FIPS 140-2 Non-Proprietary Security Policy

McAfee Email Gateway for Virtual Environments 7.0.1

Document Version 1.5

August 11, 2014

Prepared For:

McAfee, Inc.

2821 Mission College Blvd

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the Email Gateway for Virtual Environments 7.0.1.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment Canada (CSEC) jointly run the Cryptographic Module Validation Program (CMVP). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates test reports for all cryptographic modules pursuing FIPS 140-2 validation. *Validation* is the term given to a cryptographic module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Email Gateway for Virtual Environments 7.0.1 from McAfee provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The McAfee Email Gateway for Virtual Environments 7.0.1 may also be referred to as the "module" in this document.

1.3 External Resources

The McAfee website (http://www.mcafee.com) contains information on the full line of products from McAfee, including a detailed overview of the Email Gateway for Virtual Environments 7.0.1 solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2014.htm) contains links to the FIPS 140-2 certificate and McAfee contact information.

1.4 Notices

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
MEG	McAfee Email Gateway
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1-1 – Acronyms and Terms

2 McAfee Email Gateway for Virtual Environments 7.0.1

2.1 Product Overview

McAfee Email Gateway integrates comprehensive inbound threat protection with outbound data loss prevention, advanced compliance, performance reporting, and simplified administration. By combining local network information with global reputation intelligence from McAfee Global Threat Intelligence, it provides the most complete protection available against inbound threats, spam and malware. Its sophisticated content scanning technologies, multiple encryption techniques, and granular, policy-based message handling prevent outbound data loss and simplify compliance. Administrators have the flexibility they need to create policies to fit their business, increasing the solutions performance. A single management console with enterprise-class logging and reporting capabilities simplifies administration and compliance workloads to significantly reduce costs.

More information on the McAfee Email Gateway solution can be found at http://www.mcafee.com/us/products/email-gateway.aspx.

2.2 Cryptographic Module Specification

The module is the McAfee Email Gateway for Virtual Environments 7.0.1. The module is a software-only multi-chip standalone module installed on a General Purpose Computer running a General Purpose Operating System.

Once configured for FIPS mode of operation (see the Guidance and Secure Operation section), the module cannot be placed into a non-FIPS mode.

The physical boundary is pictured in the images below:

