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

Software Versions 3.1 and 3.1.1

(Document Version 1.02)

March 2008

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

This security policy defines all security rules under which the Fortress Secure Client (Client) must operate and enforce, including rules from relevant standards such as FIPS 140-2. The Client complies with all FIPS 140-2 level 1 requirements.

The Client is a *cryptographic software application* that operates as a multi-chip standalone cryptographic module. The cryptographic boundary of the module is the compiled application executable. The physical boundary is the hardware platform, such as a typical PC or a PDA, on which the Client is installed. The Client identifies network devices and encrypts and decrypts traffic transmitted to and from those devices.

The Client software and computer hardware combination operates as an *electronic encryption application* designed to prevent unauthorized access to data transferred across a wireless network. The Client encrypts and decrypts traffic transmitted on that network, protecting the user of the application on the hardware platform. Only authorized personnel, such as the administrator (cryptographic officer), can log into the module to configure profiles.

The Client operates at the datalink layer of the OSI model and is installed as an application and an intermediate driver. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

The Client is designed to operate on the following operating systems and hardware platforms:

- Windows 2000 Professional, SP4 on an Intel/AMD Processor
- Windows XP Professional, SP2 on an Intel/AMD Processor
- Windows 2003 Server, SP2 on an Intel/AMD Processor
- Windows CE V3.0 on an ARM Processor
- Windows CE V4.0 on an ARM Processor
- Windows CE V5.0 on an ARM Processor

The cryptographic officer role manages the cryptographic configuration of the Client. This role can configure user profiles. Both Cryptographic Officers and User can review module status and change profiles where appropriate.
The cryptographic setting can only be configured within profiles and only by the cryptographic officer when the modules are operating in FIPS mode. Because the Client automates cryptographic processing, end users do not have to actively initiate cryptographic processing; the Client encrypts and decrypts data sent or received by users operating authenticated devices connected to the Client.

The Client offers point-to-point-encrypted communication between protected devices. Two or more Clients can communicate with each other directly or a Client can communicate to devices protected by a Fortress Wireless Security Gateway. The product encrypts outgoing data from a client device and decrypts incoming data from networked computers located at different sites.

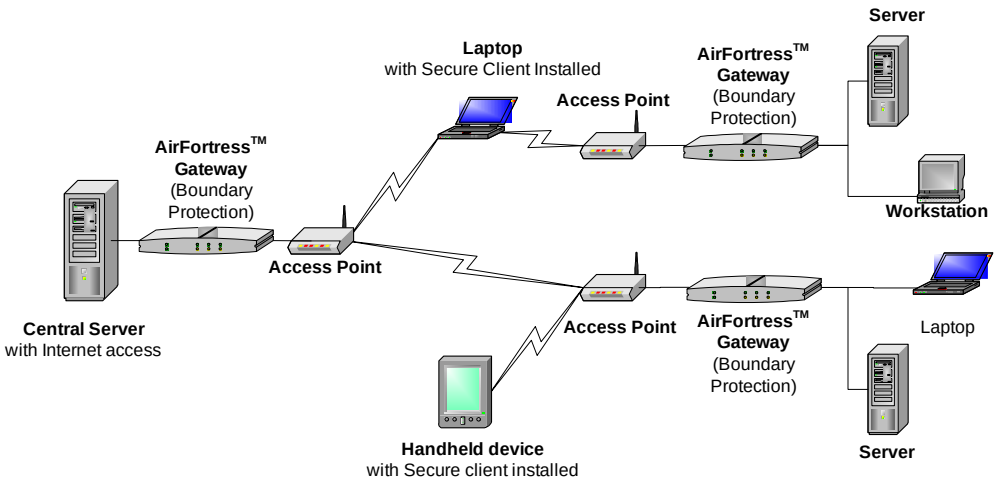

Figure 1: Example Configuration of Fortress Secure Client Deployment

2.0 CLIENT SECURITY FEATURES

The Client provides true datalink layer (OSI Layer 2) security. To accomplish this, it was designed with the minimum-security features described in the following sections.

