FIPS 140-2 Non-Proprietary Security Policy

IBM Security XGS 3100, XGS 4100, XGS 5100, and XGS 7100

FW version 5.3.1

Document Version 0.9

February 17, 2016

Prepared For:

IBM Security
6303 Barfield Road
Atlanta, GA 30328
www.ibm.com

Prepared By:

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
www.safelogic.com

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140-2

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) runs the FIPS 140-2 program. The CMVP accredits independent testing labs to perform FIPS 140-2 testing; the CMVP also validates test reports for products meeting FIPS 140-2 validation. *Validated* is the term given to a product 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 XGS 3100, XGS 4100, XGS 5100, and XGS 7100 from IBM Security 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-approved mode of operation.

The IBM Security XGS 3100, XGS 4100, XGS 5100, and XGS 7100 may also be referred to as the "modules" in this document.

1.3 External Resources

The IBM Security website (http://www.ibm.com) contains information on the full line of products from IBM Security, including a detailed overview of the XGS 3100, XGS 4100, XGS 5100, and XGS 7100 solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains links to the FIPS 140-2 certificate and IBM Security contact information.

1.4 Notices

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

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
BMC	Baseboard Management Controller (a motherboard system management process)
CBC	Cipher Block Chaining
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
PCT	Pairwise Consistency Test
DTR	Derived Testing Requirement
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
FW	Firmware
GPC	General Purpose Computer
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IBM	International Business Machines
ISS	Internet Security Systems
KAT	Known Answer Test
NDRNG	Non-deterministic Random Number Generator
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SEL	System Error Log
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 IBM Security XGS 3100, XGS 4100, XGS 5100, and XGS 7100

2.1 Product Overview

The Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability. The appliances are purpose-built, Layer 2 network security appliances that you can deploy either at the gateway or the network to block intrusion attempts, denial of service (DoS) attacks, malicious code, backdoors, spyware, peer-to-peer applications, and a growing list of threats without requiring extensive network reconfiguration.

The XGS 3100, XGS 4100, XGS 5100, and XGS 7100 can be securely managed via SiteProtector, which is a central management console for managing appliances, monitoring events, and scheduling reports

2.2 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	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Validation Level	**2**

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.

2.3 Cryptographic Algorithms

2.3.1 Approved Algorithms and Implementation Certificates

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

Algorithm Type	Algorithm	CAVP Certificate	Use
Asymmetric Key	RSA FIPS186-2: ALG[ANSIX9.31]: SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 , ALG[RSASSA-PKCS1_V1_5]: SIG(ver): 1024 , 1536 , 2048 , 3072 , 4096 , SHS, FIPS186-4: 186-4KEY(gen): FIPS186-4_Fixed_e _Value PGM(ProbRandom: (2048 , 3072) PPTT:(C.2 , C.3) ALG[ANSIX9.31] Sig(Ver): (1024 SHA(1 , 256 , 384 , 512)) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(1 , 256 , 384 , 512)) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(224 , 256 , 384 , 512)) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512))	XGS3100: 1691 XGS4100: 1692 XGS5100: 1693 XGS7100: 1694	Sign / verify operations Key transport

Algorithm Type	Algorithm	CAVP Certificate	Use
	ECDSA 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 ExtraRandomBits TestingCandidates) PKV: CURVES(ALL-P ALL-K ALL-B) SigGen: CURVES(P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) P-521: (SHA-224, 256, 384, 512) K-233: (SHA-224, 256, 384, 512) K-283: (SHA-224, 256, 384, 512) K-409: (SHA-224, 256, 384, 512) K-571: (SHA-224, 256, 384, 512) B-233: (SHA-224, 256, 384, 512) B-283: (SHA-224, 256, 384, 512) B-409: (SHA-224, 256, 384, 512) B-571: (SHA-224, 256, 384, 512)) SigVer: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: (SHA-1, 224, 256, 384, 512 B-163: (SHA-1, 224, 256, 384, 512) B-233: (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512)	XGS3100: 640 XGS4100: 641 XGS5100: 642 XGS7100: 643	

