Secure File Transfer Appliance
Security Policy

Document *Version 1.8*

Accellion, Inc.

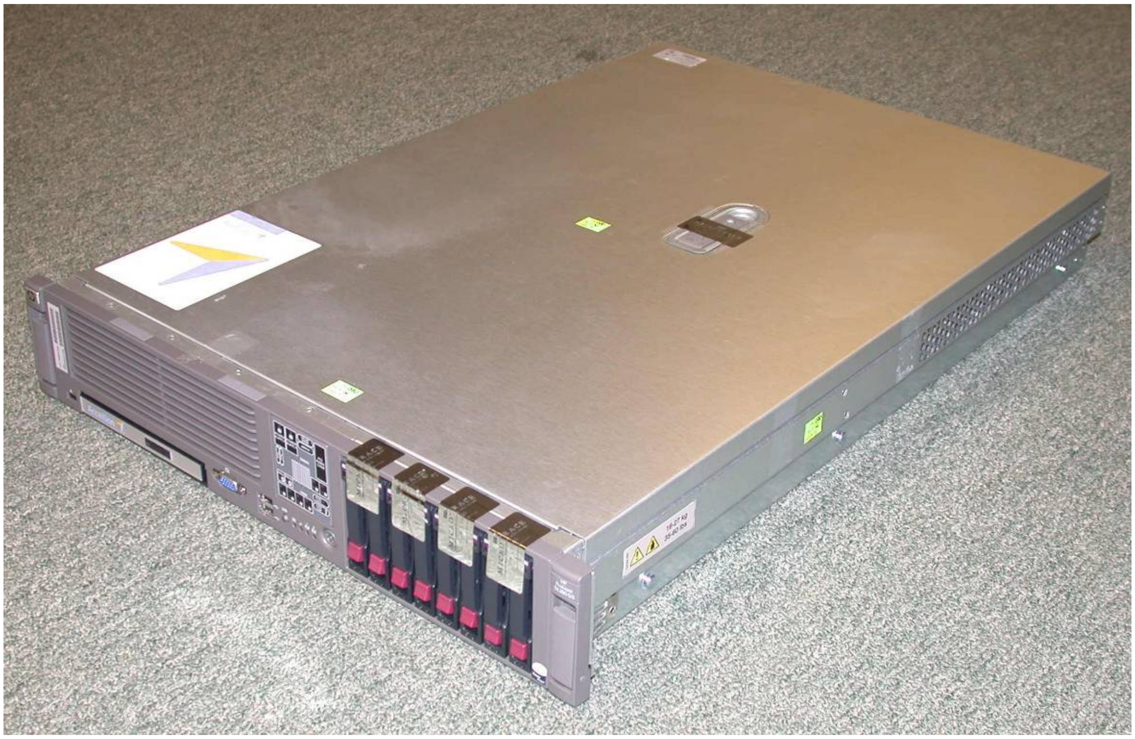
July 29, 2009

TABLE OF CONTENTS

1. Module Overview

The Accellion Secure File Transfer Appliance (HW P/N ACFIPS-01 Version 1.0.0; FW Version FTA_8_0_3) is a multi-chip standalone cryptographic module as defined in the FIPS 140-2 standard. The cryptographic boundary is the external surface of the hard, opaque, commercial grade metal case. The primary purpose for this device is to provide data security for file transfers.

Figure 1 – Image of the Cryptographic Module



2. Security Level

The Secure File Transfer Appliance cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

The Secure File Transfer Appliance cryptographic module only supports a FIPS Approved mode of operation; it is placed into FIPS mode when initialized with a valid license key. The user can determine if the cryptographic module is running in FIPS mode via execution of the "Show Status" service.

Approved mode of operation

The Secure File Transfer Appliance module supports the following FIPS Approved algorithms:

- AES ECB mode with 128 bit keys for decryption of the file (Cert. #843)
- AES CBC mode with 128 bit keys for decryption of the license (Cert. #844)
- AES CBC mode with 128 and 256 bit keys for encryption and decryption in the TLS (Cert. #845)
- TDES TCBC mode for encryption and decryption in the TLS (Cert #771)
- HMAC SHA-1 for message authentication (Cert. #468)
- DSA with 1024 bit keys for digital signature verification (Cert. #307)

- SHA-1 for hashing (used with TLS implementation) (Cert. #836)
- SHA-1 for hashing (used with HMAC implementation) (Cert. #835)
- SHA-1 for hashing (used with DSA implementation) (Cert. #842)