2.1 Cryptographic Module

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

1. Use strong, proven encryption solutions such as Triple DES (TDES), and AES.
2. Protect data at or below the level of vulnerability, by protecting a packet starting at the datalink level, meaning not just the customer's data, but also the IP network layer is protected.
3. Minimize the human intervention to the module operation with a high degree of automation to prevent human error and to ease the use and management of a security solution.
4. 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 Wireless Link Layer Security™ (wLLS) 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 wLLS operates at the datalink layer, header information is less likely to be intercepted. In addition to applying standard strong encryption algorithms, wLLS also compresses data, disguising the length of the data to prevent analytical attacks and yielding a significant performance gain on network throughput.

The Client requires no special configuration to operate once correctly installed by the cryptographic officer, although 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 Client allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools.

2.2 Module Interfaces

The Client provides logical interfaces for input and output; it does not support separate ports for cryptographic key management or data authentication. Inbound and outbound traffic is received through the communication port of the hardware device on which the Client is installed. The information is processed by the Microsoft® NDIS Intermediate protocol and then to the packet capture component, which identifies packets as incoming or outgoing and encrypts or decrypts the packets accordingly. This NDIS interface interacts with third-party applications installed on the computer that receives packets and with the device communication port (NIC, RJ-45 port, serial port, or other option).

Data sent and received through the NDIS interface to a connected access point are always encrypted; the Client does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 2 shows this information flow in relation to a standard set of computer components that will be present on any platform on which the Client is installed.

The module has one logical interface for information flow, which handles all communication into and out of the module. When in FIPS Mode data is transmitted to the network as ciphertext unless a trusted device is configured. The Client does not require physically separate entry and exit ports. The device communications port serves as both a data entry and exit port for secured network communications, as the data streams are bi-directional and conform to the real-time information exchange over the network.

2.3 FIPS Mode

The approved mode of operation (FIPS mode) is enabled during installation of the Secure Client on a workstation, laptop or handheld. The FIPS Mode is only activated if a Profile is used that has the following:

- Encryption Enabled
- AES or Triple-DES Selected
- A Diffie-Hellman key of 1024 or greater
- No Trusted Devices configured
- 802.1x traffic set to none

Refer to the User Guide [1] for installation procedures. Each Client can be configured to accept and send packets as ciphertext or cleartext, but as stated above, to be in FIPS approved mode, the client must be configured to send packets in ciphertext. Only a connection using ciphertext can the client communicate with other secured Fortress modules.

The Client is a software application designed to be installed on a range of hardware devices that access a secured LAN or WLAN. According to FIPS 140-2 terminology, the Client is a multi-chip standalone cryptographic module, whose cryptographic boundary is the self-contained compiled executable.

The Client offers point-to-point-encrypted communication for the wireless electronic device it protects. It encrypts outgoing messages (data) from the device to the wired network where a Fortress Wireless Security Gateway is installed and decrypts incoming messages (data) to the host device from other devices within the Fortress Gateway-protected network. Two devices with Client installed and configured appropriately can also communicate with each other directly.

The Client units designed for government use apply FIPS-approved encryption algorithms, Triple Data Encryption Standard and Advanced Encryption Standard. These algorithms operate on text blocks of 64 bits and 128 bits, respectively, to encrypt and decrypt plaintext into ciphertext and ciphertext into plaintext.

