Fortress Secure Client
Version 4.1.1
Security Policy

Version 1.3
March 2009

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

Table of Contents

List of Figures

List of Tables

This page is intentionally blank

1.0 Introduction

This is a non-proprietary Fortress Secure Client security policy. This security policy defines all security rules the Fortress Secure Client version 4.1.1 (also referred to throughout the Security Policy as "Module") must operate under and enforce. The Module complies with all FIPS 140-2 level 1 requirements.

2.0 References

- Secure Client 4.1 User Guide
- Fortress FC-X (X=250, 500 or 1000)
- Fortress Gateway User Guide for the AirFortress 7500 or 2100.
- Fortress MAPS User Guide
- Fortress ES-520 User Guide
- Compatible Radius vendors' User Guides
    - See Fortress Secure Client User Guide for compatible Radius vendors
- Compatible Smart Card vendors' User Guides
    - See Fortress Secure Client User Guide for compatible Smart Card vendors

3.0 Document Organization

This document is the FIPS 140-2 Security Policy is for the Fortress Secure Client version 4.1.1. Section 1.0 is a brief introduction of the module. Section 2 will call out the references needed to understand the module. Section 3.0 (this section) will summarize the document organization. Section 4.0 will describe the security rules under which this cryptographic module will operate. This includes a definition of the Module, its components, roles and services, key management and algorithms. Section 5.0 will detail the secure operation of the Module. And finally Section 6.0 will explain installation issues and how to contact Fortress if necessary.

4.0 Security Rules

4.1 Introduction

The Fortress Secure 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 module is installed. The module 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 module encrypts and decrypts traffic transmitted over the network to protect data passing to and from the module on the wireless network.

The module 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.

4.2 Cryptographic Module

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

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

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 used to configure the module to implement secure connections. This will help 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 module requires no special configuration to operate once correctly installed. Cryptographic Officers are, however, 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 module allows role-based access to user interfaces for access to the appropriate set of management and status monitoring tools.

4.3 Module Interfaces

The module 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 driver then sent to the packet capture component, which identifies packets as incoming or outgoing and encrypts or decrypts the packets accordingly. This 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).

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 or feature requiring clear text is configured. The module does not allow plaintext transmission of cryptographic keys, or critical security parameters across a LAN or WLAN. The module 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.

Figure 1 shows the cryptographic boundary for the module. The boundary will include FIPS relevant modules and non-FIPS relevant modules including Windows modules.[1]

[1] The following modules are excluded from the cryptographic boundary: FTIGINA2.DLL, FSNOTIFY.DLL, FTISERVICE.EXE, MSPYMINI.SYS and FSVPNDRVR.SYS plus all Windows components.