Algorithm Type	Algorithm	CAVP Certificate	Use
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	XGS3100: 2740 XGS4100: 2741 XGS5100: 2742 XGS7100: 2743	Message digest in TLS sessions Module integrity via SHA-1
Keyed Hash	HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	XGS3100: 2099 XGS4100: 2100 XGS5100: 2101 XGS7100: 2102	Message verification

Algorithm Type	Algorithm	CAVP Certificate	Use
Symmetric Key	AES ECB (e/d; 128 , 192 , 256); CBC (e/d; 128 , 192 , 256); CFB1 (e/d; 128 , 192 , 256); CFB8 (e/d; 128 , 192 , 256); CFB128 (e/d; 128 , 192 , 256); OFB (e/d; 128 , 192 , 256); CTR (ext only; 128 , 192 , 256) CCM (KS: 128 , 192 , 256) (Assoc. Data Len Range: 0 - 0 , 2^16) (Payload Length Range: 0 - 32 (Nonce Length(s): 7 8 9 10 11 12 13 (Tag Length(s): 4 6 8 10 12 14 16) CMAC (Generation/Verification) (KS: 128; Block Size(s): Full / Partial ; Msg Len(s) Min: 0 Max: 2^16 ; Tag Len(s) Min: 0 Max: 16) (KS: 192; Block Size(s): Full / Partial ; Msg Len(s) Min: 0 Max: 2^16 ; Tag Len(s) Min: 0 Max: 16) (KS: 256; Block Size(s): Full / Partial ; Msg Len(s) Min: 0 Max: 2^16 ; Tag Len(s) Min: 0 Max: 16) GCM (KS: AES_128(e/d) Tag Length(s): 128) (KS: AES_192(e/d) Tag Length(s): 128) (KS: AES_256(e/d) Tag Length(s): 128) IV Generated: (Internally (using Section 8.2.2)) ; PT Lengths Tested: (0 , 128 , 256 , 8 , 248) ; AAD Lengths tested: (0 , 128 , 256) ; IV Lengths Tested: (96 , 1024) ; 96BitIV_Supported ; OtherIVLen_Supported GMAC_Supported	XGS3100: 3307 XGS4100: 3308 XGS5100: 3309 XGS7100: 3310	Data encryption / decryption
	Triple-DES TECB, TCBC, TCFB64, TOFB;	XGS3100: 1883 XGS4100: 1884 XGS5100: 1885 XGS7100: 1886	

Algorithm Type	Algorithm	CAVP Certificate	Use
DRBG 800-90A	DRBG (HMAC_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), HASH_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), CTR_DRBG (AES-128- ECB, AES- 192-ECB, AES-256-ECB)	XGS3100: 756 XGS4100: 757 XGS5100: 758 XGS7100: 759	Deterministic Random Bit Generation

Table 3 – Algorithm Certificates (OpenSSL)

Algorithm		CAVP Certificate	Use
RSA Key Generation	186-4KEY(gen) (2048 to 3072 bits)	XGS3100: 1677 XGS4100: 1679 XGS5100: 1680 XGS7100: 1681	Sign / verify operations Key transport
RSA Signature Generation	PKCS#1.5 (2048 to 3072 bits) (SHA-224,SHA-256,SHA- 384,SHA-512)		
RSA Signature Verification	PKCS#1.5 (1024, 2048, 3072 bits) (SHA-1,SHA-224,SHA- 256,SHA-384,SHA-512)		
ECDSA KeyPair Generation	P: 224, 256, 384, 521 K: 233, 283, 409, 571 B: 233, 283, 409, 571	XGS3100: 633 XGS4100: 635 XGS5100: 636 XGS7100: 637	Sign / verify operations
ECDSA PKV	P: 192, 224, 256, 384, 521 K: 163, 233, 283, 409, 571 B: 163, 233, 283, 409, 571		
ECDSA Signature Generation	P: 224, 256, 384, 521 K: 233, 283, 409, 571 B: 233, 283, 409, 571		
ECDSA Signature Verification	P: 192, 224, 256, 384, 521 K: 163, 233, 283, 409, 571 B: 163, 233, 283, 409, 571		
ECC CDH Component (SP800-56A)	P: 224, 256, 384, 521	XGS 3100 CVL: #463 XGS 4100 CVL: #465 XGS 5100 CVL: #466 XGS 7100 CVL: #467	Cofactor Diffie-Hellman Primitive
SHA message digest generation	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	XGS3100: 2718 XGS4100: 2720 XGS5100: 2721 XGS7100: 2722	Message digest in TLS sessions Module integrity via SHA-1

