Non-Proprietary Security Policy for the FIPS 140-2 Level 1 Validated Fortress Secure Client Cryptographic Module Version 2.5.6

Document Revision 2.7

May 2007

This security policy of Fortress Technologies, Inc., Fortress Secure Client Cryptographic Module defines general rules, regulations, and practices under which the Client was designed and developed and for its correct operation. These rules and regulations have been and must be followed in all phases of security projects, including the design, development, manufacture service, delivery and distribution, and operation of products.

Contents

1.0 INTRODUCTION

This Security Policy defines all security rules under which the Fortress Secure Client Cryptographic module, hereafter referred to as the Client, must operate 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 compiled application executable. The physical boundary is the hardware platform, such as a typical PC or a Personal Digital Assistant (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 all clients "behind" it on a protected network. Only the Cryptographic Officer can log into the module.

The Client operates at the datalink, (also known as Media Access Control (MAC)) layer of the Open System Interconnection (OSI) model. Most of the security protocols are implemented without human intervention to prevent any chance of human error.

The Client is designed to operate using both Linux and Microsoft Operating Systems. The products operate with minimal intervention from the user. It secures communication within Local Area Networks (LANs), Wide Area Networks (WANs), and Wireless LANs (WLANs).

The Cryptographic Officer manages the cryptographic configuration of the Client. 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 or Controller. The products encrypt outgoing data from a client device and decrypt incoming data from networked computers located at different sites.

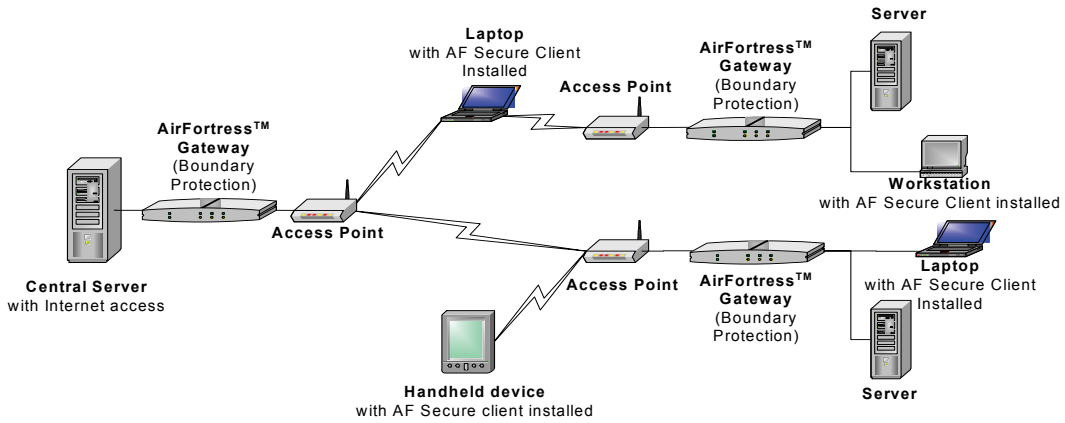

Figure 1: Example Configuration of Fortress Secure Client Deployment

2.0 CLIENT SECURITY FEATURES

The Client provides true datalink layer security. To accomplish this, it was designed with the security features described in the following sections.

2.1 Cryptographic Module

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

1. Use FIPS-approved and NIST recommended cryptographic algorithms, such as, Triple-DES and AES.
2. 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.
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 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 using FIPS-approved and NIST recommended cryptographic 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 customers 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 module has one logical interface for information flow, which handles all communication into and out of the module. Data is transmitted to the secure network exclusively as ciphertext. 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 Operational Mode (FIPS Mode):

During Client installation the Cryptographic Officer selects FIPS mode. The Client AccessID, algorithm and key size must be set to that used by the other Fortress cryptographic modules in the network. Only in this way can the Client communicate with other secured Fortress modules operating in FIPS mode. The Client units operating in FIPS mode must apply only FIPS-approved AES and Triple-DES encryption algorithms to the plaintext. The Cryptographic Officer must configure the host operating system in single user mode. To determine FIPS mode status, access the GUI (Web) interface and click on the locked padlock symbol located in the system tray.