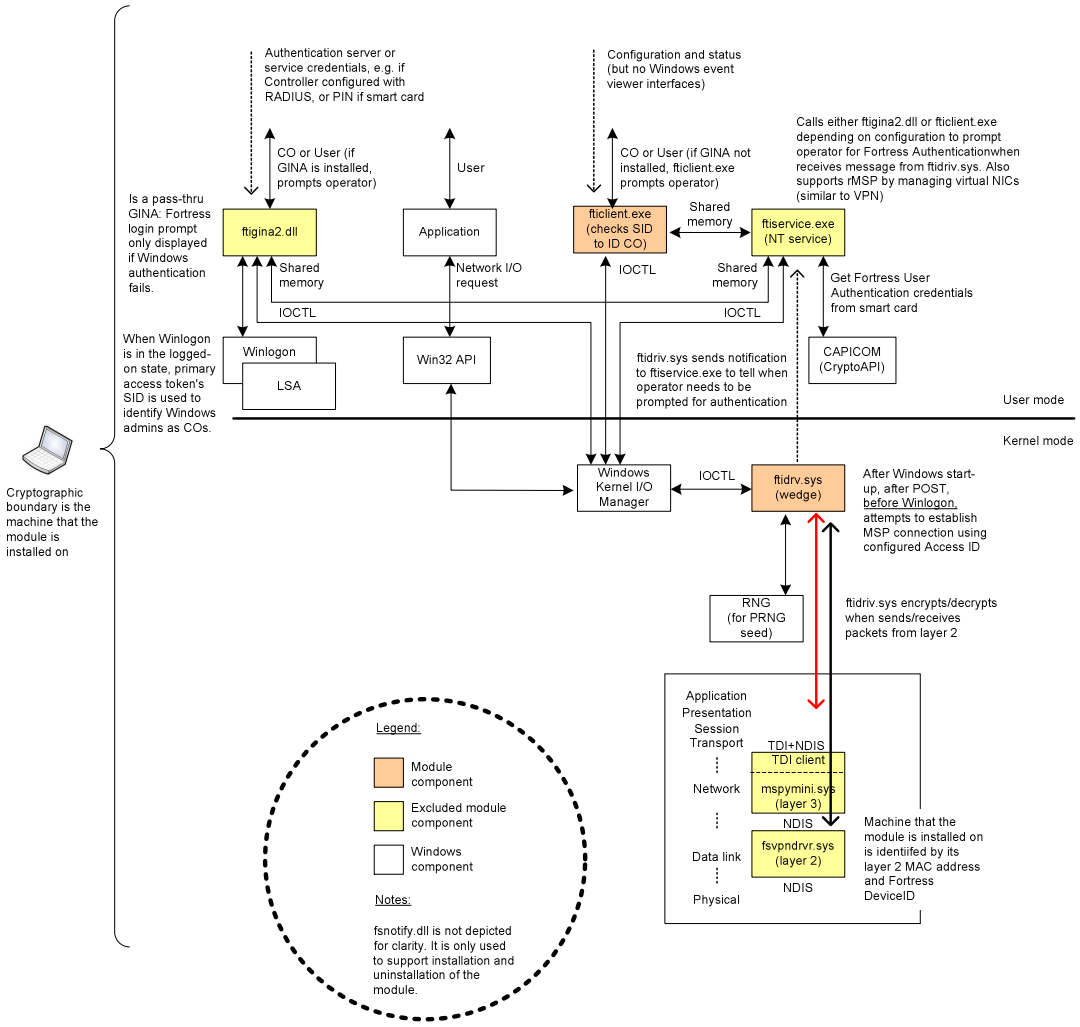

Figure 1: Cryptographic module components and interfaces

4.4 Roles and Services

There are no unauthenticated services. There is a Crypto Officer role and a User role.

4.4.1 Crypto Officer Role Services

Crypto Officers are authenticated by the operating system, not by the module.

The Crypto Officer is the Windows Administrator. The module checks to see that the user is the Windows Administrator before allowing access to the sections of the Graphically User Interface (GUI) that configure the cryptographic module. In general the Crypto Officer can configure profiles, endpoints and other options. Crypto Officer Services are shown in Table 1.

Table 1: Crypto Officer Role services

Service	Description	Input	Output	Key/CSP
Perform Power-up Self-tests	Initiates the power-up self-tests of the module, which are run when the GPC is powered-on	None	Status of command	None
Global settings update[2]	Update information that is used in presentation of the GUI	Commands and configuration data	Status of commands and configuration data	None
Profiles update[3]	Update End Point connection information.	Commands and configuration data	Status of commands and configuration data	None
Endpoints update[4]	Update End Point connection organization information and End Point power-up connection state[5]	Commands and configuration data	Status of commands and configuration data	Access ID (write)

[2] Secure Client Interfaces to update Global settings include saving the Profile that should be loaded on power-up, the last Profile ID created, the last End Point ID created, the Device ID to be used for all Endpoints, as well as the interfaces described in section “Secure Client Options” of the Secure Client User Guide.
[3] Secure Client Interfaces to configure Profiles can be found in section “Profiles” of the Secure Client User Guide.
[4] Secure Client Interfaces to configure Endpoints can be found in section “Endpoints” of the Secure Client User Guide.
[5] May contain 0 or 1 MSP Endpoints, or 0, 1, or 2 rMSP Endpoints.

4.4.2 User Role Services

Users are authenticated by the use of the Access ID. Both sides must have the same Access ID in order for a secure connection to be made. The Access ID can only be configured by the Crypto Officer. The User can pick a profile, perform diagnostics or can exit the FIPS mode by turning off all encryption. User Services included are shown in Table 2.

Table 2: User Role services

Service	Description	Input	Output	Key/CSP
Fortress (non-module) User Authentication[6]	Prompts operator for Fortress User Authentication information according to Gateway MSP configuration.	Fortress User Authentication Credentials	Status of commands	None
Select Profile[7]	Set Crypto Officer-configured Profile to use	Commands	Status of commands	None
Establish MSP connection[8]	Initiate MSP connection (perform initial key exchanges at OSI layer 2)	Commands, Static Key Exchange parameters, Dynamic Key Exchange parameters, MSP inputs and data	Status of commands and MSP connection information, MSP outputs and data	The following keys/CSPs are used/generated as a result of executing this service: Access ID, Device ID, Hardkey, DH Static public and private keys, Static Secret Encryption Key, DH Dynamic public and private keys, Dynamic Secret Encryption Key
Establish rMSP connection[9]	Initiate rMSP connection (perform initial key exchanges at OSI layer 3)	Commands, Static Key Exchange parameters, Dynamic Key Exchange parameters, MSP and rMSP inputs and data	Status of commands and MSP and rMSP connection information, MSP and rMSP outputs and data	The following keys/CSPs are used/generated as a result of executing this service: Access ID, Device ID, Hardkey, DH Static public and private keys, Static Secret Encryption Key, DH Dynamic public and private keys, Dynamic Secret Encryption Key
Winsock API (indirect interface to MSP)	Perform re-key exchanges at OSI layer 2, and encrypt and decrypt packets at layer 2.	Refresh Dynamic Key Exchange parameters, Encrypted Data Exchange parameters, MSP inputs and data	MSP outputs and data	The following keys/CSPs are used/generated as a result of executing this service: Static Secret Encryption Key, DH Dynamic public and private keys, Dynamic Secret Encryption Key
Winsock API (indirect interface to rMSP)	Perform re-key exchanges at OSI layer 3, and encrypt and decrypt packets at layer 2.	Refresh Dynamic Key Exchange parameters, Encrypted Data Exchange parameters, MSP and rMSP inputs and data	MSP and rMSP outputs and data	The following keys/CSPs are used/generated as a result of executing this service: Static Secret Encryption Key, DH Dynamic public and private keys, Dynamic Secret Encryption Key
Secure Client Monitoring[10]	View connection information and perform diagnostic tests.	Commands	Status of commands and MSP and rMSP connection information	None