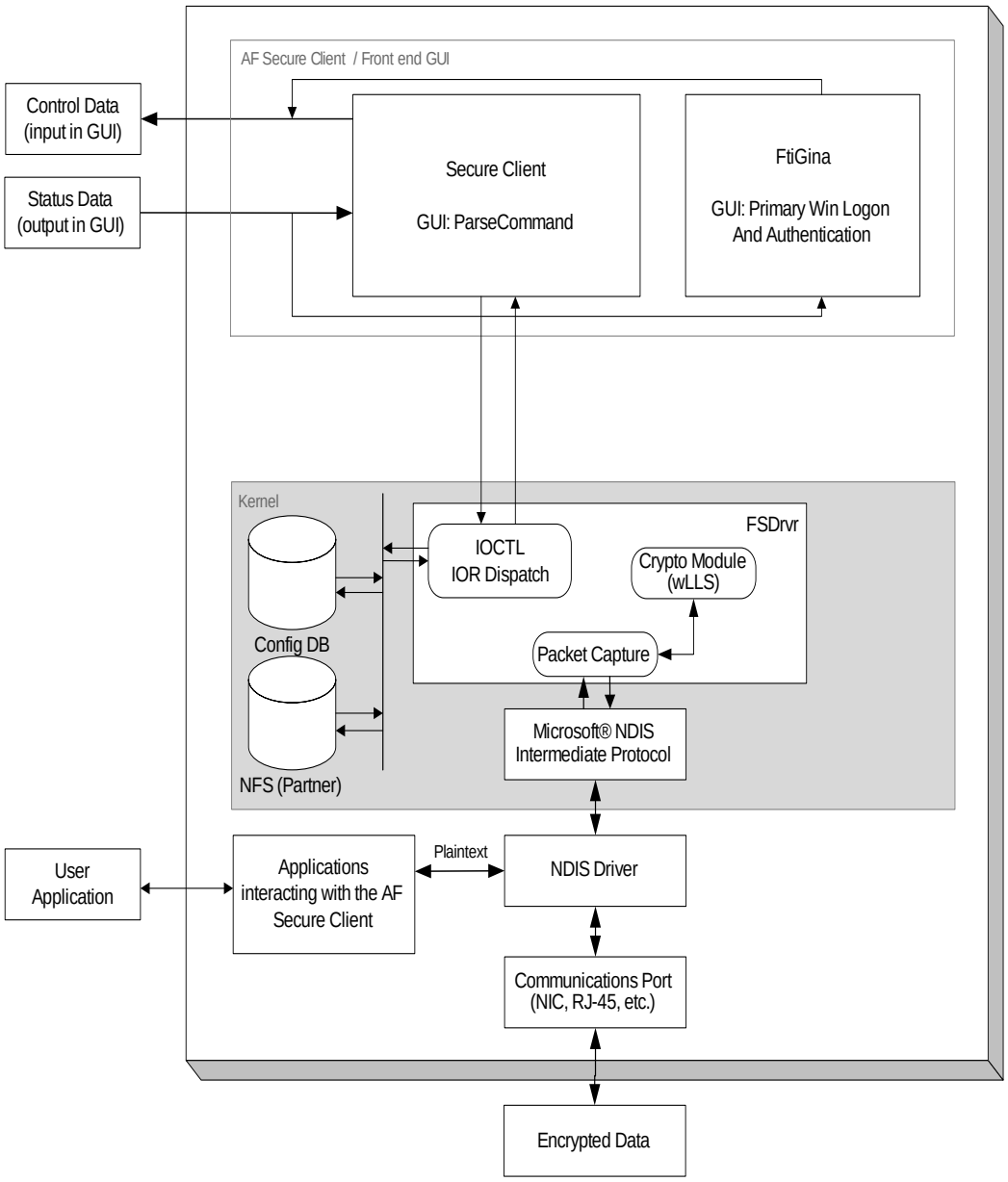

Figure 2: Information Flow Through the Client

3.0 IDENTIFICATION AND AUTHENTICATION POLICY

3.1 Roles

The Client supports two roles, the user role and the cryptographic officer role. Role based authentication of the cryptographic officer is supported.

3.1.1 The User

The user role is the default, unauthenticated role of the module. It can monitor system status and perform the following tasks:

- Use Profile
- Set Default Profile
- View Statistics
- Enable Auth Prompt
- Restart Sessions
- Partner Tracking
- Restart the Client
- AES/Triple DES Encryption
- Self Test

3.1.2 The Administrator - Cryptographic Officer

The Cryptographic Officer role requires a password of 8-16 characters for authentication. The password can contain upper and lowercase letters, special characters, numbers, and spaces, for a total of 64 possible characters. Therefore the odds of a random attempt of guessing the password succeeding are 1 in 64^8. As the module takes 8 seconds to process an incorrect password entry, there could be up to 7.5 authentication attempts within one minute. Therefore, the probability of a random attempt succeeding within one minute is 7.5 in 64^8. The role is assumed to perform a set of cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions). The cryptographic officer performs the following tasks in particular:

- Install the Client
- Configure, Edit and Delete Profiles
  - Name Profile
  - Select Binding
  - Enable or Disable Encryption
  - Select the type of encryption
  - Select the Diffie-Hellman Key Size

  - Configure Access IP
  - Configure Trusted Devices
  - Allow 802.1x Traffic
  - Enable and Configure Submit roaming
- Use Profile
- Set Default Profile
- Enable Auth Prompt
- Restart Sessions
- Partner Tracking
- Restart the Client
- AES Encryption
- Change Administration Password
- Self Test