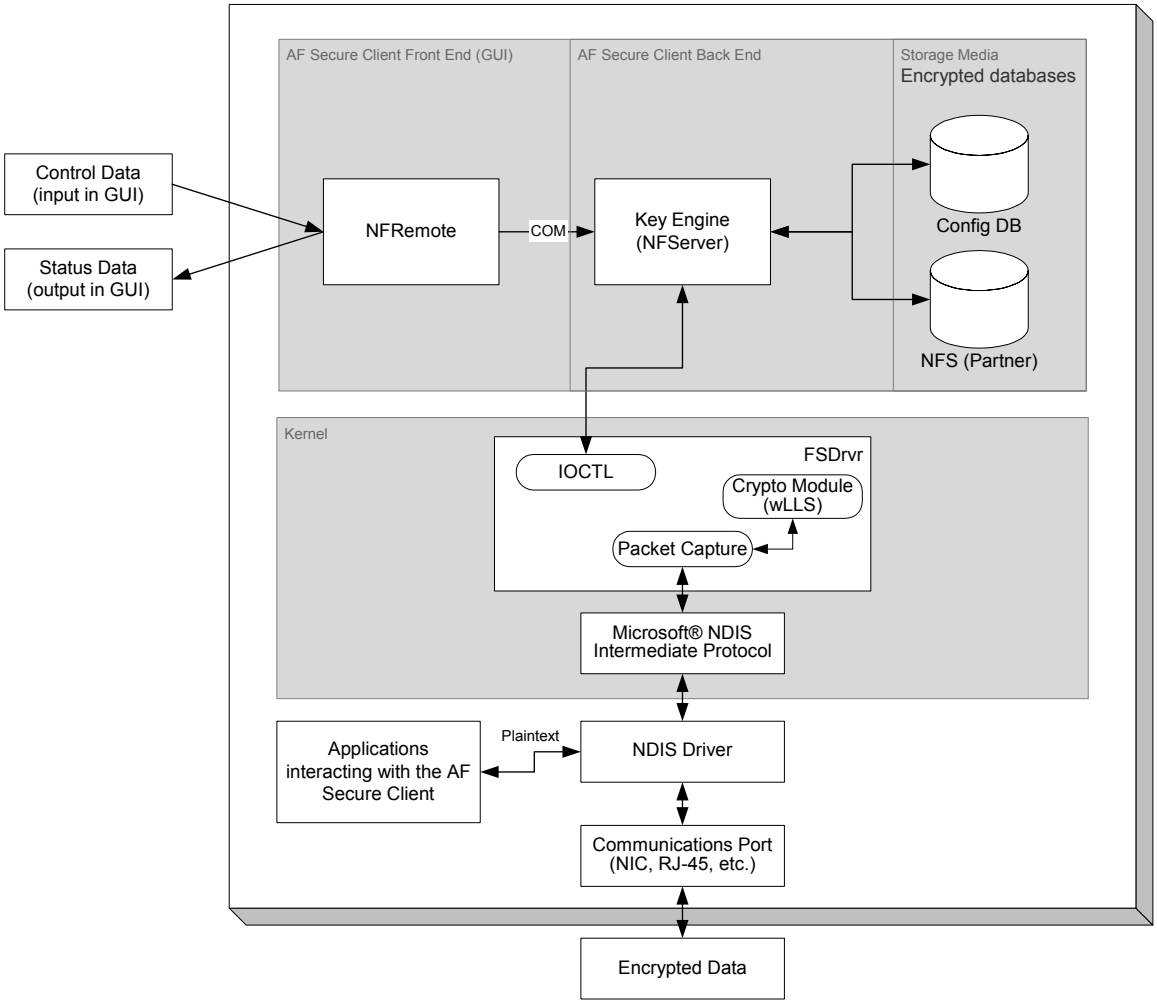

Figure 2: Information Flow Through the Client

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 is supported.

3.1.1 The User Role

The User role can monitor system status and perform the following tasks:

- Review system status information
- Reset current session keys (effectively zeroizing the session keys)
- Cryptographic Services (encryption/decryption)

The User cannot change any critical system or cryptographic settings. The User role is assumed by connecting to the module with knowledge of the configured Access ID.

3.1.2 The Cryptographic Officer Role

The Cryptographic Officer role 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/uninstall the Client
- Configure the unique Access ID
- Import an Access ID
- Select the cryptographic algorithm to use
- Set operation mode to FIPS or non-FIPS
- Configure Cryptographic Officer password
- Reset current session keys (zeroizes the current session key)

The Cryptographic Officer performs most tasks while installing the Client. Access to other cryptographic controls after the product is installed requires the Cryptographic Officer to enter the correct password. Passwords must be of a minimum specified length.

3.2 Services

The following key management services are provided in the Client without requiring operator intervention:

- Establishing the module Secret keys
- Establishing cryptographic keys using encrypted Diffie-Hellman exchanges to prevent man-in-the-middle attacks
- Authenticating devices (User Role) attempting to communicate with the Client
- Reinitiating key exchange at specified intervals
- Zeroizing keys if power to the module is turned off

The following cryptographic operations services are provided in the module without requiring operator intervention:

- Filtering packets to prevent any unencrypted (and, therefore, unauthorized) packets from entering the network
- Encrypting and decrypting packets at the datalink layer (OSI level 2)
- Authenticating the origin of packets

Other services performed by the module include monitoring and displaying device status and performing all self-tests.

The following table shows the services supported and allowed to the Cryptographic Officer and the User roles.

Table 1: Summary of Module Services

Service	Input	Output	Role	Access
Configure Cryptographic Officer password	Command	Password	CO	Write
Configure the unique Access ID	Command	ID	CO	Write
Set Device MAC	Device ID	Device ID	CO	Read
FIPS mode on/off	Command	Status	CO	Write
Install/set-up the Client	Command	Configured Client	CO	Write
Cryptographic algorithm Selection	Command	DES*, Triple-DES, AES	CO	Write
Key Establishment	None	Diffie-Hellman intermediate values during session establishment	U	Execute
Encryption	Plain text	Cipher text	U	Execute
Decryption	Cipher text	Plain text	U	Execute
Reset current session	Command	New status	CO, U	Execute
Show status	Command	Status	CO, U	Read
Self-tests	Command	Status	CO, U	Execute

Note: CO- Cryptographic Officer, U-user; *DES cannot be used in FIPS mode

3.3 Self-Tests

The following list of all self-tests includes both power-up tests and conditional tests that apply to the Client.