[6] If the module's Fortress GINA (Graphical Identification and Authentication library which is a component of the Microsoft Windows operating systems that provides secure authentication and interactive logon services) component has been installed, a pass-thru GINA works together with the Windows logon dialogs to authenticate Users to Gateways (not the module). If the module's Fortress GINA component has not been installed, the module displays only its own dialogs to authenticate Users to Gateways (not the module).

[7] Secure Client Interfaces to change profiles can be found in section "Switching Profiles" of the Secure Client User Guide.

[8] Secure Client Interfaces to initiate MSP connections can be found in section "Connecting to Secure Networks" of the Secure Client User Guide.

[9] Secure Client Interfaces to initiate rMSP connections can also be found in section "Connecting to Secure Networks" of the Secure Client User Guide.

[10] Secure Client Interfaces to view MSP and rMSP connection information can be found in section "Monitoring the Secure Client Driver" of the Secure Client User Guide.

4.5 Cryptographic Key Management

There are keys and CSPs that are not associated with any protocols. There are also keys and CSPs associated with the Fortress Secure Client's PRNG and MSP protocol. Client keys and CSPs are identified and described in the tables below.

Table 3: Keys and CSPs: Non-Protocol

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Access ID	16- or 32 hex character string (only use 32 characters in FIPS mode)	Input plaintext (using GUI)[11]	Not output	Plaintext on disk	Not actively zeroized by the module. Formatting of HD is method for zeroization	Used as input to derive the Hardkey (a.k.a. Module Secret Key).
Device ID	32 hex character string	Not input (generated using PRNG during module installation)	Not output	Plaintext on disk	Not actively zeroized by the module. Formatting of HD is method for zeroization	The Device ID (along with the MAC address) are used to identify the module (but not the operator) to controllers as part of the MSP protocol.
Machine Hardkey	HMAC key	Not input (derived using the Fortress-proprietary non-FIPS hardkey generation method)	Not output	Plaintext on disk	Not actively zeroized by the module. Formatting of HD is method for zeroization	Used as HMAC key to compute the HMAC-SHA-256-based software integrity value used in the power-up self-test

[11] It is recommended that the Access ID be a randomly generated value to increase security, since this would reduce the risk of repeating patterns being used for different Access IDs.

Table 4: Fortress Technologies Approved PRNG's: Keys and CSPs: PRNG

Fortress Technologies Approved PRNG's			
Algorithm	Type	Seed	Uses
X9.31	Triple-DES 2 Key	Fortuna[12]	Generation of Diffie-Hellman components
X9.31	Triple-DES 2 Key	NFRandom[13]	Used as an event source for Fortuna.

Table 5: Fortress Technologies Non-Approved PRNG's: Keys and CSPs: PRNG

Fortress Technologies Non-Approved PRNG's			
Algorithm	Type	Seed	Uses
NFRandom	32 bit	Time	Inside Fortuna to pick a pool and to seed the X9.31 that is used as an event source for Fortuna.
Fortuna	32 bit	OS PRNG and X9.31	Used to seed the X9.31 when it is used for building keys.

Table 6: Windows OS: Non-Approved PRNG's: Keys and CSPs: PRNG

Window Operating System Non-Approved PRNG's		
Algorithm	Type	Uses
FIPS.SYS	64 bit	Used as an event source for Fortuna on Windows 2000 and Windows XP
Crypto API	64 bit	Used as an event source for Fortuna on Windows Vista

[12] Fortuna is an implementation of a cryptographically secure pseudorandom number generator (PRNG) devised by Bruce Schneier and Niels Ferguson named the Fortuna after the Roman goddess of chance. From Practical Cryptography (ISBN: 0-471-22357-3)
[13] NFRandom is the "minimal standard random" routine by Stephen K. Park and Keith W. Miller, in "Random number generators: good ones are hard to find", in the Oct 1988 CACM (v.31, no.10).

