Non-Proprietary Security Policy for the FIPS 140-2 Level 1 Validated Fortress Secure Client Bridge (SCB)

Hardware Version 1.0

Firmware Version 2.1.1

(Document Version 1.03)

December 2007

Prepared by the Fortress Technologies, Inc.,
Government Technology Group
4023 Tampa Rd. Suite 2000. Oldsmar, FL 34677

Contents

List of Figures

List of Tables

1.0 INTRODUCTION

The AirFortress® Secure Client Bridge Cryptographic Module Version 2.1, Figure 1 and Figure 2, hereafter SCB, is a standalone hardware and firmware cryptographic module and security client designed to prevent a hacker from "sniffing" and reading data transferred across a wired or wireless network. This security appliance provides a secure link to the corporate network by protecting communications between attached devices and the rest of the network. The SCB accepts traffic from IP or serial connections and creates a secure connection on their behalf to an AirFortress® Gateway as shown in Figure 3. Because the SCB implements encryption at the Media Access Control (MAC) layer, not only does it protect important network information, it functions as a bridge so it can be quickly and transparently be integrated into an existing network. Operation is automatic, requiring no administrator intervention as it protects data transmitted on WLANs (wireless LANs) and between WLAN devices and the wired local area network.

The SCB requires no special configuration for different network applications. Its security protocols are implemented without human intervention to prevent any chance of human error. Authorized personnel (Cryptographic Officer) can log into the SCBs browser based management tool using his/her PIN/password for SCB configuring and monitoring. The length of the password is selectable 8-16 characters from keyboard using standard and special characters.

The SCB is a hardware security solution. According to FIPS 140-2 terminology, the SCB is a multi-chip standalone cryptographic module, whose cryptographic boundary is the entire enclosure of the device, including its physical ports, which constitute the module's physical boundary.

The SCB always operates in FIPS-enabled operating mode. In the FIPS mode the SCB offers point-to-point-encrypted communication for the user's computer and Local Area Network (LAN) or Wireless LAN (WLAN) it protects. It encrypts outgoing messages/data from a "client" site (unencrypted Ethernet port), and decrypts incoming messages/data from client computers located at different sites (encrypted 802.11b or Ethernet port). Two or more units can also communicate with each other directly, but an 802.11b AP is required to act as a relay if the wireless link is used for the encrypted interface. The SCB units apply FIPS-validated, symmetric-key encryption using Triple-DES, AES with 128 bits, 192 bits or 256 bits key length. All of these encryption operation modes are FIPS 140-2 validated.

The control input interface is the same as the message/data communication interface.

The SCB uses a unique 16-digit hexadecimal string that represents the client's Access ID.

At each consecutive power-on, after it is installed at a site, the SCB performs self-tests and adapts itself to the network automatically. An authorized administrator can reboot the module when needed, oversee self-tests and normal operation, and keep an eye on the physical security of the host hardware platform on which the SCB is installed.

Zeroization of all cryptographic keys and CSPs can be manually processed by rebooting the SCB.