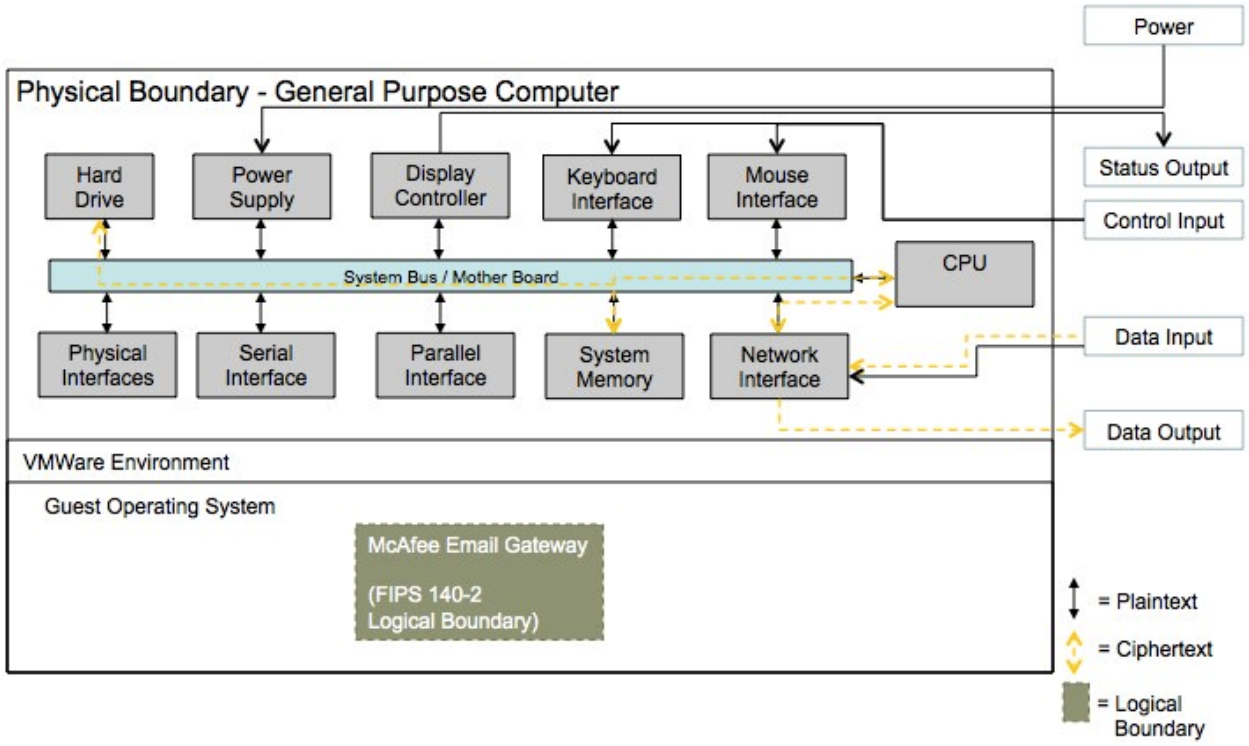

Figure 1 – Physical Boundary

2.3 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	3
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Validation Level	**1**

Table 2-1 – Validation Level by DTR Section

The “Mitigation of Other Attacks” section is not relevant as the module does not implement any countermeasures towards special attacks.

2.4 Cryptographic Algorithms

2.4.1 Algorithm Implementation Certificates

The modules' cryptographic algorithm implementations[1] have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048-bit	ANSI X9.31	1041	Sign operation
	RSA 1024, 1536, 2048-bit	ANSI X9.31	1041	Verify operation
	DSA 1024-bit	FIPS 186-2	638	Verify operation
Hashing	SHA-1, SHA-256	FIPS 180-2	1762	Hashing
Keyed Hash	HMAC-SHA1	FIPS 198	1217	Message verification Message digest Module integrity
Symmetric Key	TDES (3-Key) CBC	FIPS 46-3	1298	Data encryption / decryption
	AES (CBC with 128bit keys)	FIPS 197	2012	Data encryption / decryption
Random Number Generation	X9.31	X9.31 (AES)	1054	Random Number Generation

Table 2-2 – FIPS-Approved Algorithm Certificates for OpenSSL Implementation ("Implementation A")

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048, 3072, 4096-bit	FIPS 186-2	1074	Sign operation
	RSA 1024, 1536, 2048, 3072, 4096-bit	FIPS 186-2	1074	Verify operation
	DSA 1024-bit	FIPS 186-2	654	Verify operation
Hashing	SHA-1, 224, 256, 384, 512	FIPS 180-2	1809	Hashing
Keyed Hash	HMAC SHA-1, 224, 256, 384, 512	FIPS 198	1260	Message verification Message digest
Symmetric Key	TDES (3-Key) TECB, TCBC, TCFB	FIPS 46-3	1330	Data encryption / decryption
	AES (128,192,256) ECB, CBC and CFB128	FIPS 197	2079	Data encryption / decryption

[1] Please note that the standards for each algorithm are listed with the respective CAVP certificate.

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Random Number Generation	X9.31	X9.31 (AES)	1077	Random Number Generation

Table 2-3 – FIPS-Approved Algorithm Certificates for OpenPGP Implementation ("Implementation B")

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA 2048-bit	X9.31, PKCS#1 V.1.5	1171	Sign / verify operations
	DSA 1024-bit	FIPS 186-2	710	Verify operation
Hashing	SHA-1, SHA-256	FIPS 180-3	1962	Digital signature generation and verification (SHA-256) Verification of legacy data (SHA-1) User password hashing
Random Number Generation	FIPS 186-2 PRNG (Change Notice 1- with and without the mod q step)	FIPS 186-2	1133	Random Number Generation
Symmetric Key	AES 128-bit and 256-bit in CBC and ECB mode	FIPS 197	2280	Data encryption/ decryption
	TDES (3-key) CBC mode	FIPS 46-3	1428	Decryption of legacy data

Table 2-4 – FIPS-Approved Algorithm Certificates for McAfee Agent Implementation ("Implementation C")

The module is comprised of three different crypto libraries associated with functions from specific calling daemons. OpenSSL handles Crypto Officer and general crypto functions, OpenPGP handles Email Gateway to Email Gateway communication encryption, and McAfee Agent handles communications for host platform firmware updates.