Table 7: Keys and CSPs: MSP Static Key Exchange

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Hardkey (a.k.a. Module Secret Key	AES CBC (e/d; 128, 192, 256) Triple-DES TCBC (e/d; KO 2) However, it is considered a CSP and not a key.	Not input (derived from the Access ID using the Fortress-proprietary non-FIPS hardkey generation method) Not generated using an Approved method.	Not output	Plaintext in RAM	Not actively zeroized by the module. Passively zeroized when power cycles.	Used to support the correct operation of the first key exchange (called the Static Key Exchange) of the MSP protocol.
Static key exchange – DH Static private key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input (generated using PRNG)	Not output	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when power cycles.	Used as part of the first key exchange (called the Static Key Exchange) of the MSP protocol to establish the Static Secret Encryption Key.
Static key exchange – DH Static public key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input. The value is calculated from the private key value using the DH equation.	Output plaintext (during the first key exchange (called the Static Key Exchange) of the MSP protocol)	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when power cycles.	Used as part of the first key exchange (called the Static Key Exchange) of the MSP protocol to establish the Static Secret Encryption Key.
Static key exchange – Static Secret Encryption Key	AES CBC (e/d; 128, 192, 256) Triple-DES TCBC (e/d; KO 2)	Not input. Derived using the result of an SP800-56A KDF based on the DH shared secret	Not output	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when power cycles.	Used to encrypt the second key exchange (called the Dynamic Key Exchange) and subsequent key exchanges (called Refresh Dynamic Key Exchanges) of the MSP protocol.

Table 8: Keys and CSPs: MSP Dynamic Key Exchanges'

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Static key exchange – Static Secret Encryption Key	See table 7.	See table 7.	See table 7.	See table 7.	See table 7.	See table 7.
Dynamic key exchange – DH Dynamic private key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input (generated using PRNG)	Not output	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when a Refresh Dynamic Key Exchange occurs Also zeroized when power cycles.	Used during the second key exchange (called the Dynamic Key Exchange, or Refresh Dynamic Key Exchange) of the MSP protocol to establish the Dynamic Secret Encryption Key.
Dynamic key exchange – DH Dynamic public key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input. The value is calculated from the private key value using the DH equation.	Output encrypted (using the Static Secret Encryption Key during the second key exchange (called the Dynamic Key Exchange) of the MSP protocol)	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when a Refresh Dynamic Key Exchange occurs Also zeroized when power cycles.	Used during the second key exchange (called the Dynamic Key Exchange, or Refresh Dynamic Key Exchange) of the MSP protocol to establish the Dynamic Secret Encryption Key.
Dynamic key exchange – Dynamic Secret Encryption Key	AES CBC (e/d; 128, 192, 256) Triple-DES TCBC (e/d; KO 2)	Not input. Derived using the result of an SP800-56A KDF based on the DH shared secret	Not output	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when power cycles.	Used to encrypt/decrypt unicast traffic at layer 2 during the protected data exchange (called the Encrypted Data Exchange) of the MSP protocol.

Table 9: Keys and CSPs: MSP Encrypted Unicast Traffic Data Exchange

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Dynamic key exchange – Dynamic Secret Encryption Key	See table 8.	See table 8.	See table 8.	See table 8.	See table 8.	See table 8.

Table 10: Keys and CSPs: MSP Group Key Exchange

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Group Static Common Key	AES CBC (e/d; 128, 192, 256) Triple-DES TCBC (e/d; KO 2) However, it is considered a CSP and not a key.	Not input (derived from the Access ID using the Fortress-proprietary non-FIPS hardkey generation method)	Not output	Plaintext in RAM	Not actively zeroized by the module. Power cycling is method for zeroization.	Used to support the correct operation of sending/receiving multicast/broadcast traffic as part of the MSP protocol.
Group Dynamic Private Key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input (generated using PRNG) However, PRNG is seeded using the Access ID, not the RNG.	Not output	Plaintext in RAM	Not actively zeroized by the module. Power cycling is method for zeroization.	Used during the Group Key Exchange of the MSP protocol to establish the Group Dynamic Common Key.
Group Dynamic Public Key	DH (512, 768, 1024, 1536, 2048) private key DH ECC (256, 384) private key	Not input The value is calculated from the private key value using the DH equation.	Output plaintext (during the Group Key Exchange of the MSP protocol)	Plaintext in RAM	Not actively zeroized by the module. Power cycling is method for zeroization.	Used during the Group Key Exchange of the MSP protocol to establish the Group Dynamic Common Key.
Group Dynamic Common Key	AES CBC (e/d; 128, 192, 256) Triple-DES TCBC (e/d; KO 2)	Not input Derived using the result of an SP800-56A KDF based on the DH shared secret	Not output	Plaintext in RAM	Zeroized when a new MSP/rMSP policy (configuration) is loaded. Also zeroized when power cycles.	Used to encrypt/decrypt multicast/broadcast traffic at layer 2 after the module determines it has the correct Group Dynamic Public Key.

