Network	5
Figure 3: Point to Multipoint Network.....	6
Figure 4: Module Block Diagram	9



1 Definitions and Acronyms

ABI – Asynchronous Bus Interface

SCADA - Supervisory Control And Data Acquisition

SEAP – SEL Encryption and Authentication Protocol

SEP – SEL Encryption Protocol

USB – Universal Serial Bus

2 References

“SEL Encryption Protocol Specification”

3 Module Overview

The Schweitzer Engineering Laboratories, Inc. SEL-3044 (hereafter referred to as the module) is a multi-chip standalone cryptographic module encased in a hard, opaque, tamper evident PCMCIA style case. The cryptographic boundary is the entire module. No components are excluded from the cryptographic boundary.

The module is a cryptographic protocol daughter card designed to reside in a host device to secure its data on a particular communication network. The SEL-3044 implements the SEP specification to protect the data in transit.

The SEL-3044 is designed to protect devices that send and receive critical, sensitive data such as electric power revenue meters, protective relays, Programming Logic Controllers (PLC), Remote Terminal Units (RTU), and SCADA equipment from unauthorized access, control, monitoring, and malicious attack. The module provides a plaintext port to connect to a device that requires data protection (e.g. the SCADA unit, RTU, or a computer). The cryptotext port connects to a distrusted channel (e.g. a modem connected to a leased phone line or network connection device) where it can communicate with a remote module to provide a secure channel over an insecure network.

The configuration of hardware and firmware for this validation is:

Hardware: v1.0

Firmware: R101



Figure 1: Image of the Cryptographic Module

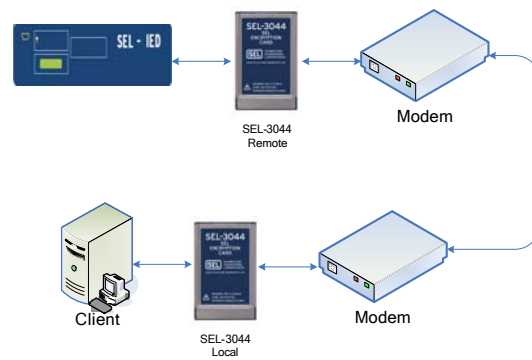


Figure 2: Point to Point Network

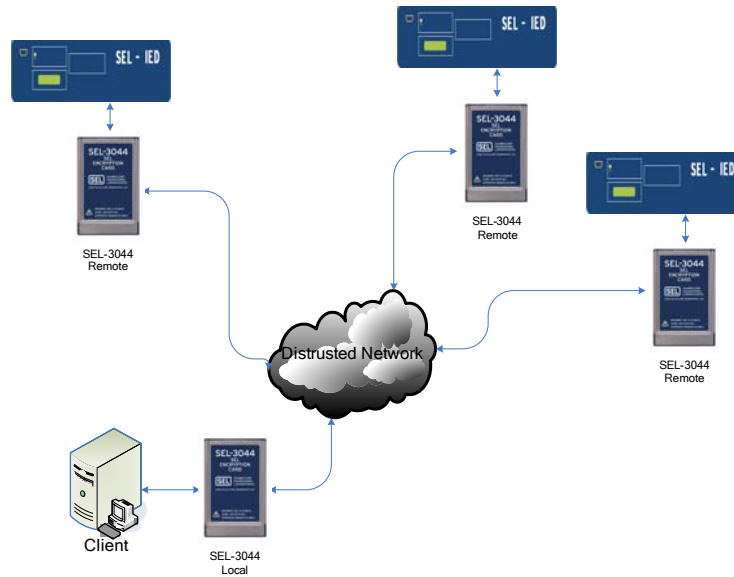


Figure 3: Point to Multipoint Network

3.1 SEP

The SEL Encryption Protocol (SEP) secures serial control system communication through the use of symmetric key cryptography. The module uses SEP to communicate with remote modules. Sessions are established with a remote module using the AES key wrap method and a static system key to transport the session keys. Under a session, frames within the network are secured by encapsulating the original message within a SEP frame. The session key of the message recipient is used to encrypt the payload using AES CTR mode. A sequence number, contained in the header, protect against message replays and create uniqueness for each frame within the session.