Note the use of DSA/RSA 1024-bit and 1536-bit verify operations are for legacy use in accordance with FIPS 140-2 IG-G.14 and SP 800-131A transition tables. Use of SHA-1 hashing for digital signature verification of data is for legacy use and SHA-1 hashing for digital signature generation is disallowed in accordance with FIPS 140-2 IG-G.14 and SP 800-131A transition tables.

2.4.2 Non-Approved Algorithms

The module implements the following non-FIPS approved algorithms:

- Software-based random number generator
    - This RNG is used only as a seeding mechanism to the FIPS-approved PRNG.

- Diffie-Hellman
    - Key agreement; key establishment methodology provides 112-bits of encryption strength (allowed for use in FIPS mode of operation).
    - Key agreement; key establishment methodology provides less than 112-bits of encryption strength (non-compliant).
- RSA
    - Key wrapping; key establishment methodology provides 112-bits of encryption strength (allowed for use in FIPS mode of operation).
    - Key wrapping; key establishment methodology provides less than 112-bits of encryption strength (non-compliant).

Implementation A	Implementation B	Implementation C
DES-CBC3-MD5	BLOWFISH	DES
DES-CBC-MD5	CAMELLIA128	MD2
DES-CBC-SHA	CAMELLIA192	MD5
DSA 1024-bit sign	CAMELLIA256	HMAC MD5
EDH-DSS-DES-CBC-SHA	CAST5	DES40
EDH-RSA-DES-CBC-SHA	DSA 1024-bit sign	RC2
EXP-DES-CBC-SHA	MD5	RC4
EXP-EDH-DSS-DES-CBC-SHA	RIPEMD160	RC5
EXP-EDH-RSA-DES-CBC-SHA	TWOFISH	ECAES
EXP-RC2-CBC-MD5	RSA 1024-bit sign	RSA PKCS#1 V.2.0 (SHA256 - OAEP)
EXP-RC4-MD5	RSA 1536-bit sign	
IDEA-CBC-MD5		
IDEA-CBC-SHA		
RC2-CBC-MD5		
RC4-MD5		
RC4-SHA		
RSA 1024-bit sign		
RSA 1536-bit sign		
DH 1024-bit		
DH 1536-bit		

Table 2-5 - Non-Approved Algorithms Per Implementation

The following algorithms are deprecated and will be disallowed according to timelines specified in NIST SP 800-131A:

- RSA (1024-bit and 1536-bit)
- DSA (1024-bit and 1536-bit)

- SHA-1
- HMAC-SHA1
- Diffie-Hellman
- RNGs specified in FIPS 186-2 and ANSI X9.31

2.5 Module Interfaces

The figure below shows the module's physical and logical block diagram:

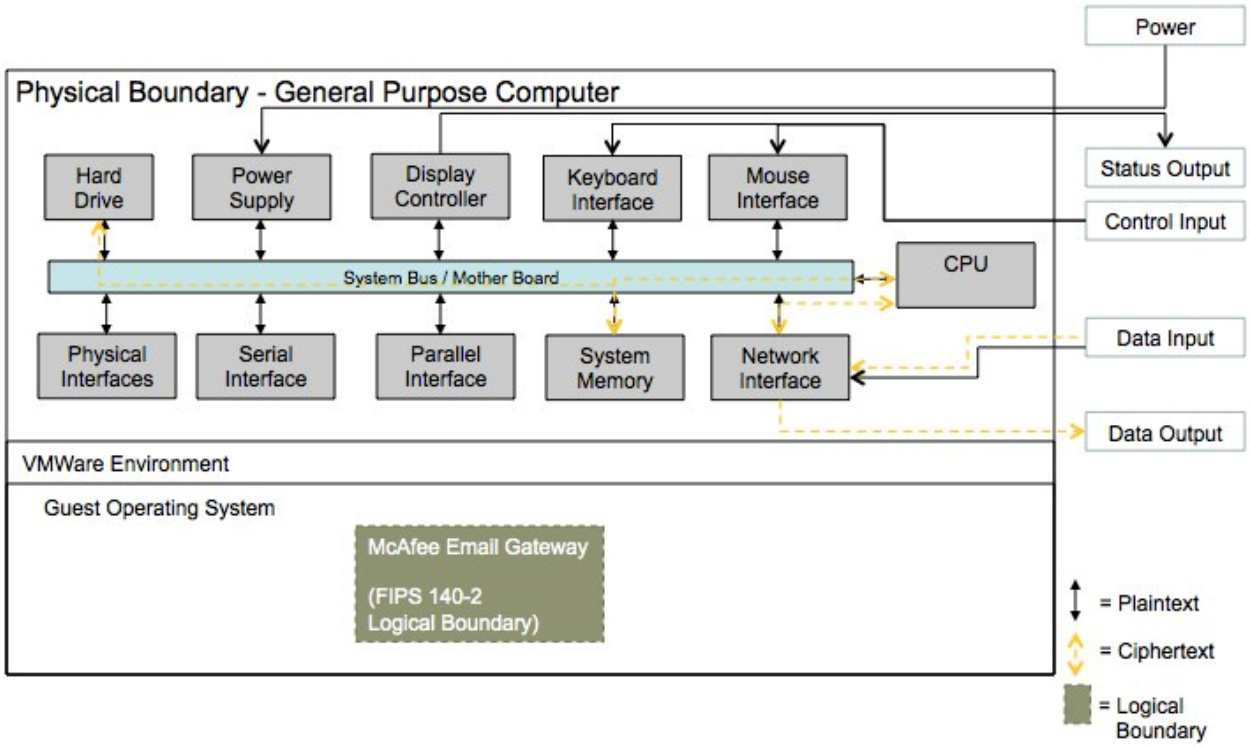

Figure 2 – Module Interfaces Diagram

The interfaces (ports) for the physical boundary include the computer keyboard port, CDROM drive, floppy disk, mouse, network port, parallel port, USB ports, monitor port and power plug. When operational, the module does not transmit any information across these physical ports because it is a software cryptographic module. Therefore, the module's interfaces are purely logical and are provided through the Application Programming Interface (API) that a calling daemon can operate. The logical interfaces expose services that applications directly call, and the API provides functions that may be called by a referencing application (see Section 2.6 – Roles, Services, and Authentication for the list of available functions).

The API provided by the module is mapped onto the FIPS 140- 2 logical interfaces: data input, data output, control input, and status output. Each of the FIPS 140- 2 logical interfaces relates to the module's callable interface, as follows:

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Data Input	Input parameters of API function calls	Ethernet/Network port
Data Output	Output parameters of API function calls	Ethernet/Network port
Control Input	API function calls	Keyboard and mouse
Status Output	For FIPS mode, function calls returning status information and return codes provided by API function calls.	Monitor
Power	None	Power supply/connector

Table 2-6 – Logical Interface / Physical Interface Mapping

The module's logical interfaces are provided only through the Application Programming Interface (API) that a calling daemon can operate. The module distinguishes between logical interfaces by logically separating the information according to the defined API.

As shown in Figure 2 – Module Interfaces Diagram, the output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

2.6 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role, which are authorized via identity-based authentication. The module does not support a Maintenance role.

2.6.1 Operator Services and Descriptions

The services available to the Crypto Officer role are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access
Configure Initializes the module for FIPS mode of operation	Configuration commands	Modified configuration file	None

Service and Description	Service Input	Service Output	Key/CSP Access
Zeroize CSPs Clears CSPs from memory	Zeroize command or module reimage	Invalidated CSP	All CSPs

Table 2-7 – Crypto Officer Services and Descriptions

The services available to the User role are as follows:

Service and Description	Service Input	Service Output	Key/CSP Access
Decrypt Decrypts a block of data Using AES or TDES	Key Encrypted byte stream	Byte stream	Symmetric Key: A Symmetric Key: B Symmetric Key: C
Encrypt Encrypts a block of data Using AES or TDES	Key Byte stream	Encrypted byte stream	Symmetric Key: A Symmetric Key: B Symmetric Key: C
Generate Keys Generates AES or TDES keys for encrypt / decrypt operations	Key Size	AES-Key TDES-Key	ANSI X9.31 PRNG seed: A ANSI X9.31 PRNG key: A ANSI X9.31 PRNG seed: B ANSI X9.31 PRNG key: B FIPS 186-2 PRNG Seed FIPS 186-2 PRNG Seed Key
Sign Signs a block with RSA or DSA	Data block to sign	RSA or DSA Signed data block	DH RSA Private Key DH DSA Private Key RSA Private Key: A DSA Private Key: A RSA Private Key: B DSA Private Key: B RSA Private Key: C DSA Private Key: C
Verify Verifies the signature of a RSA-signed or DSA-signed block	RSA or DSA Signed data block	Verification success/failure	DH RSA Public Key DH DSA Public Key RSA Public Key: A DSA Public Key: A RSA Public Key: B DSA Public Key: B RSA Public Key: C DSA Public Key: C

Key Generation Generate random number.	Entropy	Random number	ANSI X9.31 PRNG seed: A ANSI X9.31 PRNG key: A ANSI X9.31 PRNG seed: B ANSI X9.31 PRNG key: B FIPS 186-2 PRNG Seed FIPS 186-2 PRNG Seed Key
HMAC Hash-based Message Authentication Code	Key, data block	HMAC value	HMAC256 Key: A HMAC key: A HMAC key: B HMAC key: C

Table 2-8 – User Services and Descriptions

The module provides for the following unauthenticated services, which do not require authentication as they are not security relevant functions. These services do not affect the security of the module; these services do not create, disclose, or substitute cryptographic keys or CSPs, nor do they utilize any Approved security functions.

Service and Description	Service Input	Service Output	Key/CSP Access
Show Status Shows status of the module	None	Module status enabled/disabled	None
Initiate self-tests Restarting the module provides a way to run the self-tests on-demand	None	Console display of success/failure. Log entry of success/failure.	None

Table 2-9 – Unauthenticated Operator Services and Descriptions

2.6.2 Operator Authentication

2.6.2.1 Password-Based Authentication

In FIPS-approved mode of operation, the module is accessed via Graphical User Interface. Other than status functions available by viewing LEDs, the services described in Section 2.6.1 are available only to authenticated operators.

Passwords must be a minimum of 6 characters. The password can consist of alphanumeric values and special characters, {a-z},{A-Z},{0-9},{`~!@#$%^&*()_+={}[]\|;:'",./<>?], yielding 93 choices per character. The probability of a successful random attempt is $1/93^6$, which is less than 1/1,000,000.

Assuming a scripted attack of 60 attempts per minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/93^6$ which is less than 1/100,000.

The module will permit an operator to change identities provided the operator knows both the User password and the Crypto Officer password.

2.6.2.2 Certificate-Based Authentication

The module also supports authentication via digital certificates. The module supports a public key based authentication with 1024-bit, and 2048-bit RSA keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{80}$ which is less than 1/100,000.

A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one-minute period is $60/2^{112}$ which is less than 1/100,000.

2.7 Physical Security

This section of requirements does not apply to this module. The module is a software-only module and does not implement any physical security mechanisms.

2.8 Operational Environment

The module operates on a general-purpose computer (GPC) running a general-purpose operating system (GPOS). The module was tested on the following (Red Hat Linux 9):

- ESXi 4.1 on Intel Xeon E5410
- ESXi 5.0 on Intel Xeon E7540

Note that portability is claimed for instances of the module running in the following environments:

- VMware ESX
- VMware Server

For FIPS purposes, the module is running on a platform in single user mode and does not require any additional configuration to meet the FIPS requirements.

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B. FIPS 140-2 validation compliance is maintained

when the module is operated on other versions of the Microsoft Windows GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

2.9 Cryptographic Key Management

The table below provides a complete list of Critical Security Parameters used within the module:

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
Firmware						
Crypto Officer Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module; defined by the human user of the module	On Disk / Plaintext	Never	Overwriting the passwords with new ones or module reimage	CO: RWD
User Password	Alphanumeric passwords externally generated by a human user for authentication to the module.	Not generated by the module; defined by the human user of the module	On Disk / Plaintext	Never	Overwriting the passwords with new ones or module reimage	User: RWD
Implementation A						
Symmetric Key: A	TDES or AES 128, AES 256	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: A	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
RSA Private Key: A	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Public Key: A	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Private Key: A	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH RSA Public Key	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH RSA Private Key	RSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH DSA Public Key	DSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	Yes	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DH DSA Private Key	DSA 1024, 1536, 2048-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
HMAC key: A	HMAC-SHA1 key	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
HMAC256 Key: A	HMAC-SHA256 key	Hardcoded at build time	RAM / Plaintext	None	Image wipe	CO: D USER: RWD
ANSI X9.31 PRNG seed: A	32-byte entropy	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG key: A	AES 128	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
Implementation B						
Symmetric Key: B	TDES or AES 128, AES 192, AES 256	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: B	RSA 1024, 1536, 2048, 3072, 4096-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Private Key: B	RSA 1024, 1536 , 2048 , 3072 , 4096-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
DSA Public Key: B	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
DSA Private Key: B	DSA 1024-bit	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
HMAC key: B	HMAC SHA-1, 224, 256, 384, 512 Key	Internal generation by FIPS-approved X9.31 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG seed: B	32-byte entropy	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
ANSI X9.31 PRNG key: B	AES 128	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
Implementation C						
Symmetric Key: C	TDES or AES 128, AES 256	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Public Key: C	RSA 2048-bit	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
RSA Private Key: C	RSA 2048-bit	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