3.2 Services

Table 1: Services

Services For the User	Role Required To use Service	Service Input	Service Output	Security Relevant Data
Use Profile	User Crypto Officer	Select on GUI	Activate Profile	none
Set Default Profile	User Crypto Officer	Select on GUI	Sets Default Profile	none
Edit Profile	Crypto Officer	Password Configuration	Changed Profile	AES 128, 192, 256, Triple DES 2 key
Add Profile	Crypto Officer	Password Configuration	Creates new Profile	AES 128, 192, 256, Triple DES 2 key
Delete Profile	Crypto Officer	Password	Deletes Profile	none
Administration Password	Crypto Officer	Old Password New Password	New Password set	crypto officer password
System Settings	Crypto Officer	Password	Activates New System Settings	crypto officer password
Enable Auth Prompts	User Crypto Officer	GUI Selection	Enables Auth Prompts	none

Restart Sessions	User Crypto Officer	GUI Selection	Restarts and Reset Session	none
View Partner Tracking	User Crypto Officer	GUI Selection	Shows Partners Information	none
Triple DES Encryption (2 key)	User Crypto Officer			Triple DES-CBC
AES Encryption (128 bits)	User Crypto Officer			AES-CBC
AES Encryption (192 bits)	User Crypto Officer			AES-CBC
AES Encryption (256 bits)	User Crypto Officer			AES-CBC
Self Test	User Crypto Officer	Power Up Reset	Log Message	Crypto Algorithm Tests SHA1 Hash and HMAC Test SHA256 Hash and HMAC Test X9.31 Known Answer Test File Integrity Check FIPS.SYS Seed Test Diffie-Hellman Monte Carlo Test

4.0 CRYPTOGRAPHIC KEY MANAGEMENT

The Client itself automatically performs all cryptographic processing and key management functions.

4.1 Key Generation

The Client uses six cryptographic keys, generated by FIPS-approved processes:

- Static Private Key
- Static Public Key
- Static Secret Encryption Key (Symmetric, Triple-DES and AES)
- Dynamic Private Key
- Dynamic Public Key
- Dynamic Session Key (Symmetric, Triple-DES and AES)

In addition to the above cryptographic keys, the module also relies on the following critical security parameters (CSPs):

- Access ID
- Crypto Officer Password
- Module's Secret Key (Symmetric, Triple-DES and AES; derived from the Access ID)

The public and private keys above are those used in the Diffie-Hellman key agreement protocol. The Module Secret Key is not generated in an Approved manner; therefore, the Static Diffie-Hellman key agreement, in which the Module Secret Key encrypts the Static Public Key, is considered to be a plaintext transmission.

An ANSI X9.31 A.2.4 pseudo-random number generator generates random numbers used for generating the module private keys.

4.2 Key Storage

No encryption keys are stored permanently in the module hardware. In accordance with FIPS 140-2 standard, the Access ID and Crypto Officer Password are considered to be stored in plaintext, as the method used to encrypt does not use an Approved key.

4.3 Zeroization of Keys

The session keys of the Client are automatically zeroized when the system is turned off and regenerated at every boot-up of the host hardware. On a PC, Zeroization of the Access ID and Crypto Officer Password can be accomplished by formatting the hard drive, on a pocket PC, they can be zeroized by performing a "hard reset" (wiping the NVRAM) of the device.

4.4 Protocol Support

The Client supports the Diffie-Hellman key agreement protocol.

4.5 Cryptographic Algorithms

The Client applies the following cryptographic algorithms:

Table 2: Algorithms Supported by the Client

FIPS Algorithms NIST-FIPS	Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	607
Triple-DES (CBC, encrypt/decrypt)	579
SHS	656
HMAC-SHA-1	313
RNG	346
Non-FIPS Algorithms	
Diffie-Hellman (Key Agreement; 512, 1024, and 2048 bit key sizes supported, but only 1024 bit or higher allowed in approved mode.), MD5	
DES (ECB, CBC, encrypt/decrypt)	

5.0 ACCESS CONTROL POLICY

The Client only allows role-based access for the Crypto Officer role to operator interfaces that access to the appropriate set of management and status monitoring tools. Direct console access supports the majority of System Administrator (Cryptographic Officer) tasks.

