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

Software Version 4.0

(Document Version 1.04)

August 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

This security policy defines all security rules the Fortress Secure Client (also referred to throughout the Security Policy as "Client" or "Module") must operate under and enforce. 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 applicable drivers and compiled application executable. The physical boundary is the hardware platform, such as a typical PC, on which the Client is installed. The Client identifies network devices and encrypts and decrypts traffic transmitted to and from those devices.

The module 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 over the network to protect data passing to and from the module on the wireless network.

The Client operates at the datalink layer of the OSI model, and is installed as an application and intermediate driver; the cryptographic processing is implemented without human intervention to prevent any chance of human error.

The Client was tested while running on the following operating systems and hardware platforms:

- Windows 2000 Professional on an Intel Processor
- Windows XP Professional on an Intel Processor

The Cryptographic Officer role manages the cryptographic configuration of the Client. This is the only role that can configure user profiles. A user profile is the configuration values needed to establish a connection with a particular network. It determines what encryption type to use, key establishment key sizes, and what cards to bind to among other option. Both the Cryptographic Officer and User can review module status and select the profile to use, where appropriate. The cryptographic settings can only be configured within profiles and only by the Cryptographic Officer when the module is operating in FIPS mode. Because the Client automates cryptographic processing, end users do not have to actively initiate cryptographic services. The Client encrypts and decrypts data sent or received by users over the encrypted connection.

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.

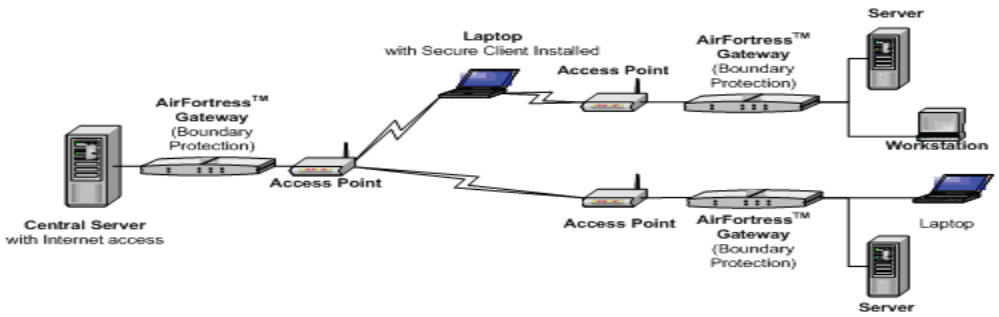

Figure 1: Example Configuration of Fortress Client Deployment

2.0 CLIENT SECURITY FEATURES

The Client provides datalink 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 Client:

1. Use strong, proven encryption solutions such as; Triple-DES and AES.
2. Protects data at or below the level of the vulnerable TCP/IP layer 3 IP information.
3. 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.
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 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 datalink layer, header information is less likely to be intercepted. In addition to applying standard strong encryption 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 Client requires no special configuration to operate once correctly installed. Cryptographic Officers are, however, required 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 for 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® operating system's Network Driver Interface Specification (NDIS) Intermediate protocol and then to the module's packet capture component, which identifies packets as incoming or outgoing. The module 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 is always encrypted. The Client does not allow plaintext transmission of data, cryptographic keys, or critical security parameters across a LAN or WLAN. Figure 3 shows the 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 uses logical controls to handle the information flow of communication, which passes 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 (alternating Bypass). 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

Each Client can be configured to accept and send packets as ciphertext or cleartext. Only with 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 applicable chip drivers and 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 the Client installed and configured appropriately can also communicate with each other directly.

The Client units designed for government use apply two FIPS-approved encryption algorithms: the Advanced Encryption Standard and Triple-DES. These algorithms encrypt and decrypt plaintext into ciphertext and ciphertext into plaintext.

512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.