Figure 1: The Secure Client Bridge

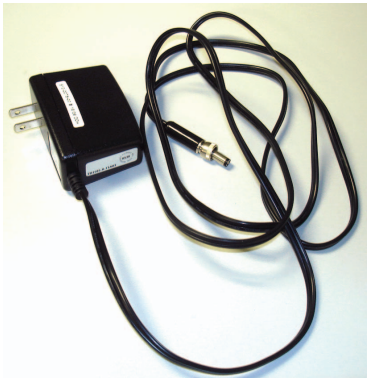

Figure 2: Power Module Secure Client Bridge

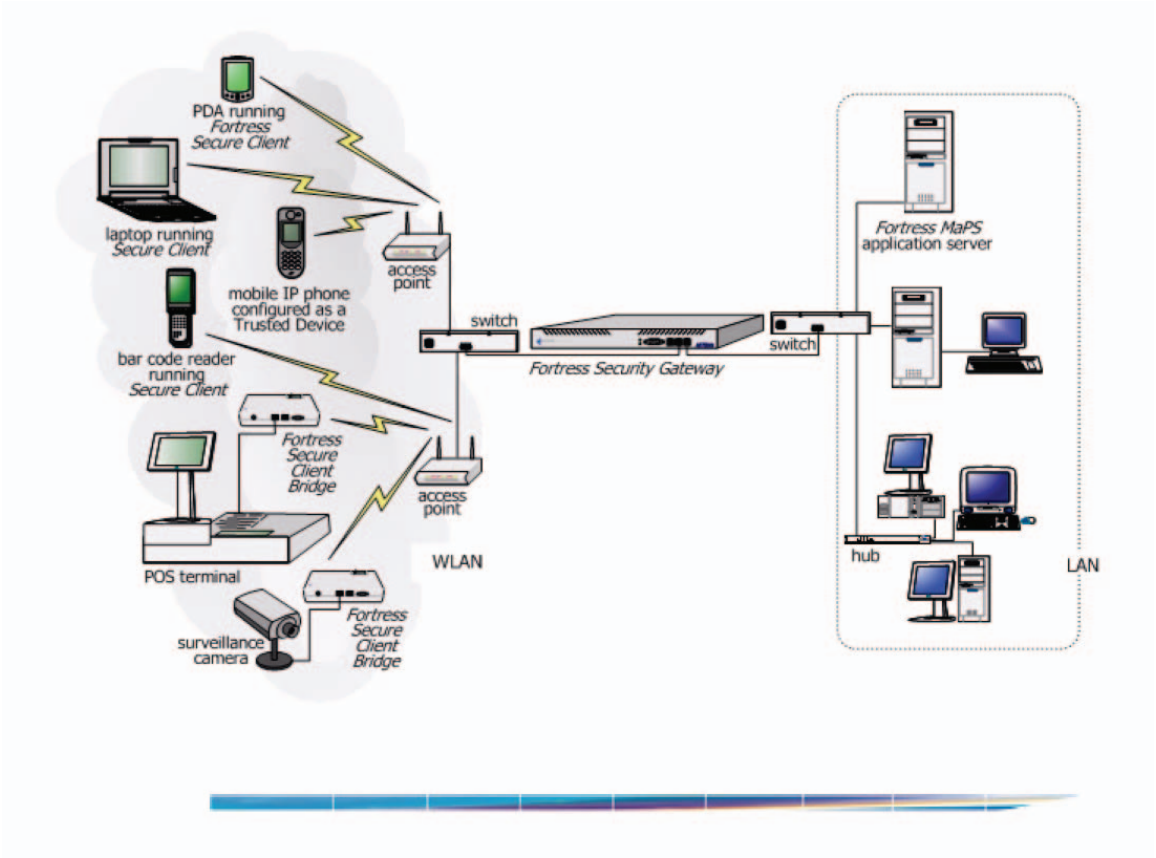

Figure 3: Example of Secure Client Bridge Application

2.0 SCB SECURITY FEATURES

The SCB provides data link layer (OSI Layer 2) security. To accomplish this, it was designed with the features described in the following sections.

2.1 Cryptographic Module

The following security design concepts guide the development of the SCB:

1. Use FIPS-approved and NIST recommended cryptographic algorithms, such as, Triple-DES and AES.
2. Minimize the human intervention to the module with a high degree of automation to prevent human error and to ease the use and management of the module.
3. Secure all points where a LAN, WLAN, or WAN can be accessed by using a unique company Access ID, defined by the customer, to identify authorized devices as belonging to the protected wireless network

The Mobile Security Protocol (MSP) architecture of the cryptographic engine ensures that cryptographic processing is secure on a wireless network and automates most security operations to prevent any chance of human error. Because MSP operates at the data link layer, header information is less likely to be intercepted In addition to using FIPS-approved and NIST recommended cryptographic algorithms, MSP also compresses data, disguising the length of the data to prevent analytical attacks and yielding a significant performance gain on network throughput.

The SCB requires no special configuration to operate once correctly installed. Cryptographic Officers are encouraged to change certain security settings, such as the Access ID for the device, to ensure that each customer has unique parameters that must be met for access. The SCB allows role-based access to user interfaces for access to the appropriate set of management and status monitoring tools.