Users can review module status and manage system settings where appropriate but not cryptographic settings when the modules are operating in FIPS mode. Because the Client automates cryptographic processing, operators do not have to actively initiate cryptographic processing; the Client encrypts and decrypts data sent or received by operators using authenticated devices connected to the Client

The Crypto-Officer must use his/her password to access the system. The password can be defined with letters, numbers and special characters. It must be minimum eight (8) characters long. (The maximum length can be 16 characters.)

The Tables 1 and 2, defined by Fortress Technologies' Access Control Policy, show the authorized access and services supported and allowed to each role. As a user does not have any interaction with the module security relevant data items.

6.0 PHYSICAL SECURITY POLICY

The Client was designed to be installed on production quality devices as defined by the FIPS PUB 140-2 for security level 1. However, as the Client is delivered as a software cryptographic module only, the physical security requirements do not apply to the module.

Table 3 and 4 show some of the hardware on which Fortress Technologies independently tested the Secure Client. This listing does not describe the hardware platforms on which FIPS validation conformance testing was performed.

Table 3: Some PCs and NICs that are Compatible with Client

MODEL	Wired NIC	Wireless NIC	OS
Optiplex GX150 Desktop	3Com Integrated (3C920)	Belkin 802.11G PCI (F5D7001)	WinXP Pro SP2
Optiplex GX150 Desktop	3Com Integrated (3C920)	3Com 802.11A/B/G PCI (3CRDAG675)	WinXP Pro SP2
Optiplex GX150 Desktop	3Com Integrated (3C920)	Linksys 802.11G PCI (WMP54G)	Win2000 SP4
Optiplex GX150 Desktop	3Com Integrated (3C920)	Cisco PCI 802.11A/B/G (AIR-PI21AG-A-K9)	WinXP Pro SP2 Win2000 SP4
Optiplex GX150 Desktop	3Com Integrated (3C920)	Netgear 802.11A/G PCI (WAG311)	WinXP Pro SP2
Latitude C840 Laptop		Dell TrueMobile 1150 Mini PCI	WinXP Pro SP2
Fujitsu N6210 Laptop		IntelPro 802.11A/B/G (2915ABG)	WinXP Pro SP2
HP Proliant ML110 Server	Vmware AMD PCNet adapter		Win2003 Standard Server Win2003 Enterprise Server
IBM 390X Laptop		Orinoco 802.11A/B/G PCI (8480FC)	WinXP Pro SP2
Compaq SFF Series Desktop		Orinoco 802.11A/B/G USB	WinXP Pro SP2
Compaq Ipaq Agency Series PD1040		Netgear USB 802.11B (MA111)	WinXP Pro SP2
IMB ThinkPad T43 Laptop		IntelPro 802.11B/G Integrated (2200BG)	WinXP Pro SP2
Compaq DeskPro Desktop	Compaq (NC3161)		WinXP Pro SP2 Win2000 SP4
Optiplex GX150 Desktop	3Com Integrated (3C920)		WinXP Pro SP2
IBM 300 PL Desktop	Intel Integrated (8255)		WinXP Pro SP2
Compaq DeskPro Desktop	Compaq (NC3161)	Proxim Orinoco 802.11B USB (8425-WD)	WinXP Pro SP2