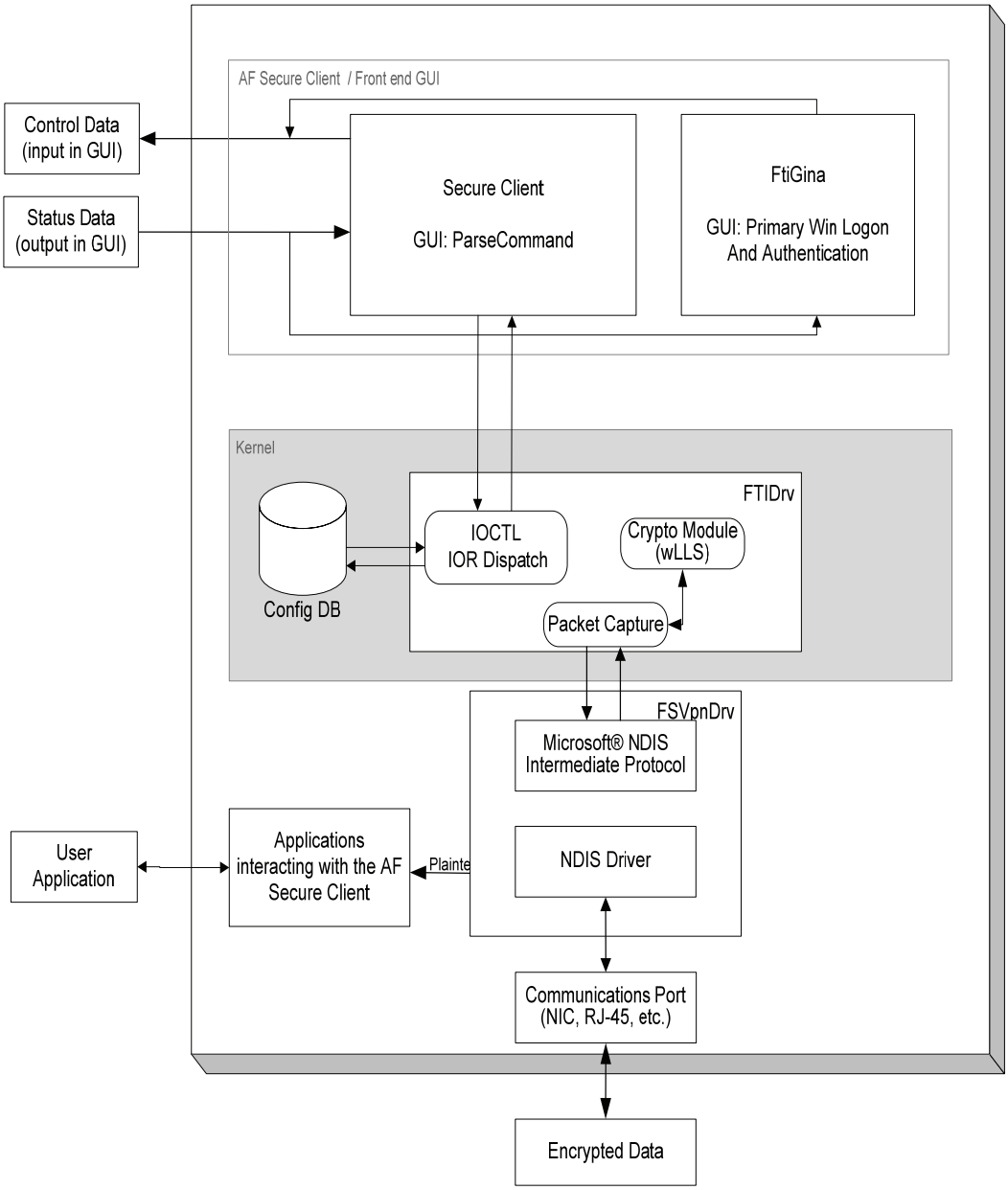

Figure 2: Information Flow through the Client

3.0 IDENTIFICATION AND AUTHENTICATION POLICY

3.1 Roles

The Client supports two roles, the User role and the Cryptographic Officer role, as follows.

