Accellion Cryptographic Module Security Policy

Document *Version 2.7*

Accellion, Inc.

September 12, 2014

TABLE OF CONTENTS

1. Module Overview

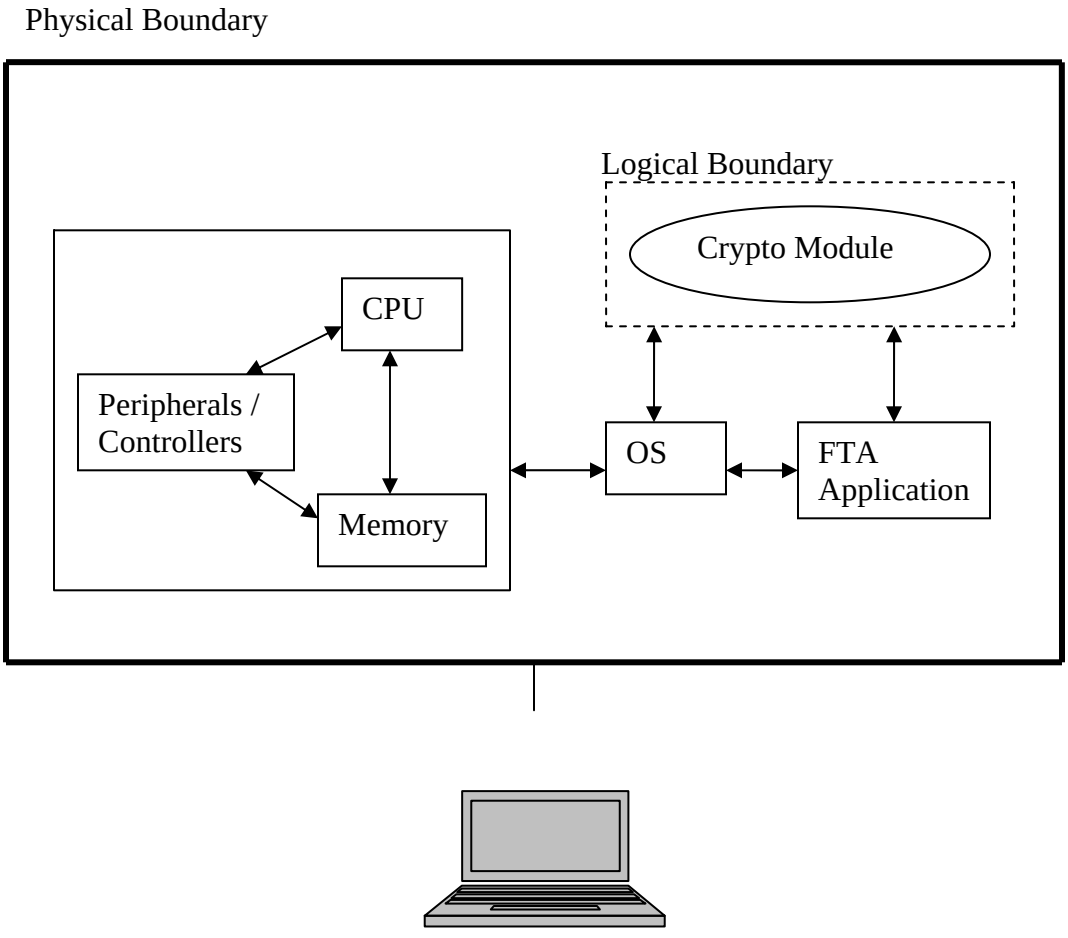
The Accellion Cryptographic Module (SW Version FTALIB_3_0_1) is a software only module that operates in a multi-chip standalone embodiment, as defined in the FIPS 140-2 standard. The physical boundary is defined as being the outer perimeter of the general purpose computer on which the software module is installed. The logical boundary is defined as the collection of the shared libraries which are as follows:

- PERL AES Library: Rijndael.so [Version: 0.05]
- PHP AES Library: libmcrypt.so.4.4.7 [Version: 2.5.7]
- TLS Library: libcrypto.so.1.0.0 [Version: 1.0.1c1]
- Core PHP Library: libphp5.so [Version: 5.2.17]
- Utils Binary: fips_utils [Version: 2.0]

The Accellion Cryptographic Module implements OpenSSL 1.0.1c1 which has been compiled with the flag -DOPENSSL_NO_HEARTBEATS to properly handle Heartbeat Extension packets (as described at https://www.openssl.org/news/secadv_20140407.txt). This Module is not susceptible to the Heartbleed vulnerability.

The primary purpose for this device is to provide data security for file transfers and sharing.

Figure 1 – Block Diagram of the Cryptographic Module



2. Security Level

The Accellion Cryptographic Module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

The Accellion 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 the license page.