HMAC	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	XGS3100: 2077 XGS4100: 2079 XGS5100: 2080 XGS7100: 2081	Message verification
AES	AES-128-CMAC, AES-192-CMAC, AES-256-CMAC. ECB, CBC, CFB1, CFB8, CFB128 & OFB AES_CCM 128, 192,or 256 bit keys (SP800-38C) AES_GCM 128, 192,or 256 bit keys (FIPS 197, SP800-38D) AES_XTS 128, 256 bit keys (FIPS SP 800-38E)[1]	XGS3100: 3280 XGS4100: 3282 XGS5100: 3283 XGS7100: 3284	Data encryption / decryption
Triple-DES	Triple-DES 192-bit keys in ECB, CBC, CFB64, and OFB mode, CMAC	XGS3100: 1867 XGS4100: 1869 XGS5100: 1870 XGS7100: 1871	Data encryption / decryption
DRBG 800-90A	HMAC_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), HASH_DRBG (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), CTR_DRBG (AES-128- ECB, AES- 192-ECB, AES-256- ECB)	XGS3100: 738 XGS4100: 740 XGS5100: 741 XGS7100: 742	DRBG
DSA	[(1024, 160) bits; (2048, 224) bits; (2048, 256) bits; (3072, 256) bits] (SHA-1, SHA-224, SHA-256, SHA-256)	XGS 3100 DSA: #937 XGS 4100 DSA: #939 XGS 5100 DSA: #940 XGS 7100 DSA: #941	Verify operations

Table 4 – Algorithm Certificates (GSKIT)

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.

2.3.2 Non-Approved but Allowed Algorithms

The module implements the following non-FIPS approved but allowed algorithms:

- True Random Number Generator (TRNG), a non-deterministic RNG (NDRNG) used to seed the DRBG.
- GSKIT: 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)

[1] AES XTS mode was CAVS validated but not implemented within the module.

- Diffie-Hellman (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength)

- EC Diffie-Hellman (key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)

2.4 Cryptographic Module Specification

The modules are running firmware version 5.3.1. Each module is classified as a multi-chip standalone cryptographic module and contains a cryptographic module to manage secure communications with SiteProtector Management System. The physical cryptographic boundary is defined as the module case (shown in Figure 1).