The Secure File Transfer Appliance module supports the following FIPS allowed algorithms and protocols:

- TLS/SSL 3.1 for secure communications and key establishment
- NDRNG to generate passwords (2 implementations, one for PHP and one for Perl)
- AES key wrap per the AES Key Wrap Specification (Cert. #845, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)
- Triple-DES (Cert. #771, key wrapping; key establishment methodology provides 80 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

The Secure File Transfer Appliance module supports the following non-FIPS Approved algorithms which do not support any security relevant operations:

- Blowfish for encryption
- MD5 for hashing

4. Ports and Interfaces

The Secure File Transfer Appliance module provides the following physical ports and logical interfaces:

- Two 10/100/1000 Ethernet ports: data input, data output, control input, status output
- Serial port (RS232-C): not used, disabled
- Keyboard port: control input
- Mouse PS/2 port: control input
- Two Video ports: status output
- Four USB ports: control input
- 10/100 Ethernet (for Integrated Lights Out Management (HP model)): control input, status output (Note: A tamper label covers this port)
- PCI Express slots: not used, disabled (protected by metal)
- Power port(s): power input

5. Identification and Authentication Policy

The Secure File Transfer Appliance module shall support three distinct operator roles (User, Cryptographic Officer and Accellion Support). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. An operator must enter a username and its password or possess the Accellion Support DSA key to log in. For the User role and the Cryptographic Officer role, the username is an alphanumeric string of 1 to 15 characters. For the Accellion Support role, the username is an alphanumeric string of 8 characters. The passwords are an alphanumeric string of minimum 6 characters randomly chosen from the 94 ASCII characters. Upon correct authentication, the role is selected based on the username of the operator.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Username and Password
Cryptographic Officer	Identity-based operator authentication	Username and Password
Accellion Support	Identity-based operator authentication	1024-bit DSA key

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/ 94^6 which is less than 1/1,000,000. Passwords are a minimum length of 6 characters from a pool of 94 possible characters (i.e., printable characters only). The probability of successfully authenticating to the module within one minute is 1/ (94^6/5) which is less than 1/100,000. The module can be configured to a specified number of unsuccessful attempts.
1024 bit DSA Key	The probability that a random attempt will succeed or a false acceptance will occur is 1/ 2^80 which is less than 1/1,000,000. The DSA key provides 80 bits of encryption strength and the processing capabilities of the module aren't sufficient to support the number of attempts required to correctly guess the key in less than one minute.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	• Decrypt Data: This service AES decrypts ciphertext data passed into the cryptographic module using the AES 128 File Decryption Key. • File Transfer: This service transfers the requested file over an SSL 3.1 or TLS connection. • Administer Account: This service allows the user to change the settings on his/her own account. • Establish Connection: This service allows an SSL 3.1 or TLS connection to be established. • Disconnect: This service allows an SSL 3.1 or TLS connection to end.
Cryptographic Officer:	• Administer Users: User account maintenance. • Administer Module: Configure the module such as network settings, file management settings, etc. • Establish Connection: This service allows an SSL 3.1 or TLS connection to be established. • Disconnect: This service allows an SSL 3.1 or TLS connection to end. • Show Status: Provide status information for the module. • Firmware Loads: Load new firmware updates into the module. • File Management: Delete and replicate files. • Shutdown/restart: Shutdown the module or restart to run self-tests. • Enable Organizational File Download: Allow download links to be forwarded to users for download within an organization following authentication. • Enable Non-Confidential Delivery: Allow anonymous file downloads.

Role	Authorized Services
	• Zeroize: Wipe all secret and private keys and CSPs from the module's hard disk and volatile memory. • ALCS: Configure the module to act in a clustering mode with another module.
Accellion Support:	• Administration Functions: Support administration and configuration.

Unauthenticated Services:

The Secure File Transfer Appliance module supports the following service that does not require an operator to assume an authorized role:

- Self-Tests: Automatically runs the self-tests necessary for FIPS 140-2.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Key Encryption Key (KEK): This is an AES 128 bit key used for encryption/decryption of AES 128 file decryption key.
- License Key: This is an AES 128 key used to decrypt the license file.
- Accellion TLS Key: This key is used for TLS connections (the factory shipped 1024 bit RSA key is replaced by the customer).
- Customer TLS Key: This key is used for TLS connections, 1024 bit RSA key.
- TLS Session Key: TDES or AES 128/256 bit key used in TLS session.
- File Decryption Key: This is an AES 128 key used to decrypt a file stored on the Secure File Transfer Appliance's hard disk.
- HMAC Key: This key is used by the login API.
- CO Password: Used to authenticate the CO.
- User Password: Used to authenticate the User.