2.2 Module Interfaces

Inbound and Outbound traffic enters through the Ethernet, 802.11 and serial interfaces and is passed into the "AFClient daemon". The driver includes the packet capture module. The "AFClient daemon" includes the "wLLS Module" (provides the module cryptographic services). "AFWeb" is used to configure the SCB.

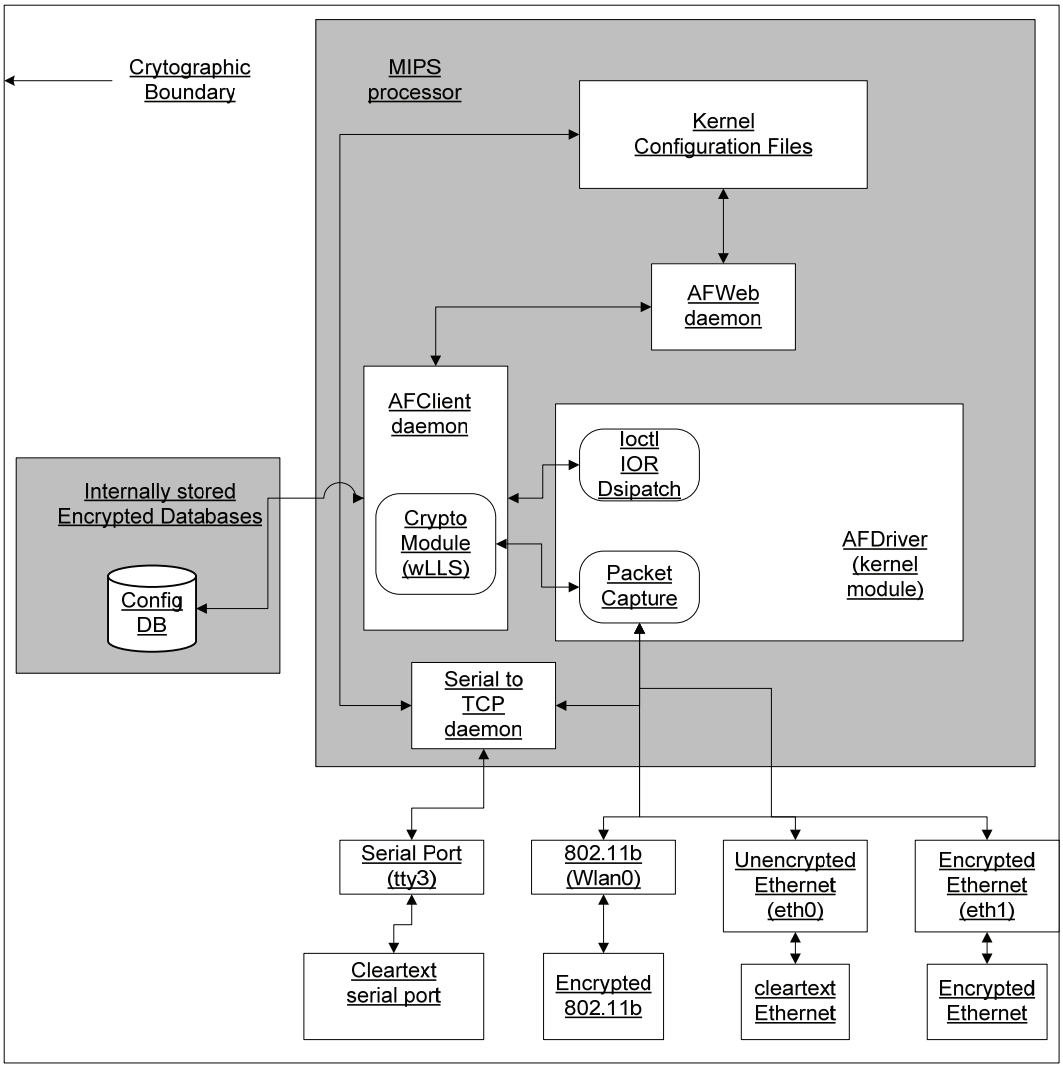

Figure 4: Fortress Secure Client Bridge (SCB) Information Flow Diagram

The encryption state of the data that flows though the SCB's ports are characterized in the table 1.