Table 11: Keys and CSPs: MSP Encrypted Multicast/Broadcast Traffic Data Exchange

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
Group Static Common Key	See MSP Group Key Exchange Keys and CSPs description	See table 10.	See table 10.	See table 10.	See table 10.	See table 10.
Group Dynamic Common Key	See MSP Group Key Exchange Keys and CSPs description	See table 10.	See table 10.	See table 10.	See table 10.	See table 10.

4.6 Cryptographic Algorithms

The Client implements the following cryptographic algorithms:

Table 12: Algorithms supported

Algorithm Supported	Certificate Number	FIPS Approved?	Allowed in FIPS mode?
AES CBC(e/d; 128,192,256)	975	Yes	Yes
HMAC-SHA-1 Key Size Ranges Tested: KS=BS	547	Yes	Yes
HMAC-SHA-256 Key Size Ranges Tested: KS=BS	547	Yes	Yes
HMAC-SHA-384 Key Size Ranges Tested: KS=BS	547	Yes	Yes
HMAC-SHA-512 Key Size Ranges Tested: KS=BS	547	Yes	Yes
ANSI X9.31 Triple-DES-2Key	552	Yes	Yes
SHA-1 BYTE-only	944	Yes	Yes
SHA-256 BYTE-only	944	Yes	Yes
SHA-384 BYTE-only	944	Yes	Yes
SHA-512 BYTE-only	944	Yes	Yes
Triple-DES TCBC(e/d; KO 2) and ECB(e/d; KO 2)	768	Yes	Yes
DES	N/A	No	No
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)	N/A	No	Yes
EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)	N/A	No	Yes
MD5	N/A	No	No
RSA (non-compliant)	N/A	No	No

4.7 Mitigation of Other Attacks

The Fortress Secure Client is designed to mitigate several specific attacks:

Man-in-the-middle (before encrypted data exchanges are performed)

MSP (and rMSP by virtue of its encapsulation of MSP messages) performs two separate Diffie-Hellman key exchanges by default, providing defense against man-in-the-middle attacks. Diffie-Hellman key exchanges are performed before the module begins encrypting/decrypting packets.

Man-in-the-middle (after encrypted data exchanges have been performed)

MSP (and rMSP by virtue of its encapsulation of MSP messages) performs additional Diffie-Hellman key exchanges at Crypto Officer-configured intervals and at Controller-configured intervals, providing further defense against man-in-the-middle attacks. Diffie-Hellman key exchanges are performed after a MSP (or rMSP) connection has been established, after the module has been encrypting/decrypting packets, when either the module initiates a Diffie-Hellman key exchange at a configured interval, or when the Controller does the same.

Denial-of-service

MSP (and rMSP by virtue of its encapsulation of MSP messages) encrypts packet IP headers by default (the IP address in the rMSP UDP message is of the rMSP endpoint), providing a defense against denial of service attacks. IP headers are encrypted before the module sends the packets.

Network eavesdropping

MSP (and rMSP by virtue of its encapsulation of MSP messages) encrypts packets at the data link layer (OSI layer 2), providing defense against network eavesdropping. Packets are encrypted at layer 2 inside MSP messages before the module sends the packets.

5.0 Secure Operation of the Fortress Secure Client

5.1 System Requirements

The Client must be installed and configured on an allowed Windows operating system. Windows must be configured to operate in Single-User Mode. System requirements are listed in the table below.

Table 13: System requirements

Component	Version
Windows operating system versions that testing was performed on	Windows 2000 Professional SP 4 Windows XP Professional SP 2 Windows 2003 Server SP2 Windows Vista Ultimate Edition (32-bit)
Fortress Secure Clients (in peer-to-peer configuration)	Fortress Secure Clients version 4.1.1
Fortress Gateway	See the FC-X (shown below) or other Fortress gateway users guide for information about compatible Fortress Secure Client versions. **Module Configuration** / **Maximum Active Devices** FC-250: 500 FC-500: 1000 FC-1500: 3300
Fortress Management Access Controller (MAPS)	See the MAPS User Guide for information about compatible Fortress Secure Client versions.
Fortress Bridge	See the ES-520 user's guide for information about compatible Fortress Secure Client versions.
RADIUS servers (in EAP configurations)	See Fortress Secure Client User Guide for compatible vendors
Smart cards	See Fortress Secure Client User Guide for compatible vendors

5.2 Installing the Module

The module should be installed according to installation section of the Fortress Secure Client User Guide.