3.2 SEAP

The SEAP protocol secures the operator communication channel with strong message encryption and authentication. SEAP allows operators to securely log into the module to input configuration items (e.g. CSPs) and view status. Each operator has a static AES encryption key, HMAC authentication key, user name, and password. These parameters uniquely identify each operator. The encryption key provides confidentiality during the session negotiation process. The authentication key provides authentication during the session negotiation process. During the session negotiation process, the user name and password are securely provided to the module to authenticate the operator and assign appropriate access privileges. Session encryption and authentication keys are transported by the module and are used to provide confidentiality and authenticity of each frame for the remainder of the session. These keys are transported encrypted using AES CBC and the operator's AES encryption key.

3.3 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	3
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	3
Mitigation of Other Attacks	N/A

4 Modes of Operation

4.1 FIPS Approved Mode of Operation

The module only provides a FIPS Approved mode of operation, comprising all services described in this document. The module will enter FIPS Approved mode following successful power up initialization. The view status command can be used by an operator to verify that the firmware version number matches one of the FIPS approved firmware versions listed in this document. The operator may inspect the module label to verify the hardware version matches one of the FIPS approved hardware versions listed in this document.

4.2 Approved and Allowed Algorithms

The cryptographic module supports the following FIPS Approved algorithms.

Table 2: FIPS Approved Algorithms Used in Current Module

FIPS Approved Algorithm	Validation Number
AES Modes: ECB, CBC, CTR (Key Sizes: 128/256 bits)	1272
SHS Modes: SHA-1, SHA-256	1170
DSA Modes: Signature Verification (Mod 1024, SHA-1)	412
RNG Modes: FIPS 186-2 General Purpose (x-Original, SHA-1)	710
HMAC Modes: SHA1, SHA-256 (Key Sizes: KS<BS)	739

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
An NDRNG is used to generate a 512-bit seed key for input into the RNG.
AES (key transport) (Cert. #1272, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength).

The cryptographic module does not support any non-Approved algorithms.

Table 4: Non-Callable Functions Present in Current Module

FIPS Approved Algorithm	Validation Number
AES Modes: ECB, CBC, CTR (Key Sizes: 128/256 bits)	1279
SHS Modes: SHA-1, SHA-256	1171,1172
DSA Modes: Signature Verification (Mod 1024, SHA-1)	413
RNG Modes: FIPS 186-2 General Purpose (x-Original, SHA-1)	714
HMAC Modes: SHA1, SHA-256 (Key Sizes: KS<BS)	744,745

The cryptographic module performs a start-up KAT on all algorithms present on the module; both callable and non-callable.

5 Ports and Interfaces

5.1 Physical Ports

Figure 4 depicts a block diagram of the module's physical ports, with the cryptographic boundary shown in red.