Approved mode of operation

The Accellion Cryptographic Module supports the following FIPS Approved algorithms within the libraries:

PERL AES Library

- AES ECB mode with 128 and 256 bit keys for decryption of the file (Cert. #2317)

PHP AES Library

- AES CBC mode with 128 and 256 bit keys for encryption and decryption. Used for decryption of the license, encryption/decryption of the administrator session, and other general encryption/decryption (Cert. #2318)

TLS Library

- AES CBC mode with 128 and 256 bit keys for encryption and decryption in TLS (Cert. #2844)
- Triple-DES TCBC mode using 3-keys for encryption and decryption in TLS (Cert # 1700)
- HMAC-SHA-1 and HMAC-SHA-256 for MAC and key derivation in TLS (Cert. #1783)
- SHA-1 and SHA-256 for hashing and key derivation in TLS (Cert. #2385)
- CVL SP 800-135 TLSv1.0/v1.1/v1.2 KDF for deriving TLS Session Keys (Cert. #268)
- FIPS 186-2 RSA with 1024 bit keys for digital signature verification (Cert. #1485)

Core PHP Library

- HMAC-SHA-1 for API token authentication (Cert. #1436)
- SHA-1 for hashing and within HMAC (Cert. #2004)

The module supports the following FIPS allowed algorithms and protocols:

- TLS v1.0/SSL v3.1 and TLS v1.1 for secure communications and key establishment (acting as client or server) with the following cipher suites:
    - TLS_RSA_WITH_AES_128_CBC_SHA (with RSA modulus >=2048 bits)
    - TLS_RSA_WITH_AES_256_CBC_SHA (with RSA modulus >=2048 bits)
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA (with RSA modulus >=2048 bits)
- TLS v1.2 for secure communications and key establishment (acting as client or server) with the following cipher suites:
    - TLS_RSA_WITH_AES_128_CBC_SHA256 (with RSA modulus >=2048 bits)
    - TLS_RSA_WITH_AES_256_CBC_SHA256 (with RSA modulus >=2048 bits)
- AES key wrap per the AES Key Wrap Specification (Cert. #2844, key wrapping; key establishment methodology provides 128 bits of encryption strength)
- Triple-DES (Cert. #1700, key wrapping; key establishment methodology provides 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 to 256 bits of encryption strength)
- SSH v2 (no security is claimed)
- MD5 within TLS key derivation (as allowed per IG D.9)

The module supports the following non-FIPS Approved algorithm which does not support any security relevant operations:

- MD5 for hashing (no security claimed)

4. Ports and Interfaces

The physical ports of the module are provided by the general purpose computer on which the module is installed. The module supports the following logical interfaces: data input, data output, control input, and status output. The data input interface consists of the input parameters of the shared libraries' functions. The data output interface consists of the output parameters of the shared libraries' functions. The control input interface consists of the actual functions of the shared libraries. The status output interface includes the return values of the functions of the shared libraries.

5. Identification and Authentication Policy

The Accellion Cryptographic Module supports two distinct operator roles (User, Cryptographic Officer). In compliance with FIPS 140-2 Level 1 standards, the module does not support user authentication for those roles. However, only one role may be active at a time and the module does not allow concurrent operators.

The User and Cryptographic Officer roles are implicitly assumed by the entity accessing services implemented by the module.

User Role: Initialize the module and perform any of the module services. This role has access to all of the services provided by the module.

Cryptographic Officer Role: Installation of the module on the host computer system.

6. Access Control Policy

Roles and Services

Table 2 – Services Authorized for Roles

Role	Authorized Services
User:	Symmetric encryption/decryption: This service provides encryption/decryption functionality for AES and Triple-DES ciphers. AES key wrapping for key transport: This service provides key wrapping functionality for file decryption key. RSA key wrapping for key transport: This service provides key wrapping functionality for TLS connection. Digital signature: This service provides functionality to verify digital signatures. Keyed Hash (HMAC): This service provides keyed hash functionality using HMAC-SHA1 or HMAC-SHA-256. Message Digest (SHS): This service provides functionality to generate message digests using SHA-1 or SHA-256.

Role	Authorized Services
Cryptographic Officer	Module Installation: Install the module on the host computer system

The following services are available to any operator without assuming an authorized role:

Self-Tests: On bootup of the host GPC and/or module instantiation, automatically runs the self-tests necessary for FIPS 140-2.

Zeroization: All the CSPs can be zeroized through Accellion's Secure File Transfer application.

Show Status: The operator can obtain the current status of the module.

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 the File Decryption Key.
- License Key: This is an AES 256 bit key used to decrypt the license file.
- Session Key: This is an AES 256 bit key used to encrypt/decrypt administrator session.
- Accellion TLS Key: This is a RSA 2048 bit private key used for TLS connections. This key is shipped from the factory and is to be replaced by the Customer TLS Key.
- Customer TLS Key: This is a RSA 2048 to 16384 bit private key used for TLS connections. This key is loaded by the customer and replaces the Accellion TLS Key.
- TLS Session Keys: The set of ephemeral Triple-DES or AES 128/256 and HMAC keys created for each TLS session.
- File Decryption Key: This is an AES 128 or 256 bit 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 through an API based authentication. This is one of the available authentication modes.
- HMAC Software Integrity Key: This key is used to calculate the HMAC-SHA1 digest of the module which is then used in the software integrity test.