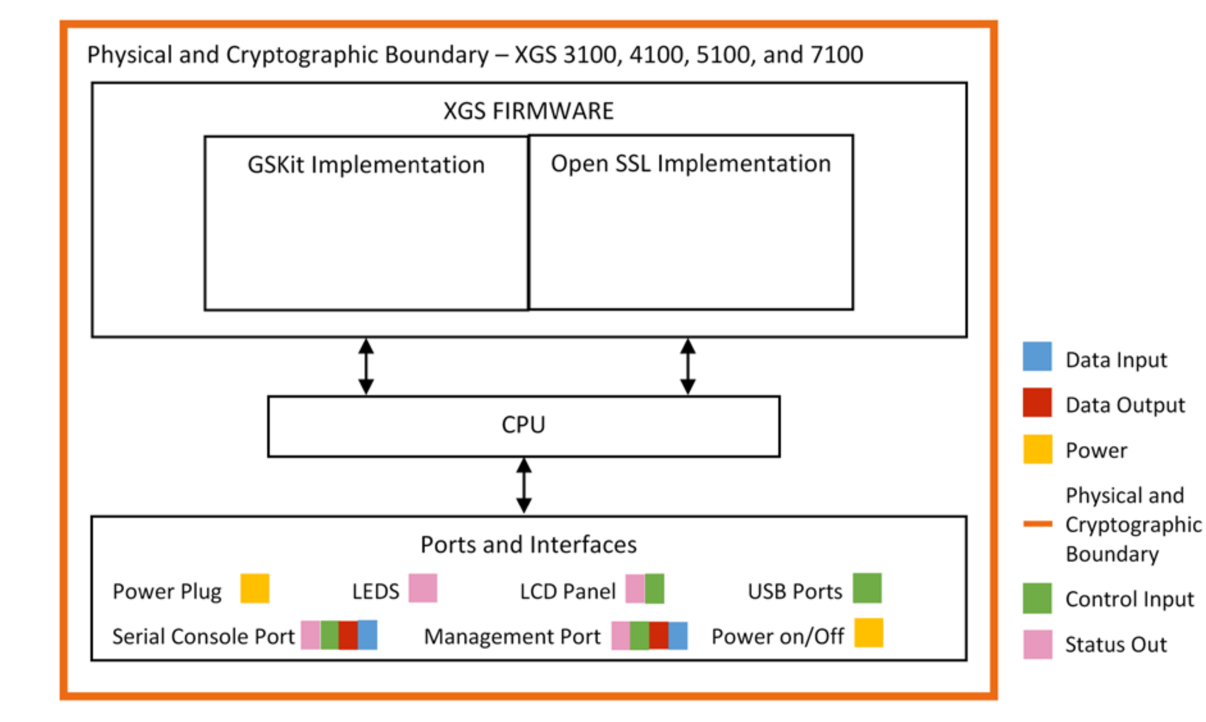

Figure 1 - Block Diagram

2.4.1 Excluded Components

Excluded components include the following:

- Monitoring Ports
  - o The network card provides input/output functionality from the motherboard to the exterior network; it does not provide any FIPS security relevant processing.

  - These 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.

- Management Port 2
  - Excluded when configured for TCP reset

Although the actual data over these interfaces is excluded, the appliances do provide analysis of data. These scan results are encrypted by the cryptographic module and sent to the management interfaces for review.

The module illustrations are provided in the table below. Top to bottom: XGS 3100, XGS 4100, XGS 5100 and XGS 7100.

Figure 2 - Module Illustrations

2.4.2 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 powered off and reimaged to FIPS mode of operation.

2.5 Module Interfaces

Each appliance runs the same version of firmware and has the same basic physical interfaces; the main difference is the number of Monitoring Ports (i.e., traffic monitoring interfaces) and the processing speed. The table below describes the main interface on each module:

Physical Interface	Description / Use
LCD	Initial network configuration, restarting or shutting down the appliance
Monitoring Ports (excluded)	Either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention uses a pair of ports per segment. Passive detection uses a single port per segment. IDS traffic is excluded from the validation.
Serial Console Port	Optional terminal-based setup and recovery
USB Ports	Connection to a CD-ROM or similar peripheral for loading images
Management Port 1	Communication with SiteProtector Management System
Management Port 2 (excluded)	Communication with SiteProtector Management System and for sending TCP Reset responses. This interface is excluded from the validation when configured for TCP Reset processing otherwise it is identical to Management Port #1.

Table 5 – Interface Descriptions

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	Management Port Serial Console Port
Data Output	Management Port Serial Console Port
Control Input	Management Port Serial Console Port USB Ports LCD Panel
Status Output	Management Port Serial Console Port LCD Panel LEDs
Power	Power Plug On/Off Switch

Table 6 – Logical Interface / Physical Interface Mapping

2.6 Roles, Services, and Authentication

The module is accessed via Local Management Interface (LMI), Command Line Interface (CLI) or the SiteProtector management application. The CLI is additionally used for installation and initial configuration of the module. The module supports basic management via the LCD panel during module initialization. The LCD Management is unauthenticated but requires physical access and only allows:

- View the IP address
- Restart the appliance
- Shutdown the appliance

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. The module supports identity-based authentication, and the respective services for each role are described in the following sections.

2.6.1 Management Options[2]

2.6.1.1 Command Line Interface

The command line interface offers the Crypto Officer role basic functions for installation and initial configuration. An authorized Crypto Officer operator can use the CLI to initially configure the following functions:

- Change Password
- Network Configuration Information
- Host Configuration
- Time Zone/Data/Time Configuration
- Agent Name Configuration
- Port Link Configuration
- Adapter Mode Configuration.