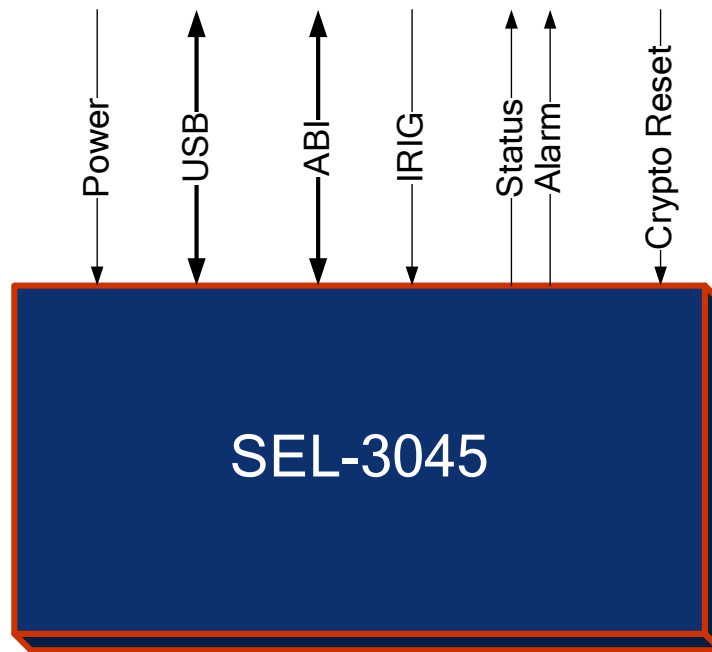


Figure 4: Module Block Diagram

Table 5: Physical Ports

Port	Description
USB	- The USB port provides a standardized device side interface for communication with host devices such as PCs. Virtual logical ports exist on this physical port to provide the services of the module. - The USB port can be used as an alternate method for supplying power to the module.
ABI	The ABI port provides a 16-bit memory mapped register interface for interfacing with other embedded host devices over their memory interface. Virtual logical ports exist on this physical port to provide the services of the module.
Power	The port is the primary power supply to the device. Alternatively the device can be powered from the USB interface.
IRIG	The IRIG port is used to receive time codes from a valid IRIG source for the purpose of synchronization with other devices and time stamping log events.
Status	The Status port indicates the health and state of the module.
Alarm	The Alarm port indicates alarm conditions due to the module entering a failed state or system events occurring during operation.
Crypto Reset	The port is used for module zeroization.

5.2 Logical Ports

Table 6: Logical Ports

Logical Interface	Description
Data Input	Data input consists of:

	- Plaintext network data entering on either the USB or ABI port. This data is processed by the SEP service and encoded into Cryptotext. - Cryptotext network data entering on either the USB or ABI port. This data is processed by the SEP service and decoded into Plaintext.
Data Output	Data output consists of: - Plaintext network data output on either the USB or ABI port. This data is generated by the SEP service from decoded Cryptotext. - Cryptotext network data output on either the USB or ABI port. This data is generated by the SEP service from encoded Plaintext.
Control Input	Control input consists of: - Cryptotext control data entering on either the USB or ABI port. This data is used to control and configure the module. - A single control input entering on the Crypto Reset port is used to zeroize all CSP and any security relevant data. - Input data entering on the ABI port is used to zeroize all CSP and any security relevant data. - Input data entering on the IRIG port is used to synchronize the clock. - Input data entering on the ABI port is used to change the clock.
Status Output	Status output consists of: - Cryptotext data exiting on either the USB or ABI port. This data is used to show status of the control and configuration the module.. - Status data exiting on the Status port. This data is used to indicate the status and health of the module. - A single status output exiting on the Alarm port. This data is used to indicate an alarm condition if the module has entered a failed state or a system event occurred during operation. - Syslog data exiting on the either USB or ABI port. This data is Syslog formatted and provides logging information of events occurring during operation. - Two status outputs exiting on the Status port allow the card to be detected by a host device.
Power Input	Power input consists of: - Power supplied on the Power port. - Power supplied on the USB port.

Module services are described in Section 7 below.

Table 7: Gemini Pins and FIPS 140-2 Ports and Interfaces

Pin	Physical Port Association	Description
GND	Ground	Ground
VCC	Power	Power (3.3 V)



D0	ABI	Data
D1	ABI	Data
D2	ABI	Data
D3	ABI	Data
D4	ABI	Data
D5	ABI	Data
D6	ABI	Data
D7	ABI	Data
D8	ABI	Data
D9	ABI	Data
D10	ABI	Data
D11	ABI	Data
D12	ABI	Data
D13	ABI	Data
D14	ABI	Data
D15	ABI	Data
A0	ABI	Address
A1	ABI	Address
A2	ABI	Address
A3	ABI	Address
A4	ABI	Address
A5	ABI	Address
A6	ABI	Address
A7	ABI	Address
A8	ABI	Address
A9	ABI	Address
A10	ABI	Address
/CS	ABI	Chip select
/OE	ABI	Output enable

/WE	ABI	Write Enable
/IRQ	ABI	Interrupt
/CRST	Crypto Reset	Zeroization
Alarm	Alarm	Alarm
VCC	Power	Power
IRIG B	IRIG	IRIG
Status	Status	Card status
CD1	Ground	Card detection
CD2	Ground	Card detection
RESET	N/A	HW reset
USB VBUS	USB / Power	Power (5 V)
USB VBUS	USB / Ground	Ground
USB D+	USB	Data
USB D-	USB	Data

6 Identification and Authentication Policy

6.1 Assumption of Roles

The module supports four distinct roles. The cryptographic module enforces the separation of roles using identity-based authentication. All operators are identified through knowledge of the appropriate key(s) and a unique operator ID.