5.3 Configuring Modes of Operation

The module supports several modes of operation, including Approved modes of operation for which only Approved algorithms shall be used/selected. There is a status output indicator on the "Status" tab called "FIPS mode" of the Fortress Secure Client GUI that indicates whether or not the Client is operating in an Approved mode. Additional modes of operation, including bypass modes, can be determined by

any operator of the module using additional tabs of the GUI to examine Client settings.

The following are the modes of operation that the Fortress Secure Client supports:

- Mode 1. MSP/rMSP Approved encrypting mode:
  - Both LAN and/or WLAN traffic is encrypted using Approved algorithms and settings described below.
  - No 802.1X traffic is allowed.
  - No trusted devices have been configured.
- Mode 2. Exclusive bypass mode:
  - Neither LAN nor WLAN traffic is encrypted.
- Mode 3. Alternating bypass mode:
  - LAN traffic is encrypted using Approved algorithms and settings described below but WLAN traffic is not (or vice versa), and/or
  - 802.1x traffic and/or trusted devices have been configured.

The Approved modes of operation consist of allowed combinations of module configuration settings as follows:

Mode 1. MSP/rMSP Approved encrypting mode configuration requirements:

- On the “Endpoints” tab, the “All cards” option is set on the “Basic options” subtab.
- On the “Endpoints” tab, neither “Trusted device IP addresses” nor “802.1x traffic” options are set on the “Advanced options” subtab.

The “FIPS mode" indicator on the “Status” tab will read FIPS “Enabled” and the “All cards” option is set on the “Basic options” tab when the Client is operating in Mode 1

Mode 2. Exclusive bypass mode configuration configuration requirements:

- On the “Status” tab, the “No Encryption” profile is selected.

The “FIPS mode" indicator on the “Status” tab will read “Bypass” and the “Current profile” indicator on the “Status” tab will read “No Encryption” when the Client is operating in Mode 2.

Mode 3. Alternating bypass mode configuration requirements:

- On the “Endpoints” tab, the “All cards” option is not set on the “Basic options” subtab and there is both a LAN and WLAN card installed and/or
- On the “Endpoints” tab, either “Trusted device IP addresses” or “802.1x traffic” options are set on the “Advanced options” subtab

The “FIPS mode" indicator on the “Status” tab will read “Bypass” when the Client is operating in Mode 3.

5.4 Powering-Up and Operating the Module

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.

See the Fortress User Guide for information about how to perform module services in general.

5.5 Power-Up and Conditional Test

The following tables will detail each of the self tests that is run by the Secure Client.

Table 14: Power-Up Self Test

Power-Up Self Tests	Test Description	Error Conditions	Conditions to Exit
File Integrity Self Tests	During installation the packet driver binary, "fsvpndrvr.sys is loaded into memory and a SHA-256 Hmac is done using the Machine Hard Key. The resulting value is stored in the configuration database. Then when the Fortress Secure Client packet driver is loaded after powerup, the binary is again loaded into memory and another SHA-1 hmac is taken using the Machine Hard Key. If the results don't match, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state and a error message is written to the Windows log and is displayed as an error in the Client GUI.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
Triple-DES Self Test	A known input is injected into the Triple-DES engines and results are checked against a known answer. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state and an audit record is generated.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
AES (256 bit key) CBC Self Test	A known input is injected into the AES engines and results are checked against a known answers. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
HMAC-MD5 Self Test	A known input is injected into the HMAC-MD5 engines and results are checked against a known answers. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device

Power-Up Self Tests	Test Description	Error Conditions	Conditions to Exit
			passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
HMAC-SHA-1 Self Test	A known input is injected into the HMAC-SHA-1 engines and results are checked against a known answers. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state. The module needs to be uninstalled and then reinstalled before the network is serviceable again.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
HMAC-SHA-256 Self Test	A known input is injected into the HMAC-SHA-256 engines and results are checked against a known answers. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log and is displayed as an error in the Client GUI.	If the test fails the network interfaces are forced into a blocked state. The module needs to be uninstalled and then reinstalled before the network is serviceable again.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
HMAC-SHA-384 Self Test	A known input is injected into the HMAC-SHA-384 engines and results are checked against a known answers. If the results don't match the known answers, the test fails and the error description is logged in the Windows Event Log.	If the test fails the network interfaces are forced into a blocked state. The module needs to be uninstalled and then reinstalled before the network is serviceable again.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
HMAC-SHA-512 Self Test	A known input is injected into the HMAC-SHA-512 engines and results are checked against a known answers. If the results don't match the known answers, the test fails	If the test fails the network interfaces are forced into a blocked state. The module needs to be uninstalled and then reinstalled before the network is serviceable	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status"

Power-Up Self Tests	Test Description	Error Conditions	Conditions to Exit
	and the error description is logged in the Windows Event Log.	again.	tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
FIPS Non-Deterministic CPRNGT (Test of the entropy engine)	This checks to see if the CPRNGT generate the same random number in two consecutive numbers generated.	If a number read from the CPRGT is the same as the last number read it's an error	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
FIPS Deterministic X9.31 PRNG	A known answer test is performed a random number received for a known seed are compared	Random number does not match known answer the test fails.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client