Definition of Public Keys:

The following are the public keys contained in the module:

- RSA Public Key: Checks the signature of the license.
- RSA Public Key – TLS: 1024 bit RSA key used in TLS which can be replaced by the

customer.

- DSA Public Key for Firmware Load: A DSA 1024 bit key used to authenticate firmware loads.
- DSA Accellion Support Public Key: A DSA 1024 bit key used to authenticate the Accellion Support role.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Use (U): This operation uses the identified CSP.
- Store (S): This operation stores the identified CSP into persistent storage.
- Zeroize (Z): This operation actively overwrites the identified CSP.

Table 5 – CSP Access Rights within Roles & Services

Role			Service	CSPs							
User	Crypto Officer	Accellion Support		Key Encryption Key	License Key	Accellion/Customer TLS Key	TLS session key	File Decryption Key	HMAC Key	Crypto Officer Password	User Password
X			Decrypt Data	U		U	U	U			
X			File Transfer	U		U	U				
X			Administer Account			U	U			U, S	U, S
X	X		Establish Connection			U	U		U	U	U
X	X		Disconnect								
	X		Administer Users		U	U	U			U, S	S
	X		Administer Module		U	U,S	U			U	
	X		Show Status		U	U	U			U	
	X		Firmware Loads		U	U	U			U	
	X		File Management			U	U			U	
	X		Shutdown/restart		U	U	U			U	

Role			Service	CSPs							
User	Crypto Officer	Accellion Support		Key Encryption Key	License Key	Accellion/Customer TLS Key	TLS session key	File Decryption Key	HMAC Key	Crypto Officer Password	User Password
	X		Enable Organizational File Downloads		U	U	U			U	
	X		Enable Non-Confidential Delivery		U	U	U			U	
	X		ALCS			U	U		S	S, U	S
	X		Zeroize	Z	Z	Z	Z	Z	Z	Z	Z
		X	All Administration Functions								

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Secure File Transfer Appliance does not contain a modifiable operational environment.

8. Security Rules

The Secure File Transfer Appliance cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide the following distinct operator roles:
   - User role
   - Cryptographic Officer role
   - Accellion Support role

   The Accellion Support role exists to facilitate troubleshooting and diagnostic activities for customers that elect this service.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. When the cryptographic module is powered cycled, any authenticated operators must reauthenticate to the module to re-enter their desired role.

5. The cryptographic module shall encrypt message traffic using the TLS/SSL3.1 algorithm.
6. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. AES ECB decryption KAT (for decryption of the file)
      b. AES CBC decryption KAT (for decryption of the license) (2 tests)
      c. AES CBC encryption/decryption KAT (for encryption/decryption in TLS) (2 tests)
      d. TDES KAT (used with TLS implementation)
      e. HMAC SHA-1 KAT
      f. DSA verify KAT
      g. SHA-1 KAT (used with TLS implementation)
      h. SHA-1 KAT (used with HMAC implementation)
      i. SHA-1 KAT (used with DSA implementation)
   2. Firmware Integrity Test – EDC used
   3. Critical Functions Tests: None

   B. Conditional Self-Tests:

   1. NDRNG Continuous RNG Test (used with PHP)
   2. NDRNG Continuous RNG Test (used with Perl)
   3. Firmware Load Test using DSA with SHA-1
7. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
8. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

This section documents the security rules imposed by the vendor:

1. Presently, the module will support a maximum of 200 concurrent individual users. Tens of thousands may be defined on the appliance.
2. If the cryptographic module remains inactive for the Cryptographic Officer role for a configurable timeout period (maximum period of 60 minutes), the module shall automatically log-out the operator. If the cryptographic module remains inactive for the User role for a maximum period of 180 minutes, the module shall automatically log-out

the operator.

3. The module enforces a timed access protection mechanism that supports a pre-configurable number of unsuccessful authentication attempts. After those configured number of consecutive unsuccessful Password validation attempts have occurred, the cryptographic module shall enforce a wait period (configurable) before any more login attempts can be attempted. This wait period shall be enforced even if the module power is momentarily removed. Note that it is advised that the number of unsuccessful authentication attempts should not exceed five attempts.