Table 8: Roles

Role	Description
Administrator	The module supports a single Administrator role. The Administrator has the privilege to control the configuration (including key and CSP data), monitor that status, and upgrade the firmware of the module.
Cryptographic Officer	An operator assigned the role of Cryptographic Officer has the privilege to control the configuration (including key and CSP data), monitor that status, and upgrade the firmware of the module.
User	An operator assigned the role of User has the privilege to control the configuration (excluding key and CSP data), monitor that status, and upgrade the firmware of the module.
Network	A Network role is any remote module that has the privilege to encode SEP packets to this module and the ability to decode SEP packets from this module. There can be up to 1500 Network roles assigned in a module.

Table 9: Identity Authentication Mechanism

Role	Authentication Mechanism	Authentication Data	Strength of Authentication
Administrator	The authentication mechanism is an identity based authentication comprised of an encryption key, authentication key, and password. A unique name is used to distinguish this role from the other operators and is hard-configured to be 'Administrator'.	Knowledge of the administrator's encryption key (256-bit AES key), authentication key (256-bit HMAC SHA-256 key) and password (6-80 printable ASCII characters).	In order to authenticate as an operator under the Administrator role an attacker must know the values of the cryptographic security parameters (CSPs) associated with the Administrator (256 bit encryption key, the 256 bit authentication key, and the password). Assuming that all parameters are independent, and that a minimum-length, eight byte password is used, the probability that a random attempt will succeed or a false acceptance will occur is $1/(2^{256} \cdot 2^{256} \cdot 92^8)$ or $1.45 \text{ E} - 170$ which is less than one in 1,000,000. Assuming that the module can process 1 guess per second (the module has a one second lockout for incorrect attempts), the probability of successfully authenticating to the module within one minute is $1.45 \text{ E} - 170 \cdot 60$ or $8.72 \text{ E} - 169$ which is less than one in 100,000.
Cryptographic Officer	The authentication mechanism is equivalent to the Administrator's.	The authentication data is equivalent to the Administrator's.	The strength of the authentication is equivalent to the Administrator's.
User	The authentication mechanism is equivalent to the Administrator's.	The authentication data is equivalent to the Administrator's.	The strength of the authentication is equivalent to the Administrator's.
Network	The authentication mechanism is an identity based authentication comprised of an encryption key. A unique 16-bit address identifier is used to distinguish between remote modules assuming this role.	Knowledge of a unique Network Encryption Key (256-bit AES key)	An attacker must know the value of the unique Network Encryption Key. The probability that a random attempt will succeed is $1/(2^{256})$ or $8.636 \text{ E} - 78$ which is less than one in 1,000,000. The module is capable of performing approximately one authentication every .001 seconds. This results in a maximum authentication processing rate of 60000 attempts per minute. The probability of successfully authenticating to the module within

			one minute is $2.938 \text{ E-}39 * 60000$ or $5.18 \text{ E-}73$ which is less than one in 100,000.
--	--	--	--

7 Access Control Policy

7.1 Roles and Services

Table 10: Roles and Service Matrix

Service	Administrator	Cryptographic Officer	User	Network	Un-Authenticated
Create a management session for the configuration of the device and status monitoring	•	•	•		
Close a management session	•	•	•		
Change non-CSP configuration. This is any data that is not considered a CSP (e.g. event log collection configuration)	•	•			
Change current operator's log-in credentials (e.g. associated password and keys)	•	•	•		
Change CSP configuration. This is any available configuration data this is considered a CSP (keys, passwords, etc.).	•	•			
View status and event logs	•	•	•		
Clear status and event logs	•	•			
Upgrade firmware and zeroize Firmware Upgrade keys	•	•	•		
Encode plaintext messages into SEP messages				•	
Create SEP sessions				•	
Decode SEP messages into plaintext messages				•	
FIPS self-tests and diagnostics					•
View status indicators such as health and alarm output indicators.					•