Additional commands are below:

[2] Please note that SiteProtector is outside of the module boundary and only the module interface to these applications are relevant to the validation.

```
Current mode commands:
certificates      Work with certificates.
fips              View FIPS 140-2 state and events.
firmware          Work with firmware images.
fixpacks          Work with fix packs.
license           Work with licenses.
logs              Work with log files.
management        Work with management settings.
opensig           Profiling information for Open Signatures.
protection        Work with protection interfaces.
services          Work with certain system services.
session           Work with user sessions.
snapshots         Work with policy snapshot files.
ssh               Work with SSH keys.
support           Work with support information files.
tools             Work with diagnostic tools.
updates           Work with firmware and security updates.
Global commands:
back              Return to the previous command mode.
exit              Log off from the appliance.
help              Display information for using the specified command.
reboot            Reboot the appliance.
shutdown          End system operation and turn off the power.
top               Return to the top level.
unconfigured.appliance:TEST>
```

Figure 3 - Additional CLI Commands

2.6.1.2 LMI

XGS also offers the Crypto-Officer a browser-based graphical user interface for local, single appliance management (LMI) with the functional overlap to the CLI. Besides the functions similar to the CLI, the LMI can also configure IPS related application policies and monitor the security events detected by the appliance.

2.6.1.3 SiteProtector

SiteProtector is the IBM central management console. SiteProtector can manage appliances, monitor events, and schedule reports. If managing a group of appliances along with other sensors, the centralized management capabilities of SiteProtector may be preferred. SiteProtector controls the following management functions of the appliance:

- Monitor appliance status
- View log files
- Configure password

2.6.2 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 (API)	Interface	Key/CSP Access	Roles
Configure	Initializes the module for FIPS mode of operation	Configuration Parameters / Module configured	Serial Console Port USB Ports LCD Panel	None	Crypto Officer
Self Test	Performs self tests on critical functions of module	Initiate self tests / Self tests run	Management Port Power switch	None	Crypto Officer User
Decrypt	Decrypts a block of data	Initiate decryption / data decrypted	Management Port	AES Session Key Triple-DES Session Key Private Key SNMP AES Key	Crypto Officer User
Encrypt	Encrypts a block of data	Initiate encryption/ data encrypted	Management Port	AES Session Key Triple-DES Session Key Public Key External Entity Public Key SNMP AES Key	Crypto Officer User
Establish Session	Provides a protected session for establishment of encryption keys with peers	Initiate session establishment / session established	Management Port	Private Key Public Key HMAC Key Premaster Secret (48 Bytes) Master Secret (48 Bytes) Session Key Symmetric Key External Entity Public Key Session Key DRBG Seed Key Entropy Input String	Crypto Officer User

Service	Description	Service Input / Output (API)	Interface	Key/CSP Access	Roles
				Hash_DRBG mechanism HMAC_DRBG mechanism CTR_DRBG mechanism	
Zeroize CSPs	Clear CSPs from memory	Terminate Session / CSPs cleared	Management Port	None	Crypto Officer User
	Clear CSPs from disk	Reimage module / CSPs cleared and module restored to factory settings	USB Serial	None	Crypto Officer
Show Status	Shows status of the module	Show status commands / Module status	Management Port Serial Console Port USB Ports LCD Panel LEDs	None	Crypto Officer User

Table 7 – Operator Services and Descriptions

2.6.3 Operator Authentication

The CO role authentication via CLI (when initially configuring the module for FIPS mode) is over SSH. The LMI connection is over HTTPS/TLS in FIPS mode. Other than the LCD panel services and status functions available by viewing LEDs, the services described in the table above are available only to authenticated operators.

The operator authenticates via username/password, and passwords are stored on the module. The module checks these parameters before allowing access. The module enforces a minimum password length of 6 characters (see Guidance and Secure Operation section of this document). The password can consist of alphanumeric values, {a-zA-Z0-9], yielding 62 choices per character. The probability of a successful random attempt is $1/62^6$, which is less than 1/1,000,000. Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one minute period is $600/62^6$, which is less than 1/100,000.[3]

[3] The password complexity rules are configurable; users can have more strict password rules. The guidance The minimum password length can be configured to be 6 to 15 characters and can be configured to require special, numeric, upper and lower case characters. The default minimum password length is 6 characters, and the account should be locked after 3 unsuccessful attempts; therefore this analysis.

Per the Configuration Guidance, the module will lock an account after 3 failed authentication attempts; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one minute period is $3/62^6$ which is less than 1/100,000.