Definition of Public Keys:

The following are the public keys contained in the module:

- RSA Public Key: This is a RSA 1024 bit public key used to check the signature of the license. (Note: 1024 bit modulus is still allowed for legacy use with signature verification).
- RSA Public Key – TLS: This is a RSA 2048 to 16384 bit public key used in TLS which

can be replaced by the customer.

- Third Party RSA Public Keys – TLS: This is a RSA 2048 to 16384 bit public key which is sent from third party users and used in TLS communications.

Definition of CSPs/Public Key Modes of Access

Table 3 defines the relationship between access to CSPs/Public Keys and the different module services. The modes of access shown in the table are defined as follows:

- Generate (G): This operation generates the identified CSP.
- Use (U): This operation uses the identified CSP.
- Input (I): This operation receives the identified CSP from outside the GPC.
- Output (O): This operation outputs the identified CSP outside of the GPC.
- Zeroize (Z): This operation actively overwrites the identified CSP.

Table 3 – CSP/Public Key Access Rights within Roles & Services

Service	Key Encryption Key	License Key	Session Key	Accellion TLS Key	Customer TLS Key	TLS Session Keys	File Decryption Key	HMAC Key	HMAC Software Integrity Key	RSA Public Key	RSA Public Key - TLS	Third Party RSA Public Keys – TLS
Symmetric encryption/decryption	U	U	U		I	U	UIO	I			I	I
AES Key Wrapping for key transport	U						IO					
RSA Key wrapping for key transport				U	U	U					U	U
Digital signature										U		
Keyed Hash (HMAC)						G		U				
Message Digest (SHS)												
Module Installation	U	U	U	U	U	U	U	U	U	U	U	
Self-Tests									U			

Service												
Zeroization	Z	Z	Z	Z	Z	Z	Z	Z	Z			
Show Status												

7. Operational Environment

The Accellion Cryptographic Module is a software module that runs on an underlying modifiable operational environment and is installed on a general purpose computer. The module is composed of the shared libraries described in Section 1 above.

When a crypto module is implemented in Accellion's SFTA environment, the SFTA application is the user of the cryptographic module. The SFTA application makes the calls to the cryptographic module. Therefore, the SFTA application is the single user of the cryptographic module, and satisfies the FIPS 140-2 requirement for a single user mode of operation, even when the SFTA application is serving multiple clients.

The Accellion Cryptographic Module has been tested on Red Hat Enterprise Linux 5.

8. Security Rules

The Accellion 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 1 module.

1. The cryptographic module shall provide the following distinct operator roles:
   - User role
   - Cryptographic Officer role
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall encrypt message traffic using the TLS v1.0/SSL v3.1, TLS v1.1, or TLS v1.2 protocol.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:

      PERL AES Library

         a. AES ECB decryption KATs (for decryption of the file) (2 tests for both 128 bit and 256 bit)

      PHP AES Library

         b. AES CBC encryption/decryption KATs (for decryption of the license, encryption/decryption of the administrator session, and other general encryption/decryption) (2 tests)

      TLS Library

         c. AES CBC encryption/decryption KATs (for encryption/decryption in TLS) (2 tests)

         d. Triple-DES encryption/decryption KAT (used with TLS implementation)

e. HMAC-SHA-1 and HMAC-SHA-256 (used with TLS implementation)

f. SHA-1 and SHA-256 KAT (used with TLS implementation)

g. SP 800-135 TLS KDF KAT (used with TLS implementation)

h. RSA verify KAT (used with TLS implementation)

Core PHP Library

i. HMAC-SHA-1 KAT (for API token authentication)

j. SHA-1 KAT (used with HMAC implementation)

Utils Binary

k. AES Key Wrap KAT

l. AES Key Unwrap KAT

2. Software Integrity Test – HMAC-SHA-1

3. Critical Functions Tests: None

B. Conditional Self-Tests: None.

5. 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. If a self-test fails, the module provides the following error: "Failed FIPS test when running. Go to FIPS error state." The module is then uninstalled and the GPC is rebooted.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. Third party clients using this module shall restrict their TLS ciphers suites to those listed in Section 3 of this document.
8. Third party clients using this module shall restrict their TLS RSA modulus to be >=2048 bits.
9. Customer TLS Keys used to replace the Accellion TLS Key shall be restricted to RSA with a modulus >= 2048 bits.

9. Physical Security Policy

The Accellion Cryptographic Module is a software module intended for use with Red Hat Enterprise Linux 5; therefore, the physical security requirements of FIPS 140-2 are not applicable.

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
API	Application Program Interface
CO	Cryptographic Officer
CSP	Critical Security Parameter (as defined in FIPS 140-2)
DES	Data Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
MD5	Message-Digest Algorithm 5
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman Algorithm
SFTA	Secure File Transfer Appliance
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
Triple-DES	Triple-Data Encryption Standard (Algorithm)
TLS	Transport Layer Security