CSP/Key	Type	Input / Generation	Storage Location / Method	Output	Zeroization	Access
DSA Private Key: C	1024-bit key	Internal generation by FIPS-approved FIPS 186-2 in firmware	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
FIPS 186-2 PRNG Seed	Seed value for PRNG	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD
FIPS 186-2 PRNG Seed Key	Seed key for PRNG	Internally generated via system entropy	RAM / Plaintext	None	Resetting / rebooting the module or generating a new value	CO: D USER: RWD

Table 2-10 – Module CSPs and Keys

Private, secret, or public keys are protected from unauthorized modification and substitution. The module ensures only authenticated operators have access to keys and functions that can generate keys. Unauthenticated operators do not have write access to modify, change, or delete private, secret, or public keys.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module will output an error dialog and will enter an error state. When the module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions.

No keys or CSPs will be output when the module is in an error state. The module will halt and the process will terminate; as such, no data will be output via the data output interface. Additionally, the module does not support a bypass function, and the module does not allow plaintext cryptographic key components or other unprotected CSPs to be output on physical ports. No external software or firmware is allowed to be loaded in a FIPS mode of operation.

The following sections discuss the module's self-tests in more detail.

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check via HMAC-SHA256
- RSA pairwise consistency key (signing and signature verification)
- DSA pairwise consistency key (signing and signature verification)
- TDES KAT (encryption and decryption on all modes and implementations)
- AES KAT (encryption and decryption on all modes, key sizes, and implementations)
- SHA-1, SHA-256, and SHA-512 KAT (on applicable implementations)
- HMAC-SHA1, HMAC-SHA256 and HMAC-SHA512 (on applicable implementations)
- PRNG KAT (on all implementations)

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

2.10.2 Conditional Self-Tests

Conditional self-tests are tests that run when certain conditions occur during operation of the module. If any of these tests fail, the module will enter an error state. The module can be restarted to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. The module performs the following conditional self-tests:

- Pairwise consistency test for RSA implementations
- Pairwise consistency test for DSA implementations
- Continuous RNG test run on output of ANSI X9.31 PRNG implementations
- Continuous test on output of ANSI X9.31 PRNG seed mechanisms
- Continuous RNG test run on output of FIPS 186-2 PRNG implementations
- Continuous test on output of FIPS 186-2 PRNG seed mechanisms
- Continuous test to ensure seed and seed key are not the same values

The module does not perform a software load test because no additional software/firmware can be loaded in the module while operating in FIPS-approved mode.

2.11 EMI/EMC

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

2.12 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

This section describes how to configure the module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Software Packaging and OS Requirements

The Email Gateway for Virtual Environments 7.0.1 must be installed on a guest operating system running in single user mode. To configure single-user mode, the following must be disabled:

- Remote registry and remote desktop services
- Remote assistance
- Guest accounts
- Server and terminal services

3.1.2 Enabling FIPS Mode

To meet the cryptographic security requirements, certain restrictions on the installation and use of the module must be followed. The steps below will ensure that the module implements all required self-tests and uses only approved algorithms. Please note that once the module is in FIPS-approved mode, it cannot transition to a non-approved mode.

3.1.2.1 Installation

1. The installation must be a new install.
2. Select the FIPS mode option at installation.

3.1.3 Additional Rules of Operation

1. All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.
2. Only 2048-bit asymmetric keys should be used where available.
3. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.

4. The Crypto Officer password on the general purpose operating system must be at least 6 characters in length.
5. Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
6. Keys and CSPs shall be zeroized when transitioning to a FIPS mode from non-FIPS mode.

3.2 User Guidance

The User must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

End of Document