Fujitsu N3510 Laptop		IntelPro 802.11B/G Integrated (2200BG) Proxim Orinoco 802.11B USB (8425-WD)	WinXP Pro SP2
IMB ThinkPad T42 Laptop	Intel Pro/1000 MT	IntelPro 802.11B/G Integrated (2200BG) Proxim Orinoco 802.11B USB (8425-WD)	WinXP Pro SP2
Acer CL32 Aspire 2000 Laptop		IntePro 802.11B Mini PCI (LAN 2100 3B) Proxim Orinoco 802.11B USB (8425-WD)	WinXP Pro SP2
Generic Chassis Server	3Com 10/100 PCI (3C905B-TX)		Win2003 SP2 Standard Server
Generic Chassis Server	Intel Pro100+ PCI		Win2000 Server SP4
HP Compaq nc6220 Laptop	Broadcom 10/100/1000 NetXtreme	IntelPro 802.11A/B/G (2915ABG)	WinXP Pro SP2
Toshiba Satellite M30-S309	Intel Pro/100 VE	Intel Pro/Wireless LAN 2100 3B	WinXP Pro SP2
Compaq SFF Series Desktop	Intel 82559 Fast Ethernet	Netgear USB 802.11B (MA111)	WinXP Pro SP2 Win2000 SP4
Compaq Ipaq Agency Series PD1040		Netgear USB 802.11B (MA111)	WinXP Pro SP2
Dell Optiplex GX-150 Desktop	3Com Integrated (3C920)		WinXP Pro SP2 Win2000 SP4
Compaq Armada 7X Laptop	Socket EA Lower Power Credit Card Eth Adapter		WinXP Pro SP2
Dell MP061 Laptop	Broadcom 440x Integrated	Dell Wireless 1390 WLAN Mini Card Rev 3.6	WinXP Pro SP2
IBM T43 268DGLI Laptop	Broadcom NetXtreme Gigabit Ethernet	Intell Pro/Wireless 2200BG Dell True Mobile 1300 802.11BG PC Card Proxim OriNOCO 11 ABG Combo Card Gold	WinXP Pro SP2
Fujitsu LifeBook P Series Laptop	Realtek TRL8139/810x		WinXP Pro SP2

Table 4: Some PDA and Handhelds Compatible with Client

Type	Make	Model	CE Build Number	NIC(s) Tested
PDA	_TEMPLATE	_TEMPLATE		Integrated
PDA	HP iPAQ	hx2490	Build 14366.1.0.1	Integrated
PDA	HP iPAQ	h4355	Build 13252	Integrated
PDA	HP iPAQ	h5455	Build 11178	Integrated

PDA	HP iPAQ	h5555	Build 13100	Integrated
PDA	HP iPAQ	hx4700	Build 14132	Integrated
PDA	Dell	Axim X3	Build 13349	Integrated
Handheld	Intermec	700 Series	Build 13100	Embedded
PDA	Dell	Axim X50	Build 14260.2.0.5	Integrated
PDA	HP iPAQ	h5450	Build 11178	Integrated
PDA	Dell	Axim X30	Build 13349	Integrated
Handheld	Symbol	MC9090	5.0 (bld 1400)	Integrated - Symbol 802.11a/b/g
PDA	Dell	Axim X51v	Build 14957.2.3.1	Integrated
Handheld	Symbol	MC70 - 7094	Build 14402.1.1.0	Integrated
Handheld	Handheld Products (HHP)	Dolphin 7900	v4.21.1088 (Build 14235.2.0.0)	integrated 802.11b
Handheld	Symbol	MC3000 - 3090G	Build 1400	

The physical security of a deployed Client is determined by the customer's security policy.

7.0 SOFTWARE SECURITY

The Client software is written in C and C++ and operates on most versions of the Windows operating system. The software is installed in the host hardware storage medium as a compiled executable.

Self-tests validate the operational status of each product, including critical functions and files. If the software is compromised, the module enters an error state in which no cryptographic processing occurs, preventing a security breach through a malfunctioning device.

8.0 OPERATING SYSTEM SECURITY

The Client operates on Microsoft® Windows® NT, 2000, XP, and CE. FIPS validation conformance testing was performed specifically on the Windows 2000 Professional (SP4), Windows XP Professional (SP2), Windows 2003 Server (SP2), Windows CE v3.0, Windows CE v4.0, and Windows CE v5.0 platforms. The operating system must be in single-user mode. The Client operates automatically after power-up.

9.0 MITIGATION OF OTHER ATTACKS POLICY

No special mechanisms for the mitigation of other attacks are built into or claimed by the Secure Client.

10.0 EMI/EMC

The Fortress Technologies, Inc.'s engineer or the customer's cryptographic officer installs the Client on FCC-compliant (Part 15, Subpart J, Class A), Class B devices.

11.0 CUSTOMER SECURITY POLICY ISSUES

FTI expects that after the module's installation, any potential *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 software installation and reinstallation for modules is performed by the cryptographic officer following the procedures defined by Fortress Technologies. Software troubleshooting to resolve an error state may require the product to be reinstalled by the cryptographic officer.

- * - * -

End of the "Non-Proprietary Security Policy for the FIPS 140-2 Level 1Validated Fortress Secure Client" document.