9. Physical Security Policy

Physical Security Mechanisms

The Secure File Transfer Appliance multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure with tamper evident seals
- Protected vents

The following excluded components are non-security relevant:

- Removable power supplies in the rear of the module
- Power regulator components in the power supply bay

Operator Required Actions

The Cryptographic Officer is required to periodically inspect the tamper evident seals, enclosure, and vents. If suspicious markings are found, it is encouraged that the cryptographic module be zeroized and returned to the manufacturer; the Cryptographic Officer should assume that the cryptographic module has been fully compromised and must abide by the restrictions required by the Cryptographic Officer's organizational security policy.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	As specified per end user policy.	Visually inspect the labels for tears, rips, dissolved adhesive, and other signs of malice.
Opaque enclosure	As specified per end user policy.	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Protected vents	As specified per end user policy.	Visually inspect the vents for tears, bent baffles, and other signs of tampering on the dust filters or vents themselves.

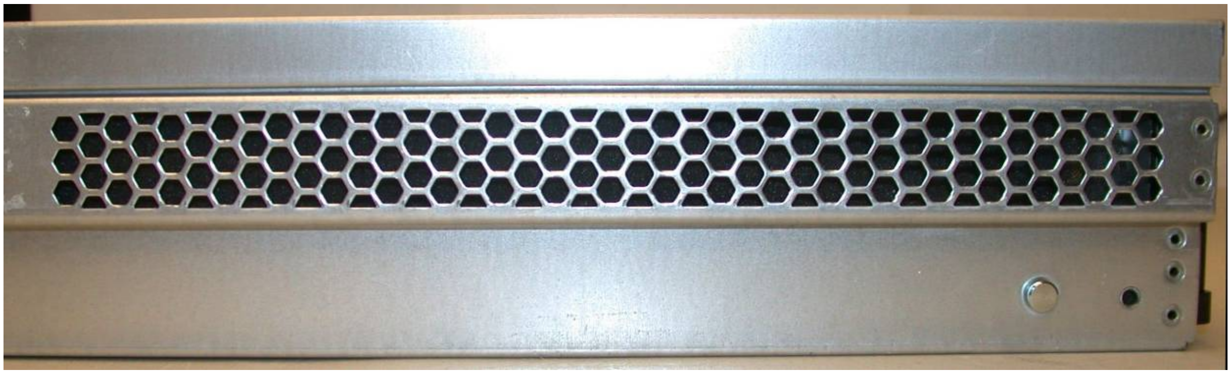


Figure 2: Right Vent Dust Filter Placement

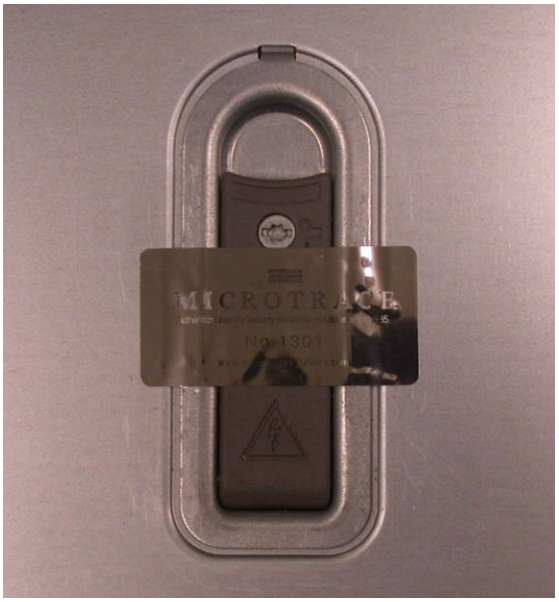


Figure 3: Tamper Evident Seal on Top Cover Latch

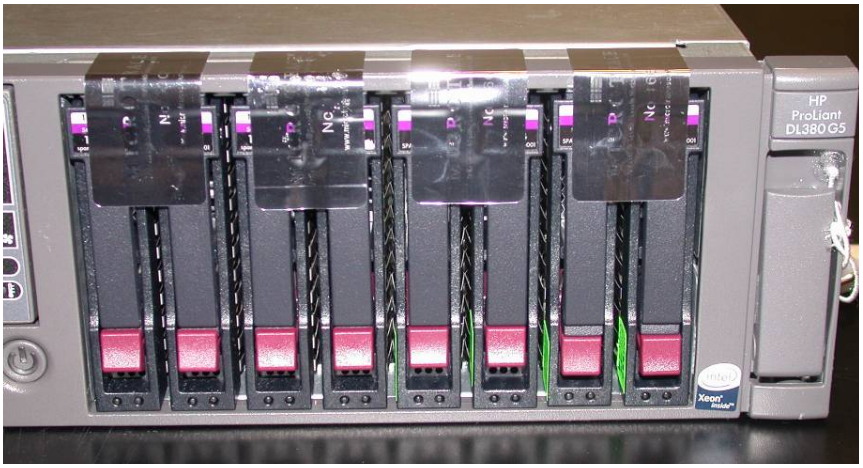


Figure 4: Tamper Seals over Front Hard Drives

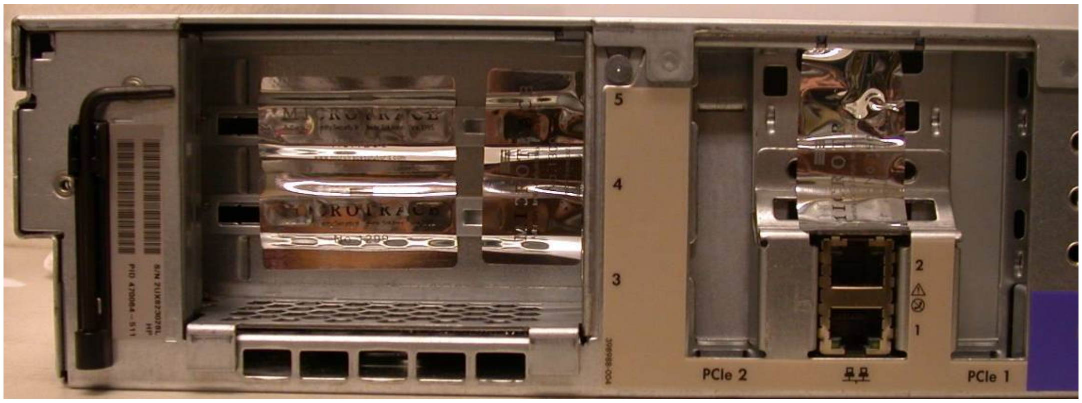


Figure 5: Rear Tamper Seals

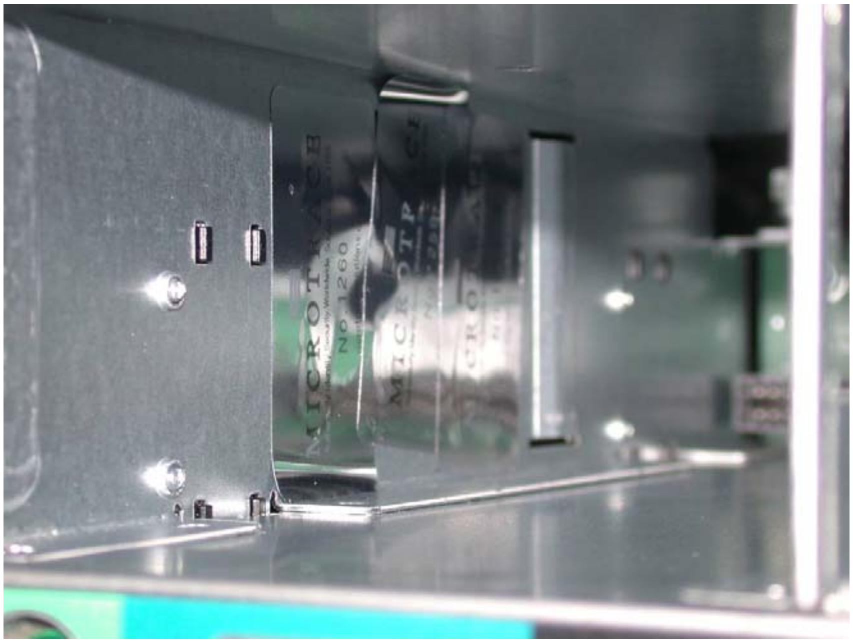


Figure 6: Tamper Seals inside Left Power Supply Slot

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks outside of the scope of FIPS 140-2.

11. Definitions and Acronyms

AES	Advanced Encryption Standard
ALCS	Accellion Local Cluster Service
API	Application Program Interface
CO	Cryptographic Officer
CSP	Critical Security Parameter (as defined in FIPS 140-2)
DES	Data Encryption Standard
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
MD5	Message-Digest Algorithm 5
NDRNG	Nondeterministic Random Number Generator
RNG	Random Number Generator
RPM	Red Hat Package Manager
RSA	Rivest, Shamir and Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus