

IBM Security FIPS 140-2 Non-Proprietary Security Policy Document Version: 1.4

Prepared By: Acumen Security 18504 Office Park Dr Montgomery Village, MD 20886

www.acumensecurity.net

Document Version 1.4

© IBM Security

Page 1 of 35

Revision	Description
September 2015, version 0.1	Initial Release
8/15/2016 version 0.9	Updated based on CMVP comments
8/24/2016 version 1.0	Updated based on CMVP comments
9/1/2016 version 1.1	Updated based on CMVP comments
10/28/2016 version 1.2	Added firmware version 5.3.3 throughout
12/13/2016 version 1.3	Updated Section 2.4.4
12/16/2016 version 1.4	Updated Section 2.4.4

Table Of Contents

1.	Intr	oduction	5
	1.1	Purpose	5
	1.2	Document Organization	5
	1.3	Notices	5
	1.4	Acronyms	5
2.	IBIV	I SECURITY MODULAR EXTENSIBLE SECURITY ARCHITECTURE	7
	2.1	Product Overview	7
	2.2	Cryptographic Module Characteristics	7
	2.3	Validation Level Detail	8
	2.4	Cryptographic Algorithms	8
	2.4.1	Approved Algorithms and Implementation Certificates	8
	2.4.2	Non-Approved But Allowed Algorithms1	.2
	2.4.3	Cryptographic Module Specification1	.3
	2.4.4	Excluded Components 1	.3
	2.4.5	FIPS Mode 1	.3
	2.5	Module Interfaces 1	.3
	2.6	Roles, Services, and Authentication1	.4
	2.6.1	Operator Services and Descriptions1	.4
	2.6.2	Operator Authentication1	.5
	2.6.3	Mechanism and Strength of Authentication1	.5
	2.7	Physical Security 1	.5
	2.8	Operational Environment1	.5
	2.8.1	Operational Environment Policy1	.5
	2.9	Cryptographic Key Management1	.6
	2.10	Self-Tests	2
	2.10.1	Power-On Self-Tests	2
	2.10.2	Conditional Self-Tests	3
	2.11	Mitigation of Other Attacks	4
3.	Gui	dance and Secure Operation3	5
	3.1	Crypto Officer Guidance	5
	3.1.1	Enabling FIPS Mode	5

3.2	User Guidance	35
3.3	General Guidance	35

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for IBM Security Modular Extensible Security Architecture. Below are the details of the product certified:

Software Version #: 5.3.1 and 5.3.3 FIPS 140-2 Security Level: 1

1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how Modular Extensible Security Architecture meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. Target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Acumen Security under contract to IBM Security. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to IBM and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.4 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DTR	Derived Testing Requirement
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface

FIPS 140-2 Non-Proprietary Security Policy

Acronym	Term
HMAC	Hashed Message Authentication Code
IBM	International Business Machines
ISS	Internet Security Systems
КАТ	Known Answer Test
NDRNG	Non-Deterministic Random Number Generator
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm
SSH	Secure Shell
TLS	Transport Layer Security
Triple-DES	Triple Data Encryption Standard

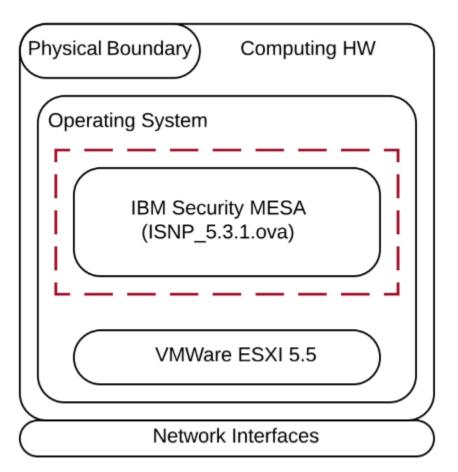
Table 1 – Acronyms and Terms

2. IBM SECURITY MODULAR EXTENSIBLE SECURITY ARCHITECTURE

2.1 **Product Overview**

This module provides the FIPS validated cryptographic services for applications requiring cryptography. The services provided by the module, includes Symmetric and Asymmetric Cryptography as well as some support for TLS, SSH, SNMP protocols. The Modular Extensible Security Architecture supports various IBM Security platforms, such as, the IBM Security GX Security Appliances and the IBM Security XGS Security Appliances.

2.2 Cryptographic Module Characteristics



The module's block diagram is shown above. The red dashed line area denotes the logical cryptographic boundary of the module which is defined as the virtual machine image. The virtual image which is supported by VMware ESXi, includes the following file,

- ISNP_5.3.1.ova
- ISNP_5.3.3.ova

While the outer black solid line denotes the physical cryptographic boundary of the module which is the enclosure of the system on which the module is executed.

Document Version 1.4

© IBM Security

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	1
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	1
Mitigation of Other Attacks	N/A
Overall Validation Level	1

Table 2 – 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 Approved Algorithms and Implementation Certificates

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program:

Algorithm	CAVP Certificate	Use
RSA (FIPS186-2)	OpenSSL - #1841	Sign / verify operations
ALG[ANSIX9.31]:		Digital Certificates
Signature Verification:		0
Key Size: 1024, 1536, 2048, 3072, 4096 bits		
Hash: SHA-1, SHA-256, SHA-384 , SHA-512		
ALG[RSASSA-PKCS1_V1_5]:		
Signature Verification:		
Key Size: 1024, 1536, 2048, 3072, 4096 bits		
Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
RSA (FIPS186-4)		
Key Generation:		
Key Size: 2048, 3072 bits		
ALG[ANSIX9.31]		
Signature Verification:		
Key Size: 1024, 2048, 3072 bits		
Hash: SHA-1, SHA-256, SHA-384 , SHA-512		

Algorithm	CAVP Certificate	Use
ALG[RSASSA-PKCS1_V1_5]		
Signature Generation:		
Key Size: 2048, 3072 bits		
Hash: SHA-224, SHA-256, SHA-384 , SHA-512		
Signature Verification:		
Key Size: 1024, 2048, 3072 bits		
Hash: SHA-224, SHA-256, SHA-384 , SHA-512		
RSA (FIPS186-2)	GSKIT – #1840	
· · · ·		
ALG[RSASSA-PKCS1_V1_5]:		
Signature Verification:		
Key Size: 1024, 1536, 2048, 3072 bits Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
ndsii. 3na-1, 3na-224, 3na-230, 3na-364 , 3na-312		
RSA (FIPS186-4)		
Key Generation:		
Key Size: 2048, 3072 bits		
· · · ·		
ALG[RSASSA-PKCS1_V1_5]		
Signature Generation:		
Key Size: 2048, 3072 bits Hash: SHA-224, SHA-256, SHA-384 , SHA-512		
110311. 311A-224, 311A-230, 311A-304 , 311A-312		
Signature Verification:		
Key Size: 1024, 2048 bits		
Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
ECDSA	OpenSSL - #727	
FIPS186-4:		
PKG:		
CURVES: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-		
233, B-283, B-409, B-571		
PKV:		
CURVES: ALL-P ALL-K ALL-B		
Signature Generation:		
CURVES: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-		
233, B-283, B-409, B-571		
Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
Signature Verification:		
CURVES: P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-		
409, K-571, B-163, B-233, B-283, B-409, B-571		
Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
ECDSA	GSKIT – #726	

Algorithm	CAVP Certificate	Use
FIPS186-4:		
PKG:		
CURVES: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-		
233, B-283, B-409, B-571		
PKV:		
CURVES: ALL-P ALL-K ALL-B		
Signature Generation:		
CURVES: P-224, P-256, P-384, P-521, K-233, K-283, K-409, K-571, B-		
233, B-283, B-409, B-571		
Hash: SHA-224, SHA-256, SHA-384 , SHA-512		
Signature Verification:		
CURVES: P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-		
409, K-571, B-163, B-233, B-283, B-409, B-571		
Hash: SHA-1, SHA-224, SHA-256, SHA-384 , SHA-512		
SHS	OpenSSL - #2941	Message digest in
		TLS sessions
SHA-1 (BYTE-only) SHA-224 (BYTE-only)		Module integrity via SHA-1
SHA-224 (BTTE-only) SHA-256 (BYTE-only)		
SHA-384 (BYTE-only)		
SHA-512 (BYTE-only)		
SHS	GSKIT – #2940	
SHA-1 (BYTE-only)		
SHA-224 (BYTE-only)		
SHA-256 (BYTE-only)		
SHA-384 (BYTE-only)		
SHA-512 (BYTE-only) HMAC	OpenSSL - #2279	Message
	Open33L - #2273	verification
HMAC-SHA1 (Key Sizes Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA224 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA256 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA384 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA512 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
НМАС	GSKIT – #2278	
HMAC-SHA1 (Key Sizes Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA224 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA224 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA384 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
HMAC-SHA512 (Key Size Ranges Tested: KS <bs ks="">BS)</bs>		
AES	OpenSSL - #3579	Data encryption /
		decryption
ECB, CBC, CFB1, CFB8, CFB128, OFB, CTR, (e/d)		
Key Size: 128 , 192 , 256		

CCM (implemented but not used) CMAC (implemented but not used) (Generation/Verification) (128, 152, 256 bits) 192, 256 bits) Massage Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16 GCM (e/d) GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128, 192, 256 bits GSKIT - #3578 ECB, CBC, CFB1, CFB2, CFB128, OFB, CTR(e/d) GSKIT - #3578 ECB, CBC, CFB1, CFB2, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length: GGM (e/d) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: 128, 192, 256 bits GGM (e/d) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 OpenSSL - #1992 TECB, TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2^16 GSKIT - #1991 TECB, TCBC, TCFB64, TOFB (e/d) SSKIT - #1991 Key Size: 3 key GSKIT - #1991 TECB, TCBC, TCFB64, TOFB (e/d) SSKIT - #1991 Key Size: 3 key GSKIT - #1991 TECB, TCBC, TCFB64, TOFB (e/d) SSKIT - #1991 TECB, TCBC, TCFB64, TOFB (e/d) GSKIT - #1991 Keying Option 1 CMAC (implemented but not used) (Generation/Ve	Algorithm	CAVP Certificate	Use
192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 216 Tag Length: Min: 0 Max: 16GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2AESGSKIT - #3578ECB, CBC, CFB1, CFB3, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length:CCM (implemented but not used) CMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 16GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 161GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 162GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 163GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 164GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 164GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 164GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 2016 <td></td> <td></td> <td></td>			
192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 216 Tag Length: Min: 0 Max: 16GCM (e/d) 			
Key Size: 128, 192, 256Message Length: Min: 0 Max: 2^16GCM (e/d)Key Size: 128, 192, 256 bitsTag Length: 128IV Generated internally using Section 8.2.2AESGSKIT = #3578ECB, CBC, CFB1, CFB128, OFB, CTR(e/d)Key Size: 128, 192, 256Message Length:CMAC (implemented but not used)CCM (implemented but not used) (Generation/Verification) (128, 192, 256 bits)Message Length:Min: 0 Max: 2^16Tag Length: Min: 0 Max: 16GCM (e/d)Key Size: 128, 192, 256 bitsTag Length: Min: 0 Max: 2^16Tag Length: Min: 0 Max: 16GCM (e/d)Key Size: 128, 192, 256 bitsTag Length: Min: 0 Max: 2^16Tag Length: Min: 0 Max: 16GCM (e/d)Key Size: 128, 192, 256 bitsTag Length: Min: 0 Max: 2^16Tag Length: Min: 0 Max: 2^16			
Message Length: Min: 0 Max: 2416 Tag Length: Min: 0 Max: 16 GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated Internally using Section 8.2.2 AES GSKIT = #3578 ECB, CFB1, CFB3, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length: CCM (implemented but not used) CMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 216 Tag Length: Min: 0 Max: 216 Tag Length: Min: 0 Max: 216 Tag Length: Min: 0 Max: 216 Triple-DES TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 216 Tag Length:			
Tag Length: Min: 0 Max: 16Image: Constraint of the second sec			
GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128 GSKIT - #3578 AES GSKIT - #3578 ECB, CGC, CFB1, CFB3, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 GSKIT - #3578 Message Length: CCM (implemented but not used) Generated internally using Section 1 (128, 132, 256 bits) Key Size: 128, 192, 256 Key Size: 128, 192, 256 bits GSKIT - #3578 GCM (e/d) Key Size: 128, 192, 256 bits GGM (e/d) Feederated internally using Section 1 (128, 132, 256 bits) GCM (e/d) Key Size: 128, 192, 256 bits GGM (e/d) Feederated internally using Section 8.2.2 Feederated internally using Section 8.2.2 Triple-DES OpenSSL - #1992 FECB, TCR, TCFB64, TOFB (e/d) Feederated internally using Section 8.2.2 Triple-DES OpenSSL - #1992 FECB, TCR, TCFB64, TOFB (e/d) Feederated internally using Section 8.2.2 Triple-DES OpenSSL - #1992 FECB, TCB, TCFB64, TOFB (e/d) Feederated internally using Section 8.2.2 Triple-DES GSKIT - #1991 FECB, TCB, CTCB64, TOFB (e/d) Feederated internally using Section 8.2.2 Triple-DES GSKIT - #1991 FECB, TCB, CTCB64, TOFB (e/d) Feederated internally using Section 8.2.2 Triple-DES GSKIT - #1991 FECB, TCB, CTCB64, TOFB (e/d) Feederated internally using S			
Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2GSKIT - #3578 AES GSKIT - #3578 ECB, CBC, CFB1, CFB3, CFB128, OFB, CTR (e/d) Key Size: 128, 192, 256 Message Length:GSKIT - #3578 CCM (implemented but not used) Cmatcher (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 16GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 16 GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 2016 Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992 Triple-DES OpenSSL - #1992 TECB, TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max:	Tag Length: Min: U Max: 16		
Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2GSKIT - #3578 AES GSKIT - #3578 ECB, CBC, CFB1, CFB3, CFB128, OFB, CTR (e/d) Key Size: 128, 192, 256 Message Length:GSKIT - #3578 CCM (implemented but not used) Cmatcher (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 16GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 16 GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max: 2016 Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992 Triple-DES OpenSSL - #1992 TECB, TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2016 Tag Length: Min: 0 Max:	GCM (e/d)		
Tag Length: 128 IV Generated internally using Section 8.2.2GSKIT - #3578AESGSKIT - #3578ECB, CBC, CFB1, CFB3, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length:GSKIT - #3578CCM (implemented but not used)Cmatcher (implemented but not used)Implemented but not used)CMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16OpenSSL - #1992GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: Min: 0 Max: 16OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Key size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16<			
AESGSKIT - #3578ECB, CBC, CFB1, CFB8, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length:SKIT - #3578CCM (implemented but not used)(Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16SKIT - #3578GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992TFiple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 3DRBGOpenSSL - #199			
ECB, CEC, CFB1, CFB3, CFB128, OFB, CTR(e/d) Key Size: 128, 192, 256 Message Length:Image: CCM (implemented but not used)CCMAC (implemented but not used)(Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16Image: Complemented but not used)GCM (e/d) Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1OpenSSL - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1DeterministicTECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1OpenSSL - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Deterministic	IV Generated internally using Section 8.2.2		
Key Size: 128, 192, 256 Message Length:Image: CCM (implemented but not used)CCMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits)Image: Complexity of the state	AES	GSKIT – #3578	
Key Size: 128, 192, 256 Message Length:Image: CCM (implemented but not used)CCMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits)Image: Complexity of the state			
Message Length:Image: CCM (implemented but not used)Image: CCM (implemented but not used) (Generation/Verification) (128, 192, 256 bits)CMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits)Image: CCM (200, 100, 100, 100, 100, 100, 100, 100,			
CCCM (implemented but not used)CCCM (implemented but not used) (Generation/Verification) (128, 192, 256 bits)192, 256 bits)Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: 128 IV Generated internally using Section 8.2.2Triple-DESOpenSSL - #1992TECB, TCEB, TCFB64, TOFB (e/d) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Triple-DESGSKIT - #1991CCMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8			
CMAC (implemented but not used) (Generation/Verification) (128, 192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16Image: Constraint of C	Message Length:		
192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16	CCM (implemented but not used)		
192, 256 bits) Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16	CMAC (implemented but not used) (Generation/Verification) (128		
Key Size: 128, 192, 256 Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16Image: Constant of Con			
Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 16Image: Constant of Constan			
Tag Length: Min: 0 Max: 16Image: Comparison of the section of the secti			
Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1OpenSSL - #1992CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1DeterministicCMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Key Size: 128, 192, 256 bits Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1OpenSSL - #1992CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1DeterministicCMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Tag Length: 128 IV Generated internally using Section 8.2.2OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991TFECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991EtcB, TCBC, TCFB64, TOFB (e/d) Keying Option 1CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
IV Generated internally using Section 8.2.2OpenSSL - #1992Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991Herein Complemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Triple-DESOpenSSL - #1992TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1OpenSSL - #1992CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Image: CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8Image: CMAC (implemented but not used) (Generation/Verification) GSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8GPENSL - #919DRBGOpenSSL - #919Deterministic		OpenSSI - #1992	-
Keying Option 1CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 3Deterministic	TECB, TCBC, TCFB64, TOFB (e/d)		
Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic	Keying Option 1		
Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Message Length: Min: 0 Max: 2^16 Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Tag Length: Min: 2 Max: 8GSKIT - #1991Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
Triple-DESGSKIT - #1991TECB, TCBC, TCFB64, TOFB (e/d) Keying Option 1GSKIT - #1991CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8Deterministic			
TECB, TCBC, TCFB64, TOFB (e/d) Image: Complemented but not used) Keying Option 1 Image: Complemented but not used) CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Image: Complemented but not used) Message Length: Min: 0 Max: 2^16 Image: Complemented but not used) Tag Length: Min: 0 Max: 8 Image: Complemented but not used) DRBG OpenSSL - #919 Deterministic		GSKIT – #1991	-
Keying Option 1 CMAC (implemented but not used) (Generation/Verification) Feasibility Key Size: 3 key Key Size: 3 key Feasibility Message Length: Min: 0 Max: 2^16 Feasibility Feasibility Tag Length: Min: 0 Max: 8 OpenSSL - #919 Deterministic			
CMAC (implemented but not used) (Generation/Verification) Key Size: 3 key Message Length: Min: 0 Max: 2^16 Tag Length: Min: 0 Max: 8August 1000000000000000000000000000000000000			
Key Size: 3 key Image: A state of the st	Keying Option 1		
Key Size: 3 key Image: A state of the st	CNAAC (implemented but not used) (Concerting (traification)		
Message Length: Min: 0 Max: 2^16			
Tag Length: Min: 0 Max: 8 OpenSSL - #919 DRBG OpenSSL - #919			
DRBG OpenSSL - #919 Deterministic			
		OpenSSL - #919	Deterministic
Hash_Based DRBG: Generation	Hash_Based DRBG:		