A. Power-Up Tests

- Cryptographic Algorithm Test
  - ◊ AES KAT
  - ◊ Triple-DES KAT
  - ◊ DES KAT
  - ◊ HMAC KAT
  - ◊ SHA-1 KAT
  - ◊ RNG KAT
- Software Integrity Test (HMAC)

B. Conditional Tests

- Continuous Random Number Generator Test

4.0 CRYPTOGRAPHIC KEY MANAGEMENT

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

4.1 Key Usage

The Client uses seven cryptographic keys:

- Module's Secret Key (Symmetric, Triple-DES and AES)
- Static Private Key (Diffie-Hellman)
- Static Public Key (Diffie-Hellman)
- Static Secret Encryption Key (Symmetric, Triple-DES and AES)
- Dynamic Private Key (Diffie-Hellman)
- Dynamic Public Key (Diffie-Hellman)
- Dynamic Session Key (Symmetric, Triple-DES and AES)

Secret symmetric DES keys are available for backward compatibility with legacy units. DES is not to be used in FIPS mode.

The public and private keys above are those used in the Diffie-Hellman key agreement protocol. These are 512-bit keys and provide 56-bits of encryption strength. These keys are encrypted using the selected symmetric encryption algorithm.

An ANSI X9.31 A.2.4 pseudo-random number generator is used in the Diffie-Hellman key agreement process.

4.2 Key Storage

All cryptographic keys are only stored temporarily in volatile RAM.

4.3 Zeroization of Keys

The Client session keys are automatically zeroized when the system is terminated and regenerated at every boot-up of the host hardware. The Cryptographic Officer can zeroize all session keys manually.

4.5 Cryptographic Algorithms

The Client applies the following cryptographic algorithms:

Table 2: Algorithms Supported by the Client

FIPS Algorithms	Certificate
AES (ECB, CBC, encrypt/decrypt; 128, 192, 256)	#427 and #437
Triple-DES (CBC, encrypt/decrypt)	#457 and #463
SHS	#498 and #505
HMAC	#201 and #205
RNG	#221 and #227
Non-FIPS Algorithms	
DES (non-compliant); MD5; Blowfish; GUAVA; IDEA; Diffie-Hellman (transitional phase only - valid until May 19, 2007; key agreement; key establishment methodology provides 56 bits of encryption strength)	

5.0 ACCESS CONTROL POLICY

The Client allows role-based access to user interfaces that access to the appropriate set of management and status monitoring tools. Direct console access supports the majority of 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 user cannot switch the module out of FIPS mode. Because of 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 Cryptographic Officer must use his/her password ID to access the system. The password can be defined with letters, numbers and special characters. It must be a minimum of eight (8) characters long; the maximum length is 16-characters.

Table 3: Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Cryptographic Officer Password	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.

6.0 PHYSICAL SECURITY POLICY

The Client is designed for installation 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. The Client was tested on the Operating System/hardware combinations shown in Table 4.

Table 4: Tested Hardware Combinations

Operating System	CPU	Type
MS Windows 2000	Intel Pentium	Desktop
MS Windows XP	Intel Pentium	Desktop
MS Windows CE 3.0	Intel ARM	Pocket PC
MS Windows CE 4.0	Intel ARM	Pocket PC
Linux (kernel 2.4.21-37:EL)	Intel Pentium	Desktop

7.0 SOFTWARE SECURITY

The Client software is written in C and C++. The software is installed in the host hardware storage medium as a compiled executable. The software cannot be upgraded when operating in FIPS mode.

A software integrity test is performed each time the system is booted. 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 was tested on the Linux (kernel 2.4.21-37:EL), Microsoft® Windows® 2000, XP, CE 3.0, and CE 4.0 Operating Systems. The Operating System must be in single-user mode. The Client operates automatically after power-up. See the appropriate user guide for detailed installation instructions.

9.0 MITIGATION OF OTHER ATTACKS POLICY

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 enforces strong authentication of communicating parties: *Mitigates "spoofing" credentials*.
3. The Client applies strong authentication of the origin of the packets: *Mitigates packet modification.*
4. The dynamic session key is changed at least once every 24 hours, with 4 hours being the factory default duration: *Mitigates key discovery.*
5. 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*.
6. All key exchanges are encrypted: *Mitigates encryption key sniffing by hackers.*
7. Data in transit is subjected to integrity checking: *Mitigates data modification and active attacks to inject traffic.*
8. 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*.
9. Encryption happens at the datalink layer so that all network layer information is hidden: *Mitigates hacker's access to the communication.*
10. No session keys are stored: *Mitigates key discovery.*

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

Fortress Technologies, Inc. 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, 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 ™ Client Cryptographic Module" document.