Table 15: Conditional Self Test

Conditional Self Test	Test Description	Error Conditions	Conditions to Exit
Deterministic CRNGT (Entropy Engine)	The test will checks the first 8-byte block of every new random number with the old one.	If the test fails the network interfaces are forced into a blocked state and a error message is written to the Windows log and is displayed as an error in the Client GUI. Note: A failure of this test does not necessary mean a problem. It's statistically possible for the same random number to be generated.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
Non-deterministic CRNGT X9.31 PRNG	The module the X9.31 PRNG routine within FIPS.SYS. The test will checks the first 8-byte block of every new random number with the old one.	If the test fails the network interfaces are forced into a blocked state and a error message is written to the Windows log and is displayed as an error in the Client GUI. Note: A failure of this test does not necessary mean a problem. It's statistically possible for the same random number to be generated.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
Bypass Test that checks the integrity of the current configuration before loading a new one	A HMAC hash is taken using the HMAC key of the configuration file before a configuration changed is made, this is compared to the previously save hash. I f they equal everything is OK the new hash is saved in place of the old hash and the configuration change is allowed to happen. If they don't equal a FIPS error occurs.	If the test fails the network interfaces are forced into a blocked state and a error message is written to the Windows log and is displayed as an error in the Client GUI.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client
Bypass Test that performs a test encrypt/decrypt when a new configuration is loaded	The test sequences are listed here as required by FIPS. The main purpose of this testing is: • to make sure that under certain precise circumstances	If the test fails the network interfaces are forced into a blocked state and a error message is written to the Windows log and is displayed as an error in the Client GUI.	Log in as Windows administrator and clear FIPS error by clicking Reset FIPS button. The "Reset FIPS state" button appears beneath the error message on the "Status" tab for Cryptographic Officer only (only the error message is displayed for Users).then

Conditional Self Test	Test Description	Error Conditions	Conditions to Exit
	specific clear text packets would be allowed to pass through or around the crypto engine to their specified destinations • while other, encrypted packets would not. The BPM test sequences are: 1. Add a fictitious partner to the existing database. 2.Bring that partner to “MSP or rMSP state” 3. Create bogus packet destined for the fictitious partner. 4. Verify that the packet gets sent out encrypted to that partner. 5. Remove that partner from the database. 6. Make sure that the packets go out clear.		reboot device. If device passes all FIPS test the module will operate normally. If the Crypto Officer want to rerun the Power On Self Test he can click the "Reset FIPS state" button or the User must reboots the secure client

5.6 Identifying FIPS-Relevant Failures

When a FIPS-relevant error occurs, the Fortress Secure Client (a.k.a. the “module”) either generates an audit record (a.k.a. an “event message”) and sends it to the operating system audit trail for storage and operator (both User and Crypto Officer) review or outputs an error message to the “Status” tab, or both.

When the module generates audit records related to power-up self-tests (both software integrity self-test and cryptographic algorithm known-answer self-tests) and conditional self-tests and sends them to the Windows Event Log.

The module sends event messages to the Windows application log specifically. The application log contains events logged by the Fortress Secure Client application in general (i.e. it includes both FIPS-relevant messages and non-FIPS-relevant messages). The FIPS-relevant errors include as shown Table 11: Audit Logs.

Table 16: FIPS-relevant audit records

Event ID	Source	Type	Event Description
0xe100	FTIDrv	Informational	FIPS Message %1[14]
0xe101	FTIDrv	Error	FIPS Error %1
0xe102	FTIDrv	Warning	FIPS: Conditional X9.31 Self-test: Failed continuous random number generator test, regenerating a new number.
0xe103	FTIDrv	Warning	FIPS: Conditional X9.31 Self-test: failed seed test, regenerating the seed.
0xe104	FTIDrv	Error	FIPS: Conditional Entropy Self-test: Failed continuous random number generator test.
0xe105	FTIDrv	Error	FIPS: Conditional TRNG Self-test: Failed continuous random number generator test.
0xe106	FTIDrv	Error	FIPS Conditional db self-test failed
0xe107	FTIDrv	Error	FIPS Conditional bypass self-test failed
0xe108	FTIDrv	Informational	FIPS Conditional bypass self-test success
0xe109	FTIDrv	Error	FIPS Power up self-test FAILED Encryption Engine Test: Encountered fatal error.
0xe10a	FTIDrv	Error	FIPS Power up self-test FAILED Hash Engine Test: Encountered fatal error.
0xe10b	FTIDrv	Error	FIPS Power up self-test FAILED PRNG Test: Encountered fatal error.
0xe10c	FTIDrv	Error	FIPS Power up self-test FAILED entropy Test: Encountered fatal error.
0xe10d	FTIDrv	Error	FIPS Power up self-test FAILED KeyAgreement Test: Encountered fatal error.
0xe10e	FTIDrv	Error	Error generating hash during FIPS file integrity test for file %1.
0xe10f	FTIDrv	Error	FIPS File Integrity Test failed for file %1
0xe110	FTIDrv	Informational	FIPS File Integrity Test success for file %1
0xe111	FTIDrv	Error	FIPS Power up self-test FAILED File Integrity Test.
0xe112	FTIDrv	Error	FIPS Power up self-test FAILED.
0xe113	FTIDrv	Informational	FIPS Power up self-test success.
0xe114	FTIDrv	Informational	FIPS Power up Self-tests completed.