Algorithm	CAVP Certificate	Use
Prediction Resistance: Enabled/Not Enabled		
Hash: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512		
HMAC_Based DRBG:		
Prediction Resistance: Enabled/Not Enabled		
Hash: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512		
CTR_DRBG:		
Prediction Resistance: Enabled/Not Enabled		
BlockCipher Use df: (AES-128, AES-192, AES-256)		
BlockCipher No df: (AES-128 , AES-192 , AES-256)		
DRBG	GSKIT – #918	
Hash Based DRBG:		
Prediction Resistance: Enabled/Not Enabled		
Hash: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512		
HMAC_Based DRBG:		
Prediction Resistance: Enabled/Not Enabled		
Hash: SHA-1 , SHA-224 , SHA-256 , SHA-384 , SHA-512		
CTR_DRBG:		
Prediction Resistance: Enabled/Not Enabled		
BlockCipher Use df: (AES-128 , AES-192 , AES-256)		
BlockCipher_No_df: (AES-128 , AES-192 , AES-256)		
CVL	GSKIT – #748	Cofactor Diffie-
		Hellman Primitive
Elliptic Curve Diffie-Hellman		
CURVES: P: 224, P-256, P-384, P-521		
Table 3 – Algorithm Certificates		

Table 3 – Algorithm Certificates

2.4.2 Non-Approved But Allowed Algorithms

The Module supports the following key establishment schemes and non-approved but allowed algorithms:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 (2048-bit keys) or 128 (3072-bit keys) bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- MD5 for use in TLS only
- NDRNG
 - The minimum number of bits of entropy requested per each GET function is 256 bits.

• RSA Key Wrapping Encrypt / Decrypt (2048, 3072 bits) Allowed to be used in FIPS mode (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

2.4.3 Cryptographic Module Specification

For FIPS 140-2 purposes, the Module is classified as a multi-chip standalone module. The Module's physical cryptographic boundary is the enclosure of the computer system on which it is executing.

The software was validated on the following platforms:

IBM X3550 M2 Server with an Intel Xeon E5530 (2x) w/ RHEL 6.3 Linux on VMware ESXi 5.5

2.4.4 Excluded Components

Excluded components including the following:

- Monitoring Ports
 - The excluded monitoring ports accept and pass data traffic that is analyzed by the internal IDS analysis engine. The traffic is not security relevant and does not interact with the cryptographic processing of the appliance. However, the IDS analysis engine uses TLS/SSL cipher suites for outbound/inbound SSL inspection/detection. Furthermore, the IDS analysis engine may use nonapproved algorithms and cipher suites to analyzing data packets on the protected network. TLS flows using non-approved/approved algorithms and cipher suites should be considered clear text and non-security relevant.

2.4.5 FIPS Mode

The module can only be enabled for FIPS mode at the time of initial configuration. Additionally, if the module enters an error state (e.g., a known answer test fails), the module must be restarted.

2.5 Module Interfaces

The physical ports of the Module are the same as the system on which it is executing. The VMware ESXi hypervisor provides virtualized ports and interfaces for the module. Interaction of with the virtual ports created by the hypervisor occurs through the host system's Ethernet port. Management, data, and status traffic must all flow through the Ethernet port. Direct interaction with the module via the host system is not possible.

The module provides logical interfaces to the system, and is mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

Interface	Description
Data Input	Virtual Network Interfaces
	Plaintext and/or ciphertext data

Interface	Description				
Data Output	Virtual Network Interfaces				
	Plaintext and/or ciphertext data				
Control	Virtual Network Interfaces				
Input	Configuration or Administrative data entered into the module				
Status	Virtual Network Interfaces				
Output	status provided or displayed via the user interfaces				

Table 4 – Interface Descriptions

2.6 Roles, Services, and Authentication

The Module assumes two roles: User role and Crypto Officer role, which are identified along with their allowed services below. The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Module.

2.6.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input / Output	Key/CSP	Roles
			Access	
Configure	Initializes the module for FIPS mode of operation	Configuration Parameters / Module configured	None	Crypto Officer
Self-Test	Performs self tests on critical functions of module	Initiate self-tests / Self tests run	None	Crypto Officer User
Decrypt	Decrypts a block of data	Initiate decryption / data decrypted	15, 16, 37, 38, 40, 41, 42	Crypto Officer User
Encrypt	Encrypts a block of data	Initiate encryption/ data encrypted	15, 16, 37, 38, 40, 41, 42	Crypto Officer User
Hash	Verifies the hash of a block of data	Initiate hash/ hash value	17, 39, 43	Crypto Officer User
Random Bit Generation	Generates Random Bits	Initiate Bit Generation/Random Bits	18, 19, 20, 21, 22, 46, 47, 48, 49, 50	Crypto Officer User
Signature Generation	Generates Digital Signature	Initiate Generation/Signature	1, 2, 3, 4, 23, 24, 25, 26	Crypto Officer User
Signature Verification	Verifies Digital Signature	Initiate verification/pass or fail	1, 2, 3, 4, 23, 24, 25, 26	
Establish Session	Provides a protected session for establishment of encryption keys with peers	Initiate session establishment / session established	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 23, 24, 25, 26, 27 28, 29, 30, 31, 32, 33, 34, 35, 36, 44, 45	Crypto Officer User
Zeroize CSPs	Clear CSPs from memory	Terminate Session / CSPs cleared	5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50	Crypto Officer User

Service	Description	Service Input / Output	Key/CSP Access	Roles
	Clear CSPs from disk	Reimage module / CSPs cleared and module restored to factory settings	1, 2, 3, 4, 23, 24, 25, 26	Crypto Officer
Show	Shows status of the	Show status commands /	None	Crypto Officer
Status	module	Module status		User

Table 5 – Operator Services and Descriptions

2.6.2 Operator Authentication

At security level 1, authentication is not required. The role is implicitly assumed on entry.

2.6.3 Mechanism and Strength of Authentication

At security level 1, authentication is not required.

2.7 Physical Security

The module is a software module. Physical security is not required.

2.8 **Operational Environment**

This Module operates in a modifiable operational environment per the FIPS 140-2 definition. The module was validated in the following environment: RHEL 6.3 Linux on VMware ESXi 5.5 with an Intel Xeon E5530 (2x) processor.

2.8.1 Operational Environment Policy

The operating system is restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

The application that makes calls to the cryptographic Module is the single user of the cryptographic Module, even when the application is serving multiple clients.

2.9 Cryptographic Key Management

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

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
KIT Implementa	tion					
mmetric Crypto	graphy					
RSA Private Key	Private key for sign / verify operations and key establishment ¹ for	Internal generation at installation by	Storage : On disk in plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer
	XGS TLS connections	DRBG	Association: The system is the one and	Output: None		RWD
			only owner. Relationship is maintained by the operating system via protected memory.			User R
RSA Public Key	Public key for sign / verify operations and key establishment ² for	Internal generation at installation by	Storage: On disk in plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer
		DRBG	Association: The system is the one and	Output: plaintext during		RWD
	Encryption/Decryption of the Premaster Secret for entry/output		only owner. Relationship is maintained by the operating system via X509 certificates.	TLS negotiation		User R
ECDSA Private Key	Private Key for sign / verify operations and key establishment for	Internal Generation	Storage: On disk in plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D
	Name CIT Implementa mmetric Crypto RSA Private Key RSA Public Key ECDSA	NameKIT Implementationmmetric CryptographyRSA Private KeyPrivate key for sign / verify operations and key establishment ¹ for XGS TLS connectionsRSA Public KeyPublic key for sign / verify operations and key establishment ² for XGS TLS connectionsRSA Public KeyPublic key for sign / verify operations and key establishment ² for XGS TLS connectionsRSA Public KeyPublic key for sign / verify operations and key establishment ² for XGS TLS connectionsEncryption/Decryption of the Premaster Secret for entry/outputECDSA Private KeyPrivate Key for sign / verify operations and key	Name Implementation GIT Implementation mmetric Cryptography RSA Private Key Private key for sign / verify operations and key establishment ¹ for XGS TLS connections Internal generation at installation by DRBG RSA Public Key Public key for sign / verify operations and key establishment ² for XGS TLS connections Internal generation at installation by DRBG RSA Public Key Public key for sign / verify operations and key establishment ² for XGS TLS connections Internal generation at installation by DRBG Encryption/Decryption of the Premaster Secret for entry/output Encryption / verify operations and key Internal Generation	Name Internal Storage: On disk in plaintext RSA Private Private key for sign / verify operations and key establishment ^a for XGS TLS connections Internal Storage: On disk in plaintext RSA Public Public key for sign / verify operations and key establishment ² for XGS TLS connections Internal Storage: On disk in plaintext RSA Public Public key for sign / verify operations and key establishment ² for XGS TLS connections Internal Storage: On disk in plaintext RSA Public Public key for sign / verify operations and key establishment ² for xGS TLS connections Internal Storage: On disk in plaintext BBG DRBG Storage: On disk in plaintext Type: Static RSA Public Public key for sign / verify operations and key establishment ² for XGS TLS connections Internal Storage: On disk in plaintext BBG DRBG DRBG Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates. ECDSA Private Key for sign / verify operations and key Internal Storage: On disk in plaintext	NameKIT Implementationmmetric CryptographyRSA Private KeyPrivate key for sign / verify operations and key establishment* for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/AType: StaticType: StaticAgreement: N/ARSA Public KeyPublic key for sign / verify operations and key establishment* for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/ARSA Public KeyPublic key for sign / verify operations and key establishment* for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/ARSA Public KeyPublic key for sign / verify operations and key establishment* for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/AType: StaticStorage: On disk in plaintextEntry: N/AOutput: plaintext during TLS negotiationEncryption/Decryption of the Premaster Secret for entry/outputInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/AECDSA Private KeyPrivate Key for sign / verify operations and keyInternal GenerationStorage: On disk in plaintextAgreement: N/A	NameNameCIT Implementationmmetric CryptographyRSA Private KeyPrivate key for sign / verify operations and key establishment ¹ for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintext Type: StaticAgreement: N/AEstablish SessionRSA Public KeyPublic key for sign / verify operations and key establishment ² for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/AEstablish SessionRSA Public KeyPublic key for sign / verify operations and key establishment ² for XGS TLS connectionsInternal generation at installation by DRBGStorage: On disk in plaintextAgreement: N/AEstablish SessionRSA Public KeyPublic key for sign / verify operations and

¹ Key establishment methodology provides 112 or 128-bits of encryption strength

² Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
		SiteProtector TLS connections.		Association : The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Output: None		User R
4	ECDSA Public Key	Public Key for sign / verify operations and key establishment for SiteProtector TLS connections.	Internal Generation	 Storage: On disk in plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 	Agreement: N/A Entry: N/A Output: plaintext during TLS negotiation.	Establish Session	Crypto Officer R W D User R
	-			certificates.			
TLS	Master Secret		lateral	Storege DAM plaintaut	A mus sure surt NI/A	Establish	Circusto
5	(48 Bytes)	Used for computing the Session Key	Internal generation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: N/A	Session	Crypto Officer None User None
6	Premaster Secret (48 Bytes)	Premaster Secret Message	Internal generation by DRBG	Storage: RAM plaintextType: EphemeralAssociation: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: Input during TLS negotiation Output: Output to server encrypted by Public Key	Establish Session	Crypto Officer None User None
7	ECDHE Private Key		Internal generation	Storage: RAM plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
		Private asymmetric key for key establishment ³ for XGS TLS connections.		Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output : Key handle from request is output only to the SiteProtector application		User R
8	ECDHE Public Key	Public asymmetric key for key establishment ⁴ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
9	ECDH Private Key	Private asymmetric key for key establishment ⁵ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
10	ECDH Public Key		Internal generation	Storage: RAM plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D

³ Key establishment methodology provides between 112 and 256 bits of encryption strength

⁴ Key establishment methodology provides between 112 and 256 bits of encryption strength ⁵ Key establishment methodology provides between 112 and 256 bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
		Public asymmetric key for key establishment ⁶ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output		Association : The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Output : Key handle from request is output only to the SiteProtector application		User R
11	DH Private Key	Private asymmetric key for key establishment ⁷ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
12	DH Public Key	Public asymmetric key for key establishment ⁸ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R

⁶ Key establishment methodology provides between 112 and 256 bits of encryption strength

 ⁷ Key establishment methodology provides 112 or 128-bits of encryption strength
 ⁸ Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
13	DHE Private Key	Private asymmetric key for key establishment ⁹ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
14	DHE Public Key	Public asymmetric key for key establishment ¹⁰ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
15	GSKIT TLS AES Session Key	AES 128, 192, 256 encryption & decryption of management traffic	Internal generation at installation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: Via secure TLS tunnel Entry: N/A Output: N/A	Decrypt Encrypt	Crypto Officer R W D User R W D

⁹ Key establishment methodology provides 112 or 128-bits of encryption strength ¹⁰ Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
16	GSKIT TLS Triple-DES Session Key	Triple-DES 192 encryption & decryption of management traffic	Internal generation at installation by	Storage : RAM plaintext Type: Ephemeral	Agreement: Via secure TLS tunnel	Decrypt Encrypt	Crypto Officer
	Session Rey		DRBG	Association : The system is the one and only owner. Relationship is maintained by the operating system via protected	Entry: N/A Output: N/A		R W D User R W D
17	GSKIT TLS HMAC key	HMAC-SHA-1, HMAC- SHA-224, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512 for message verification	Internal generation at installation by DRBG	memory. Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: None	Establish Session	Crypto Officer R W D User R W D
DRE	3G						
18	DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	Generated internally by non-Approved RNG	Storage: RAM plaintext Type: Ephemeral	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer None User
				Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		None
19	Entropy Input String	Input value for entropy calculation	Generated internally by non-Approved	Storage: RAM plaintext Type: Ephemeral	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer None
			RNG	Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		User None

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
20	Hash_DRBG mechanism	V and C values	Generated internally by non-Approved RNG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: N/A	Establish Session	Crypto Officer None User None
21	HMAC_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: N/A	Establish Session	Crypto Officer None User None
22	CTR_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: N/A	Establish Session	Crypto Officer None User None
-	enSSL Implemen						
Asy	mmetric Cryptog	graphy					
23	RSA Private Key	Private key for sign / verify operations and key establishment ¹¹ for	Internal generation at installation by	Storage : On disk in plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer
		XGS TLS connections	DRBG		Output: None		RWD

¹¹ Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
				Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.			User R
24	RSA Public Key	Public key for sign / verify operations and key establishment ¹² for XGS TLS connections Encryption/Decryption of the Premaster Secret for entry/output	Internal generation at installation by DRBG	 Storage: On disk in plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates. 	Agreement: N/A Entry: N/A Output: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
25	ECDSA Private Key	Private Key for sign / verify operations and key establishment for SiteProtector TLS connections.	Internal Generation	 Storage: On disk in plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates. 	Agreement: N/A Entry: N/A Output: None	Establish Session	Crypto Officer R W D User R
26	ECDSA Public Key	Public Key for sign / verify operations and key establishment for SiteProtector TLS connections.	Internal Generation	Storage: On disk in plaintextType: StaticAssociation: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: plaintext during TLS negotiation.	Establish Session	Crypto Officer R W D User R

¹² Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
TLS	;						
27	Premaster Secret (48 Bytes)	Premaster Secret Message	Internal generation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: Input during TLS negotiation Output: Output to server encrypted by Public Key	Establish Session	Crypto Officer None User None
28	Master Secret (48 Bytes)	Used for computing the Session Key	Internal generation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: N/A	Establish Session	Crypto Officer None User None
29	ECDHE Private Key	Private asymmetric key for key establishment ¹³ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D

¹³ Key establishment methodology provides between 112 and 256 bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
				Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output : Key handle from request is output only to the SiteProtector application		User R
30	ECDHE Public Key	Public asymmetric key for key establishment ¹⁴ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
31	ECDH Private Key	Private asymmetric key for key establishment ¹⁵ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
32	ECDH Public Key	Public asymmetric key for key establishment ¹⁶ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D

 ¹⁴ Key establishment methodology provides between 112 and 256 bits of encryption strength
 ¹⁵ Key establishment methodology provides between 112 and 256 bits of encryption strength
 ¹⁶ Key establishment methodology provides between 112 and 256 bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
		Encryption/Decryption of the Premaster Secret for entry/output		Association : The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Output : Key handle from request is output only to the SiteProtector application		User R
33	DH Private Key	Private asymmetric key for key establishment ¹⁷ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
34	DH Public Key	Public asymmetric key for key establishment ¹⁸ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
35	DHE Private Key	Private asymmetric key for key establishment ¹⁹ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer R W D

 ¹⁷ Key establishment methodology provides 112 or 128-bits of encryption strength
 ¹⁸ Key establishment methodology provides 112 or 128-bits of encryption strength
 ¹⁹ Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
				Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output : Key handle from request is output only to the SiteProtector application		User R
36	DHE Public Key	Public asymmetric key for key establishment ²⁰ for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
37	OpenSSL TLS AES Session Key	AES 128, 192, 256 encryption & decryption of management traffic	Internal generation at installation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: Via secure TLS tunnel Entry: N/A Output: N/A	Decrypt Encrypt	Crypto Officer R W D User R W D
38	OpenSSL TLS Triple-DES Session Key	Triple-DES 192 encryption & decryption of management traffic	Internal generation at installation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: Via secure TLS tunnel Entry: N/A Output: N/A	Decrypt Encrypt	Crypto Officer R W D User R W D

²⁰ Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
39	OpenSSL TLS HMAC key	HMAC-SHA-1, HMAC- SHA-224, HMAC-SHA-	Internal generation at	Storage: RAM plaintext	Agreement: N/A	Establish Session	Crypto Officer
		256, HMAC-SHA-384, HMAC-SHA-512 for	installation by DRBG	Type: Ephemeral	Entry: N/A		RWD
		message verification		Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: None		
SN	MP						
40	SNMP AES Key	AES CBC 256-bit key for encryption / decryption of	Internal generation by	Storage: RAM plaintext	Agreement: N/A	Encrypt	Crypto Officer
		SNMP traffic	DRBG	Type: Ephemeral	Entry: N/A	Session Officer R W D Encrypt Crypto Officer R W D User R W D	
				Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		
SSF	1		I			-1	
41	SSH AES Session Key	AES 128, 192, 256 encryption & decryption of	Internal generation at	Storage: RAM plaintext	Agreement: Via secure SSH tunnel	<i>,</i> .	
		management traffic	installation by DRBG	Type: Ephemeral	Entry NI/A		
			DRBG	Association: The system is the one and	Entry: N/A		
				only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		
42	SSH Triple- DES Session	Triple-DES 192 encryption & decryption	Internal generation at	Storage: RAM plaintext	Agreement: Via secure SSH tunnel		
	Кеу	of management traffic	installation by DRBG	Type: Ephemeral	Entry: N/A		R W D
				Association: The system is the one and			User
				only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		RWD

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
43	SSH HMAC key	HMAC-SHA-1, HMAC- SHA-224, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512 for message verification	Internal generation at installation by DRBG	Storage: RAM plaintext Type: Ephemeral Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: None	Establish Session	Crypto Officer R W D User R W D
44	DH Private Key	Private asymmetric key for key establishment ²¹ for XGS TLS connections.	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
45	DH Public Key	Public asymmetric key for key establishment ²² for XGS TLS connections. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation	Storage: RAM plaintext Type: Static Association: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	Agreement: N/A Entry: N/A Output: Key handle from request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
DRI	3G						