Table 1: Encryption State of Data Flow

Port Name	Traffic Type	Direction	Encrypted/Unencrypted
Serial Port (DB-9)	RS-232 ASCII bit stream	To SCB	Unencrypted
Serial Port (DB-9)	RS-232 ASCII bit stream	From SCB	Unencrypted
802.11b Wireless	802.11b packet SDU	To SCB	*Encrypted
802.11b Wireless	802.11b packet SDU	From SCB	*Encrypted
Unencrypted Ethernet	802.3 packet SDU	To SCB	Unencrypted
Unencrypted Ethernet	802.3 packet SDU	From SCB	Unencrypted
Encrypted Ethernet	802.3 packet SDU	To SCB	*Encrypted
Encrypted Ethernet	802.3 packet SDU	From SCB	*Encrypted

*The SCB never passes any unencrypted clear text data traffic over the encrypted ports.

2.3 Secure Operation

This section describes how to place and keep the module in FIPS-approved mode of operation.

The Crypto-Officer must insure that the Diffie-Hellman key size of 512-bits is not selected. Use of Diffie-Hellman using 512-bit intermediate values is not permitted in FIPS-mode.

3.0 IDENTIFICATION AND AUTHENTICATION POLICY

3.1 Roles

The SCB supports two Cryptographic Officer roles and one Users role as shown below:

Table 2: Roles

Roles	Authentication Method	Port	Tasks
Cryptographic Officer			
Administrator	Password	GUI Data I/O	- Configuration - Diagnostics - Monitoring - Cryptographic Services
Operator	Password	GUI Data I/O	- Diagnostics - Monitoring - Cryptographic Services
Users Role			
End User	Access ID	Data/I/O	- Cryptographic Services

Note: A Maintenance role is not supported.

Table 3: Strength of Authentication Mechanisms

Authentication Mechanism	*Strength of Mechanism*
Cryptographic Officer	8-alphanumeric characters. 72^8 combinations exceeds the standard 1/10^6 success rate. The cycle time for the module to deny access and present a fresh login interface is eight seconds. The number of login attempts available in a minute is seven and a half (7.5) login attempts per minute. At this rate, the possibility of guessing the password in a one-minute interval exceeds the 1 in 10^5 requirements of the standard.
User	16-Hex Access ID (64-bit). The probability guessing the Access ID exceeds the standard 1/10^6 success rate. The module is designed to attempt eight User authentication attempts after start-up. If it fails to authenticate with the User, it enters a non-functioning idle state until a reset occurs, then another authentication attempt is made. Since the reset initialization is outside of the User's control, a User can make 8 attempts at authentication in a given one-minute interval. This leaves a probability of 8*(1/2)^64 = (2^3)/(2^64) = (1/2)^61 for a false acceptance in a one minute interval; greatly exceeding the 1 in 10^5.

Note: Level 1 cryptographic modules do not require authentication to assume a role.

3.2 Services

Table 4 defines the services, service input, and service output of the SCB. Some service like the LEDs shows a status by turning on or blinking a LED, other services shows various system status on the GUI while other perform services, like self test, encryption service or communication services, that are transparent to someone using the SCB,