- **Cryptographic Officer:** The Cryptographic Officer has complete authority over the client. The Cryptographic Officer is the Windows System Administrator and is only one who can configure profiles or Endpoints. The Cryptographic Officer role is assumed by authenticating to the OS as an Administrator.
- **User:** The User has the ability to select a preconfigured profile and monitor certain services. A User cannot configure or change any cryptographic parameter. The User role is assumed by connecting to the module with knowledge of the Access ID.

Note: Level 1 cryptographic modules do not require authentication to assume a role. The authentication has not been tested for compliance to FIPS 140-2.

3.2 Services

The following table defines the services available for the module.

Table 1: Module Services

Category	Service	Monitor	Change	Automatic
Security Functions	Encrypt/Decrypt			X
	Bypass			X
Self Tests	Crypto Algorithm Tests			X
	Software Integrity Check			X
	SHA1 and HMAC Test			X
	SHA256 Hash HMAC Test			X
	Continuous Rand Number Generator Test			X
	Bypass Test			X
	Hardware Identifier Check			X
	Seed Test			X
	DH Monte Carlo Test			X
Control Input (GUI)	Profiles	X	X	
	Endpoints	X	X	
	Encryption Type	X	X	
	Key Establishment	X	X	
	Access ID	X	X	
	Block Peer-to-Peer	X	X	
	Use SmartCard	X	X	
	Encrypted Traffic to	X	X	
	Enable and set Auto Compression	X	X	
	Allow multiple MSP Connections	X	X	
	Trusted Devices (Bypass)	X	X	
	IEEE 802.1x traffic	X	X	
	Subnet routing	X	X	
	System Options	X	X	
	Windows Login	X	X	
	Preferences	X	X	
Status Output (GUI)	Status	X		
	Diagnostics	X		
	Log	X		

4.0 ACCESS CONTROL POLICY

The Client allows role-based access to user interfaces that access the appropriate set of management and status monitoring tools. Direct access supports 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. The Client automates cryptographic processing so 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 System Administrator (Cryptographic Officer) is assumed by authenticating to the Windows OS as any Windows Administrator.

Note: Level 1 cryptographic modules do not require authentication to assume a role. The authentication has not been tested for compliance to FIPS 140-2.

The following list defines the services available to each of the authorized roles of the module. Each service is further defined in Table 1, above.

System Administrator (Cryptographic Officer):

- Perform Security Functions
- Run Self-Tests
- Enter Control Input via the module GUI
- Status Output via the module GUI

User:

- Perform Security Functions
- Run Self-Tests
- Status Output via the module GUI

5.0 CRYPTOGRAPHIC KEY MANAGEMENT

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

5.1 Key Management

The Client uses seven cryptographic keys, as follows:

Table 2: Keys Supported by the Client

Key	Key Type	Creation	Notes
Module Secret Key (MSK) (AES/Triple-DES)	AES (128, 192, or 256 bits) Triple-DES (196-bits)	If 16 digit Access ID: Seeded with 8 bytes of Access ID and 8 bytes of Fortress pre-defined constant. Seed is SHA1 hashed and result sent to encryption engine to form the key, or,	N/A
		If 32 digit Access ID: Seeded with 16 bytes of Access ID. Seed is SHA-256 hashed and result sent to encryption engine to form the key	N/A
Static Private Key (Diffie-Hellman Intermediate value)	512-bit, 1024-bit, or 2048-bit key	For 512-bit keys: Seeded with 16 bytes of pre-defined constant. Seed is SHS hashed and used per the Diffie-Hellman protocol.	512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.
		For 768-bit, 1024-bit, 1536-bit, or 2048-bit keys: 512-2048 bits are created by the ANSI X.9.31 RNG and used as this key.	N/A
Static Public Key (Diffie-Hellman Intermediate value)	512-bit, 1024-bit, or 2048-bit key	Above Diffie-Hellman Static Private Key is used to create this key per the Diffie-Hellman protocol.	512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.
Static Secret Encryption Key (AES/Triple-DES)	AES (128, 192, or 256 bits) Triple-DES (196-bits)	Established through Diffie-Hellman Key Establishment	N/A
Dynamic Private Key (Diffie-Hellman Intermediate value)	512-bit, 1024-bit, or 2048-bit key	512-2048 bits are created by the ANSI X.9.31 RNG and used as this key.	512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.
Dynamic Public Key (Diffie-Hellman Intermediate value)	512-bit, 1024-bit, or 2048-bit key	Above Diffie-Hellman Dynamic Private Key is used to create this key per the Diffie-Hellman protocol.	512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.
Dynamic Session Key (Dynamic Common Secret Key) (AES/Triple-DES)	AES (128, 192, or 256 bits) Triple-DES (196-bits)	Established through Diffie-Hellman Key Establishment	N/A