 ²¹ Key establishment methodology provides 112 or 128-bits of encryption strength
 ²² Key establishment methodology provides 112 or 128-bits of encryption strength

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
46	DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	Generated internally by non-Approved RNG	Storage: RAM plaintext Type: Ephemeral	Agreement: N/A Entry: N/A	Establish Session	Crypto Officer None
				Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		
47	Entropy Input String	Input value for entropy calculation	Generated internally by	Storage: RAM plaintext	Agreement: N/A	Session C Session C Establish Session C C C C C C C C C C C C C C	Crypto Officer
			non-Approved RNG	Type: Ephemeral	Entry: N/A		None User
				Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		None
48	Hash_DRBG mechanism	V and C values	Generated internally by non-Approved	Storage: RAM plaintext Type: Ephemeral	Agreement: N/A Entry: N/A		Crypto Officer None User None
			RNG	Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		
49	HMAC_DRBG mechanism	V and Key values	Generated internally by	Storage: RAM plaintext	Agreement: N/A		Crypto Officer
			non-Approved RNG	Type: Ephemeral	Entry: N/A		None User
			KNG	Association : The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	Output: N/A		None
50	CTR_DRBG mechanism	V and Key values	Generated internally by	Storage: RAM plaintext	Agreement: N/A		Crypto Officer
				Type: Ephemeral	Entry: N/A		None

#	Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privilege s
			non-Approved				User
			RNG	Association : The system is the one and only owner. Relationship is maintained by the operating system via protected	Output: N/A		None
				by the operating system via protected memory.			

R = Read W = Write D = Delete Table 6 - Key/CSP Management Details

The TLS, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP. Please see NIST document SP800-131A for guidance regarding the use of non FIPS-approved algorithms.

2.10 Self-Tests

The modules include 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 modules will output an error dialog and will shut down. When a module is in an error state, no keys or CSPs will be output and the module will not perform cryptographic functions. The module does not support a bypass function.

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

2.10.1 Power-On Self-Tests

The module uses a default entry point built into the software to ensure that power-on self-tests are run upon every initialization of each module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. Each module implements the following power-on self-tests:

- Module integrity check (HMAC-SHA1)
- OpenSSL Implementation
 - RSA KAT (Signature Generation)
 - RSA KAT (Signature Verification)
 - ECDSA pairwise consistency (Signature Generation)
 - ECDSA pairwise consistency (Signature Verification)
 - AES KAT (Encryption)
 - AES KAT (Decryption)
 - Triple-DES KAT (Encryption)
 - Triple-DES KAT (Decryption)
 - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
 - HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
 - DRBG SP 800-90A KAT
- GSKIT Implementation
 - RSA KAT (Signature Generation)
 - RSA KAT (Signature Verification)
 - ECDSA pairwise consistency (Signature Generation)
 - ECDSA pairwise consistency (Signature Verification)
 - AES KAT (Encryption)
 - AES KAT (Decryption)
 - Triple-DES KAT (Encryption)

- Triple-DES KAT (Decryption)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- DRBG SP 800-90A KAT

Each 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 continuously during operation of each module. If any of these tests fail, the module will enter an error state. The module can be re-initialized to clear the error and resume FIPS mode of operation. No services can be accessed by the operators. Each module performs the following conditional self-tests:

- OpenSSL Implementation
 - Pairwise consistency test for RSA (Signature Generation)
 - Pairwise consistency test for RSA (Signature Verification)
 - Pairwise consistency test for ECDSA implementation (Signature Generation)
 - Pairwise consistency test for ECDSA implementation (Signature Verification)
 - FIPS-Approved DRBG CRNGT
 - NDRNG CRNGT
- GSKIT Implementation
 - Pairwise consistency test for RSA (Signature Generation)
 - Pairwise consistency test for RSA (Signature Verification)
 - Pairwise consistency test for ECDSA implementation (Signature Generation)
 - Pairwise consistency test for ECDSA implementation (Signature Verification)
 - FIPS-Approved DRBG CRNGT
 - NDRNG CRNGT

The module implements the following health conditional tests on the FIPS-approved DRBG:

- OpenSSL Implementation
 - SP 800-90A Health Tests
 - Instantiate Test
 - Generate Test
 - Reseed Test
 - Uninstantiate Test

- GSKIT Implementation
 - SP 800-90A Health Tests
 - Instantiate Test
 - Generate Test
 - Reseed Test
 - Uninstantiate Test

2.11 Mitigation of Other Attacks

The module does not mitigate other attacks.

3. Guidance and Secure Operation

This section describes how to configure the modules for FIPS-approved mode of operation. Operating a 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 Enabling FIPS Mode

When first powering on the module, the operator will be guided through a configuration wizard. In the CLI, the following will appear:

Enable FIPS mode

To initialize the module for FIPS mode, the Crypto Officer must select Y at this prompt then 1 to enable FIPS mode.

Note: The module can only be enabled for FIPS mode at the time of initial configuration. If the module enters an error state (e.g., a known answer test fails), the module must be powered off and reimaged to FIPS mode of operation.

3.2 User Guidance

The User role is defined by a management session over a TLS tunnel. As such, no additional guidance is required to maintain FIPS mode of operation.

3.3 General Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the software version of the module is Version 5.3.1 or Version 5.3.3. No other version can be loaded or used in FIPS mode of operation.
- Only FIPS approved or allowed algorithms and key sizes may be used. Please refer to section 2.3 for more information.