Table 4: Services, Operations and Functions of the Cryptographic Module

Service	Service Input	Service Output
Show Status		
LED – Unencrypted Ethernet	Operation of the Unencrypted Ethernet	Light
LED – Encrypted Ethernet	Operation of the Encrypted Ethernet	Light
LED – Serial Port	Operation of the Serial Port	Light
LED – Wireless NIC	Operation of the Wireless NIC	Light
LED – SCB Status	Various Condition within the SCB	Light
LED – Power Indicator	Power is On	Light
GUI – System Status	Values taken from different places in the SCB	Values
GUI – Version Information	Hard Coded Information within the flash	Values
GUI – Tracking	Status of the partners	Values
GUI – Interface Information	Taking from the interface drivers	Values
GUI – System Log	Various conditional within the SCB with generate a message	Log Messages
Perform Self Test		
Cryptographic Algorithm Tests	Crypto Algorithm	Self-tests passed message sent to log.
Firmware Integrity Check	Operating Application	Firmware integrity test passed message sent to log
SHA-1 and HMAC Test	SHA-1 and HMAC Routines	Self-tests passed message sent to log.
Firmware Load Test	Installation Firmware	Firmware load passed message sent to log.
Continuous Rand Number Generator Test	X9.31 PRNG	RNG test passed message sent to log.
Security Services		
Encrypt AES	• Packets coming from an unencrypted interface or from the GUI to be encrypted • Packet coming from an encrypted interface to be unencrypted	• Packets coming from an unencrypted interface or from the GUI to be encrypted • Packet coming from an encrypted interface to be unencrypted
Encrypt Triple-DES	• Packets coming from an unencrypted interface or from the GUI to be encrypted • Packet coming from an encrypted interface to be unencrypted	• Packets coming from an unencrypted interface or from the GUI to be encrypted • Packet coming from an encrypted interface to be unencrypted
Diffie-Hellman Key Agreement (1024-bits or 2048-bits)	Random Number	Encryption Key
SHA-1	Packet	Hash
PRNG	Seed Value	Pseudo Random Number
Non-Approved Security Functions		
Diffie-Hellman Key Agreement (512 bits)	Random Number	Encryption Key

Service	Service Input	Service Output
SSL-Only uses SHTTP	• Unencrypted packets from to GUI • Encrypted Packets coming from a browser on a remote workstation	• Encrypted packets going to a browser on a remote workstation • Unencrypted packets going to GUI
Communication Services		
Bridging	Input Packet	Output Packet
WLAN Configuration	GUI Input by Admin	Feature Configured
Ethernet Configuration	GUI Input by Admin	Feature Configured
Serial Configuration	GUI Input by Admin	Feature Configured
WLAN Communication	Input Packet	Output Packet
Ethernet Communication	Input Packet	Output Packet
Serial Communications	Input Packet	Output Packet
Reset Connections	GUI Input by Admin	Connections Reset
DHCP Usage	DHCP Request Packet	DHCP Response Packet
DHCP Configuration	GUI Input by Admin	Feature Configured
Release DHCP Connection	GUI Input by Admin	DHCP Connection Released
Ping	GUI Input by Admin or Operator	Ping Packet Sent
Traceroute	GUI Input by Admin or Operator	Traceroute Packet Sent

4.0 ACCESS CONTROL POLICY

Table 5 shows the access control policy concerning each service of the SCB. Some services everyone (User, Operator and Administrator) can access while other service only certain roles can access.

Table 5: Access Control Table

Service	CSP Access	Roles
Show Status		
LED – Unencrypted Ethernet	None	All
LED – Encrypted Ethernet	None	All
LED – Serial Port	None	All
LED – Wireless NIC	None	All
LED – SCB Status	None	All
LED – Power Indicator	None	All
GUI – System Status	None	Administrator Operator
GUI – Version Information	None	Administrator Operator
GUI – Tracking	None	Administrator Operator
GUI – Interface Information	None	Administrator Operator
GUI – System Log	None	Administrator Operator
Perform Self Test Services		
Crypto Algorithm Tests	None	All
Firmware Integrity Test	None	All
SHA1 and HMAC Test	None	All
Firmware Load Test	None	All
Continuous Rand Number Generator Test	None	All
Security Services		
Enter Access ID	Read and Write	Administrator
Encrypt AES	Execute	All
Encrypt Triple-DES	Execute	All
Diffie-Hellman Key Agreement	Execute	All
SHA -1	Execute	All
HMAC SHA-1	Execute	All
SHA-256	Execute	All
HMAC SHA-256	Execute	All
PRNG	Execute	All
SSL-Only uses SHTTP.	None	Administrator Operator
Configure Remote Administration	None	Administrator
Configure Peer to Peer Communication	None	Administrator
Configure DMZ	None	Administrator
Configure Peer to Peer Communication	None	Administrator
Configure DMZ	None	Administrator
Change Passwords	None	Administrator
Configure Remote Administration	None	Administrator
System Settings		
Reboot SCB	None	Administrator
Restore SCB Settings	Read and Write	Administrator
Backup SCB Settings	Read Only	Administrator
Firmware Load	None	Administrator
Communication Services		