Zeroize the device. This service removes all CSP data from NV memory (except the Firmware Upgrade keys) and returns the device to its factory default state.					•
Change Time					•
Output Syslog event logs					•

7.2 Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 11: CSPs

Name	Description
Administrator Encryption Key	A 256-bit AES key used during the management session creation to encrypt the session creation messages that create an operator session. This key is used to encrypt the transport of the Operator Session Encryption Key and Operator Session Authentication Key.
Administrator Authentication Key	A 256-bit HMAC (SHA-256) used during the during the management session creation to authenticate session creation messages that create an operator session.
Administrator Password	An 8 to 80 character password used during the during the management session creation to authenticate the operator.
Operator[s] Encryption Key	Equivalent to the Administrator Encryption Key. This key is used to authenticate an operator assuming the role of a Cryptographic Officer or User and protect the transport of the session keys. There can be up to 32 operators.
Operator[s] Authentication Key	Equivalent to the Administrator Authentication Key. This key is used to authenticate an operator assuming the role of a Cryptographic Officer or User. There can be up to 32 operators.
Operator Password[s]	Equivalent to the Administrator Password. This key is used to authenticate an operator assuming the role of a Cryptographic Officer or User. There can be up to 32 operators.
Operator Session Encryption Key	A 256-bit AES key generated during the management session creation and used to encrypt all frames travelling to and from the management interface data during a management session.
Operator Session Authentication Key	A 256-bit authentication key generated during the management session creation and used to authenticate all frames travelling to and from the management interface data during a management session.
DRNG State	A 512-bit state maintained by the FIPS 186-2 DRNG.
DRNG Seed Key	A 512-bit key used to seed the FIPS 186-2 DRNG.
FW Upgrade Encryption Key	A 256-bit AES key used to decrypt received FW upgrades.
Remote Network Device System Key[s]	A 256-bit AES key used during the SEP key exchange handshake to establish a SEP session with a remote device. This key is used with the AES key wrap algorithm to wrap the Remote Network Device Session Encryption and Decryption Key. There can be up to 1500 remote devices (and consequently up to 1500 keys).
Remote Network Device Session Encryption Key[s]	A 256-bit AES key used to encode the data sent under a SEP session to a remote device. There can be up to 1500 remote devices (and consequently up to 1500 keys).

Remote Network Device Session Decryption Key[s]	A 256-bit AES key used to decode the data received under a SEP session from a remote device. There can be up to 1500 remote devices (and consequently up to 1500 keys).
---	---

7.3 Definition of Public Keys

The module contains the following public keys:

Table 12: Public Keys

Name	Description
FW Upgrade Authentication Key	1024-bit DSA key used to verify a received firmware image was signed by an authenticated source.

7.4 Definition of CSPs Modes of Access

The below table defines the relationship between access to CSPs and the different module services and roles. 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 13: CSP Access Rights within Roles & Services

Name	Access Control	Service
Administrator Encryption Key	R	Create a management session
	W	Change CSP configuration
	Z	Zeroize
Administrator Authentication Key	R	Create a management session
	W	Change CSP configuration
	Z	Zeroize
Administrator Password	R	Create management session
	W	Change CSP configuration
	Z	Zeroize
Operator Encryption Key[s]	R	Create a management session
	W	Change CSP configuration
	Z	Zeroize
Operator Authentication Key[s]	R	Create a management session
	W	Change CSP configuration