The public and private keys above refer to those used in the Diffie-Hellman key agreement protocol. 512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode.

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

5.2 Key Storage

No encryption keys are stored permanently in the module.

5.3 Zeroization of Keys

The session keys of the Client are automatically zeroized when the system is turned off and recreated at every boot-up of the host hardware. All other keys are zeroized immediately after use.

5.4 Protocol Support

The Client supports the Diffie-Hellman key agreement protocol using a configurable Diffie-Hellman key size of 512, 1024 or 2048 (512-bit Diffie-Hellman Intermediate Values may not be used in FIPS mode).

5.5 Cryptographic Algorithms

The Client applies the following cryptographic algorithms:

Table 3: Algorithms Supported by the Client

FIPS Algorithms	Certificate number
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	427, 437
Triple-DES (CBC, encrypt/decrypt)	457, 463
SHS	498, 505, 573
HMAC-SHA-1	201, 205
HMAC-SHA-256	256
RNG	221, 227
Non-FIPS Algorithms	
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength; non-compliant less than 80-bits of encryption strength); DES; MD5; RSA (non-compliant)	

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 (128, 293, 256 bits), Triple-DES KAT, DES KAT, HMAC-SHA-1 KAT, HMAC-SHA-256 KAT, SHA-1 KAT, SHA-256 KAT, and RNG KAT
- Software Integrity Test: HMAC (SHA-256).
- Critical Functions Tests: Diffie-Hellman Monte Carlo Test

B. Conditional Test

- Continuous Random Number Generator test
- Seed Test
- Bypass Test

Failure of any self-test listed above puts the module in its error state. The Software Integrity Test is performed over each module component individually at power-up.

6.0 PHYSICAL SECURITY POLICY

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

7.0 SOFTWARE SECURITY

The module was tested on Microsoft® Windows® 2000 and Microsoft® Windows® XP. The Client software is written in C and C++ and operates on the Microsoft® Windows® NT, 2000, XP, and CE Operating Systems (not tested on NT or CE). 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 module was tested on Microsoft® Windows® 2000 and Microsoft® Windows® XP. The Client operates on Microsoft® Windows® NT, 2000, XP, and CE (not tested on). 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 are built in the Client; 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 Client units using this same unique value can establish key exchange: *Mitigates unauthorized connections to the module.*
2. The Client uses FIPS-approved SHS (NIST certification #498, #505 and #575) and HMAC hashing (NIST certification #205, #201 and #256) and FIPS-approved encryption/decryption methods: Triple-DES (certification #457 and #463), AES (certification #427 and #437): *Mitigates attacks to decrypt traffic and crack keys*.
3. The Client enforces strong authentication of communicating parties: *Mitigates "spoofing" credentials*.
4. The Client 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. The Client passes encrypted communication and plaintext communication for trusted devices and for 802.1x connections. Trusted devices and 802.1x must be specifically configured: *Mitigates unauthorized access to the sent data.*
11. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
12. No encryption keys are stored permanently in the module: *Mitigates key discovery.*
13. All software data are stored in executable format in the module: *Mitigates access to the module software.*
14. When the Client 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

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

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 software installation and reinstallation for modules is performed by the Cryptographic Officer following the procedures defined by Fortress Technologies, Inc. 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 Validated Fortress Secure Client Cryptographic Module" document.