Service	CSP Access	Roles
Bridging	None	All
WLAN Configuration	None	Administrator
Ethernet Configuration	None	Administrator
Serial Configuration	None	Administrator
WLAN Communication	None	All
Ethernet Communication	None	All
Serial Communications	None	All
Reset Connections	None	Administrator Operator
DHCP Client Usage	None	All
DHCP Server Configuration	None	Administrator
Release DHCP Connection	None	Administrator
Ping	None	Administrator Operator
Traceroute	None	Administrator Operator

5.0 CRYPTOGRAPHIC KEY MANAGEMENT

The SCB automatically performs all cryptographic processing and key management functions.

General Cryptographic Information

Encryption Algorithms

- Triple-DES
- AES (128-bits, 192-bits, 256-bits)

Random Number Generators

- X9.31 Pseudo Random Number Generator

Hash Algorithms

- SHS (SHA-1, SHA-256)

HMAC

- HMAC (SHA-1)
- HMAC (SHA-256)

Key Exchange

- The SCB uses Diffie-Hellman Key exchange.
- If the SCB is running multiple Diffie-Hellman keys simultaneously:
    - The SCB will send broadcast keys using the smallest configured Diffie-Hellman key.
    - Devices exchanging keys will negotiate to select the largest common Diffie-Hellman key length.
    - The SCB will track the last used Diffie-Hellman key length of each partner and use the appropriate public key.
    - Clients will monitor the public keys passed down and only compute common keys with the compatible Diffie-Hellman public keys.
    - If two devices are using incompatible Diffie-Hellman key lengths, (e.g., Client A is using Diffie-Hellman-1024, SCB is using Diffie-Hellman-2048) then that partner should be placed in a ‘block state’ until a compatible Diffie-Hellman key is detected.

Cryptographic Keys
The following keys are employed by the module.

Table 6: Key Table

Key	*Key Type*	*Key Length*
Module Secret Key (MSK)	AES	128-bits, 192-bits, or 256-bits
	Triple-DES	168-bits
Static Private Key	Diffie-Hellman intermediate value	1024-bits, or 2048-bits
Static Public Key	Diffie-Hellman intermediate value	1024-bits, or 2048-bits
Static Secret Encryption Key	AES	128-bits, 192-bits, or 256-bits
	Triple-DES	168-bits
Dynamic Private Key	Diffie-Hellman intermediate value	1024-bits, or 2048-bits
Dynamic Public Key	Diffie-Hellman intermediate value	1024-bits, or 2048-bits
Dynamic Session Key	AES	128-bits, 192-bits, or 256-bits
	Triple-DES	168-bits
Static Group Key	AES	128-bits, 192-bits, or 256-bits
	Triple-DES	168-bits
Public Dynamic Group Key	Diffie-Hellman intermediate value	1024-bits
Private Dynamic Group Key	Diffie-Hellman intermediate value	1024-bits
Dynamic Group Key	AES	128-bits, 192-bits, or 256-bits
	Triple-DES	168-bits

5.2 Key Storage

No encryption keys are stored permanently in the module.

5.3 Zeroization of Keys

The session keys of the SCP are automatically zeroized when the system is turned off and regenerated at every boot-up of the host hardware.

5.4 Key Agreement

The SCP supports the Diffie-Hellman key agreement protocol using a Diffie-Hellman key size of 512-bits*, 1024-bits, or 2048-bits.