[14] This is the error code as shown in the next table.

Table 17: FIPS-relevant audit record error codes

Error Code (hex)[Note]	Event Description
0x30f000000	FIPS_GENERAL
0x30f000001	FIPS_ENGINE_NOT_FOUND
0x30f000002	FIPS_FAILED_ENTROPY_MATERIAL
0x30f000003	FIPS_FILE_INTEGRITY_TEST
0x30f000004	FIPS_stub2
0x30f000005	FIPS_TOO_SMALL
0x30f000006	FIPS_RESOURCE_ERROR
0x30f000007	FIPS_SEEDING_ERROR
0x30f000008	FIPS_FAILED_SEED_TEST
0x30f000009	PRNG_NOT_SEEDED
0x30f0000f1	SELFTEST_KEY_AGREEMENT
0x30f0000f2	SELFTEST_HMAC
0x30f0000f3	SELFTEST_HASH
0x30f0000f4	SELFTEST_ENCRYPTION
0x30f0000f5	SELFTEST_X931PRNG
0x30f0000f6	SELFTEST_SEEDMGR
0x30f0000f9	SELFTEST_BYPASS
0x30f0000fA	SELFTEST_DH_KEY
0x30f0000fB	SELFTEST_ENTROPY
0x30f0000fC	SELFTEST_UNIQUESERIALNO
0x30f0000fD	SELFTEST_MIC
0x30f0000fE	SELFTEST_X931_CONDITIONAL
0x30f0000ff	SELFTEST_TRNG_CONDITIONAL

Operators (both User and Crypto Officer) can view event messages generated by the module using the Windows Event Viewer as follows:

1. Click Start, and then click Control Panel. Click Performance and Maintenance, then click Administrative Tools, and then double-click Computer Management. Or, open the MMC containing the Event Viewer snap-in.
2. In the console tree, click Event Viewer. The Application, Security, and System logs are displayed in the Event Viewer window.

How to View Event Details:

1. Click Start, and then click Control Panel. Click Performance and Maintenance, then click Administrative Tools, and then double-click Computer Management. Or, open the MMC containing the Event Viewer snap-in.
2. In the console tree, expand Event Viewer, and then click the log that contains the event that you want to view.

3. In the details pane, double-click the event that you want to view. The Event Properties dialog box containing header information and a description of the event is displayed.

How to identify FIPS-relevant events:

FIPS-relevant log entries are classified by type, and contains a description of the event as follows:

- Date – The date the event occurred.
- Time – The time the event occurred.
- User – The user name of the user (User or Crypto Officer operator) that was logged on when the event occurred.
- Computer – The name of the computer where the event occurred.
- Event ID – An event number that identifies the event type. Event IDs corresponds to FIPS-relevant errors are listed in the table below.
- Source – The source of the FIPS-relevant errors will always be “FTIDrv”.
- Type – The type of event. Event types corresponding to FIPS-relevant errors are listed in the table below.
- Category – FIPS-relevant log entries do not include “Category” fields.

FIPS-relevant errors include as what is shown in the table above.

5.7 Performing Zeroization

Ephemeral keys and CSPs are zeroized generally speaking when MSP sessions end and MSP key exchanges occur, and when the power is cycled, as described in section “Cryptographic Key Management”.

Persistent keys and CSPs as identified in section “Cryptographic Key Management” require the hard drive to be formatted.

To zeroize all keys and CSPs, format the hard drive and reboot. Both steps are required given the module loads and starts operating without operator intervention after the Windows kernel loading boot phase completes.

5.8 CAC Suport

The Common Access Card (CAC) is a United States Department of Defense (DoD) smart card issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD other government employees and State Employees of the National Guard and eligible contractor personnel.

Even through the CAC is supported by this version of Fortress Client software it should not be used in the FIPS mode of operation. The CAC was not submitted for FIPS testing.

6.0 Contacting Fortress

6.1 Installation

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.

6.2 Support and Service

Any issues concerning support or if help is needed contact:

Fortress Technologies, Inc

4023 Tampa Road, Suite 2000

Oldsmar, Florida 34677

Tel: 813 288-7388

Or access the web site at http://www.fortresstech.com/

End of document