	Z	Zeroize
Operator Password[s]	R	Create a management session
	W	Change CSP configuration
	Z	Zeroize
Operator Session Encryption Key	G	Create a management session
	R	Change non-CSP configuration
		View non CSP configuration
		Change CSP configuration
		View status and event logs
		Clear status and event logs
		Upgrade firmware
	Z	Zeroize
Operator Session Authentication Key		Close management session
	G	Create a management session
	R	Change non-CSP configuration
		View non CSP configuration
		Change CSP configuration
		View status and event logs
		Clear status and event logs
		Upgrade firmware
DRNG State	Z	Zeroize
		Close management session
DRNG Seed Key	G	N/A
	Z	N/A
FW Upgrade Encryption Key	G	N/A
	Z	N/A
FW Upgrade Encryption Key	R	Upgrade firmware
	W	Upgrade firmware
	Z	Upgrade firmware
Remote Network Device System Key[s]	W	Change CSP configuration
	R	Create SEP session
	Z	Zeroize
Remote Network Device Session Encryption Key[s]	G	Create SEP session
	R	Encode plaintext messages

	Z	Zeroize
Remote Network Device Session Decryption Key[s]	G	Create SEP session
	R	Decode SEP messages
	Z	Zeroize
FW Upgrade Authentication Key	R	Upgrade firmware
	W	Upgrade firmware
	Z	Upgrade firmware

8 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because SEL-3044 does not contain a modifiable operational environment.

9 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.

1. The cryptographic module shall provide four distinct operator roles. These are the Administrator, User, and the Cryptographic Officer, and Network roles.
2. The cryptographic module shall provide identity-based authentication.
3. The cryptographic module shall clear previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall perform the following tests
 - A. Power up Self-Tests
 1. Failure of any of the self tests listed here will cause the module to enter a failed state where it will be unresponsive and cease all cryptographic functions.
 2. The operator shall be capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
 3. Cryptographic algorithm tests
 - a. DSA Verify Known Answer Test
 - b. SHA-1 Known Answer Test
 - c. SHA-256 Known Answer Test
 - d. HMAC-SHA-1 Known Answer Test
 - e. HMAC-SHA-256 Known Answer Test
 - f. RNG Known Answer Test
 - g. AES Encrypt and Decrypt Known Answer Test
 4. Firmware Integrity Test
 - a. A 32-bit CRC is calculated over the program image. If the calculated CRC value does not match the value in NV memory, the module declares a failure and disables itself.
 - B. Critical Functions Tests

1. Failure of any of the critical tests listed here will cause the module to enter a failed state where it will be unresponsive and cease all cryptographic functions.
2. Runtime volatile memory tests
 - a. Read and write tests are performed on the memory. This continuously checks the memory address space during runtime. If an error is detected, the device declares a failure and disables itself.
3. Settings integrity test
 - a. A 32-bit CRC is calculated over the settings image. If the calculated CRC value does not match the value in NV memory, the device declares a failure and disables itself.

C. Conditional Self-Tests

1. Continuous Random Number Generator Tests
 - a. One test compares the last 32 bit NDRNG output with the current 32 bit NDRNG output. If the two values are equal the module declares a failure and disables itself.
 - b. A second test compares the last 512 bit RNG output with the current 512 bit RNG output. If the two values are equal the module declares a failure and disables itself.
 2. Firmware Load Test
 - a. The device will reject the potential firmware if the firmware load test fails.
 - b. The module verifies a DSA digital signature when loading firmware.
6. Power-up self tests do not require any operator action.
 7. Data output shall be inhibited during key generation, 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. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
 10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
 11. The module does not support concurrent operators.
 12. The module does not support a maintenance interface or role.
 13. The module does not support manual key entry.
 14. The module does not have any external input/output devices used for entry/output of data.
 15. The module shall not support a bypass capability.
 16. The module does not enter or output plaintext CSPs.
 17. The module does not output intermediate key values.

10 Physical Security Policy

10.1 Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components



- Hard potting material encapsulation of multiple chip circuitry enclosure with removal and/or penetration attempts causing serious damage
- Hard metallic composite enclosure comprises the cryptographic boundary

10.2 Operator Required Actions

The operator is required to periodically inspect the enclosure for tamper evidence.

The operator is required to verify that the module was delivered in a secure manner using the following steps:

1. Inspect to make sure the shipment packaging and seals have not been broken.
2. Inspect to make sure the tamper-evident case of the module has not been broken.
3. Inspect to make sure the module on first power up is in the default state.

11 Mitigation of Other Attacks Policy

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