* Does not provide sufficient encryption strength and is not to be used in FIPS-mode

5.5 Cryptographic Algorithms

The SCB uses the FIPS approved cryptographic algorithms as shown in Table 7

Table 7: Approved Functions

Functions	CAVP Certificate #
Triple-DES (CBC (K1, K2, K3))	#541
AES (CBC, encrypt/decrypt; 128-bit, 192-bit, 256-bit)	#545
SHS (SHA-1, SHA-256 (Byte))	#609
PRNG (ANSI X9.31)	#312
HMAC (SHA-1, SHA-256)	#286

Table 8: Non-Approved Functions

Non-Approved Functions Allowed in FIPS-Mode
Diffie-Hellman (key agreement; key establishment provides 80 (1024-bit intermediate values) and 112 bits (2048-bit intermediate values) of encryption strength)
Non-Approved Functions Not Allowed in FIPS-Mode
Diffie-Hellman (key agreement; key establishment methodology provides 56 bits of encryption strength, 56 bit mode does not provide sufficient encryption strength), DSA (non-compliant), RSA (non-compliant), MD2, MD5, Blowfish, CAST, IDEA, RC2, RC4, RC5

5.6 Self Tests

The module conducts the following self-tests at power-up and conditionally as needed, when a module performs a particular function or operation:

A. Power-Up Tests

- Cryptographic Algorithm Known Answer Tests: AES KAT, Triple-DES KAT, HMAC-SHA-1 KAT, HMAC-SHA-256 KAT, SHA-1 KAT, and SHA-256 KAT, PRNG KAT
- Firmware Integrity Test: HMAC (SHA-256)

B. Conditional Test

- Continuous Random Number Generator test
- Firmware Load Test: HMAC (SHA-1)

Failure of any self-test listed above puts the module in its error state.

6.0 PHYSICAL SECURITY POLICY

The SCB was designed to use production quality components, and is contained in a hard plastic enclosure. The module meets the requirements for level 1 physical security.

7.0 FIRMWARE SECURITY

The SCB executes in a non-modifiable operating environment

8.0 OPERATING SYSTEM

The SCB uses the Fortress Proprietary operating system.

9.0 MITIGATION OF OTHER ATTACKS POLICY

No special mechanisms are built in the SCB; however, the cryptographic module is designed to mitigate several specific attacks. Features, which mitigate attacks, are listed here:

1. Use of a network-specific *access ID* assures that only SCB units using this same unique value can establish key exchange: *Mitigates unauthorized connections to the module.*
2. The SCB uses FIPS-approved SHS and HMAC hashing and FIPS-approved encryption/decryption methods: Triple-DES *Mitigates attacks to decrypt traffic and crack keys*.
3. The SCB enforces strong authentication of communicating parties: *Mitigates "spoofing" credentials*.
4. The SCB applies strong authentication on the origin of packets: *Mitigates packet modification.*
5. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
6. A second Diffie-Hellman key exchange produces a dynamic common secret key in each of the modules by combining the other module's dynamic public key with the module's own dynamic private key: *Mitigates "man-in-the-middle" attacks*.
7. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
8. Data in transit is subjected to integrity checking: *Mitigates data modification and active attacks to inject traffic.*
9. Compression and encryption of header information inside of the frame, making it impossible to guess. Use of strong encryption further protects the information. Any bit flipping would be useless in this frame to try to change the IP address of the frame: *Mitigates active attacks from both ends*.
10. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
11. No encryption keys are stored permanently in the module: *Mitigates key discovery.*
12. All firmware data are stored in executable format in the module: *Mitigates access to the module firmware.*
13. When the SCB is operated in accordance to the vendor's physical security policy, the host server hardware platform is located in a controlled-access area or under permanent control of the user: *Mitigates access to the module hardware.*

10.0 EMI/EMC

The SCB meets the requirements for FCC CFR 47 Part 15. Subpart B, Class A (Business use)

11.0 CUSTOMER SECURITY POLICY ISSUES

Fortress Technologies, Inc. expects that after the module's installation, any. *customer* (government organization or commercial entity or division) *employs its own internal security policy* covering all the rules under which the module(s) and the customer's network(s) must operate. In addition, the customer systems are expected to be upgraded as needed to contain appropriate security tools to enforce the internal security policy.

12.0 MAINTENANCE ISSUES

All installation and reinstallation for modules is performed by the Cryptographic Officer following the procedures defined by Fortress Technologies. Troubleshooting to resolve an error state may require the product to be reinstalled by the Cryptographic Officer or to be sent back to Fortress Technologies.

- * - * -

End of the "Non-Proprietary Security Policy for the FIPS 140-2 Validated Secure Client Bridge" document.