For authentication of SiteProtector sessions (i.e., the User Role), the module supports a public key based authentication with 2048 bit keys via RSA. A 2048-bit RSA key has 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

Each module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. The modules' production-grade enclosure is made of a hard metal, and the enclosures contain a removable cover. The baffles installed by IBM Security satisfy FIPS 140-2 Level 2 requirements for module opacity. For details on tamper evidence, please see Section 1.16.4 – Placement of Tamper Evidence Labels.

2.8 Operational Environment

The modules operate in a limited operational environment and do not implement a General Purpose Operating System.

The modules meet 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.

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	Privileges
GSKIT Implementation						
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**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
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**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
HMAC key	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 for	Internal generation at installation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

	message verification		**Association**: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: None		User R W D
Crypto Officer Password	Alphanumeric passwords externally generated by a human user for authentication to the operating system.	Not generated by the module; defined by the human user of the workstation	**Storage**: on disk/obfuscated **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry via operating system **Output**: NA	Configure	Crypto Officer R W D
User Password	Alphanumeric passwords externally generated by a human user for authentication to the operating system.	Not generated by the module; defined by the human user of the workstation	**Storage**: on disk/obfuscated **Type:** Static **Association**: controlled by the operating system	**Agreement**: NA **Entry**: Manual entry via operating system **Output**: NA	Configure	Crypto Officer D User R W
External Entity Public Key	RSA Public key associated with remote entities (such as SiteProtector)	External generation by FIPS-approved technique	**Storage**: RAM plaintext **Type:** Ephemeral **Association**: The system is the one and only owner. Relationship is maintained by the operating system via X509 certificates.	**Agreement**: NA **Entry**: Plaintext **Output**: NA	Establish Session	Crypto Officer R W D User R W D
DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	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**: NA		User None
Entropy Input String	Input value for entropy calculation	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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None

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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
RSA Private Key	Private key for sign / verify operations and key establishment[4] for XGS TLS connections	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 protected memory.	**Agreement**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R
RSA Public Key	Public key for sign / verify operations and key establishment[5] 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**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R

[4] Key establishment methodology provides 112 or 128 bits of encryption strength
[5] Key establishment methodology provides 112 or 128 bits of encryption strength

ECDHE Private Key	Private asymmetric key for key establishment[6] 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**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R
ECDHE Public Key	Public asymmetric key for key establishment[7] 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**: NA **Entry**: NA **Output**: Key handle from API request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
ECDSA Private Key	Private key for sign / verify operations and key establishment for XGS 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**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R

[6] Key establishment methodology provides between 128 and 256 bits of encryption strength
[7] Key establishment methodology provides between 128 and 256 bits of encryption strength

ECDSA Public Key	Public key for sign / verify operations and key establishment for XGS 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**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
DSA Public Key	Public key for sign / verify operations and key establishment for XGS 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**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
OpenSSL Implementation						
Session Key	AES CBC 256-bit key for encryption / decryption of management traffic	Derived from the Master Secret	**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**: NA **Output**: NA	Decrypt Encrypt	Crypto Officer R W D User R W D
DRBG Seed	160-bit system Entropy seed the DBRG	Use dev/random to gather bytes from several areas of system data (including	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

		time/date), concatenate them together and hash via SHA-1	**Association:** The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
RSA Private Key	Private key for sign / verify operations and key establishment[8] for XGS TLS connections	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 protected memory.	**Agreement**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R
RSA Public Key	Public key for sign / verify operations and key establishment[9] 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**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R
ECDHE Private Key	Private asymmetric key for key establishment[10] for XGS TLS connections.	Internal generation	**Storage**: RAM plaintext **Type:** Static	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer R W D

[8] Key establishment methodology provides 112 or 128 bits of encryption strength
[9] Key establishment methodology provides 112 or 128 bits of encryption strength
[10] Key establishment mythology provides between 128 and 256 bits of encryption strength

			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: None		User R
ECDHE Public Key	Public asymmetric key for key establishment[11] 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 X509 certificates.	**Agreement**: NA **Entry**: NA **Output**: Key handle from API request is output only to the SiteProtector application	Establish Session	Crypto Officer R W D User R
Premaster Secret (48 Bytes)	RSA-Encrypted 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**: NA **Entry**: Input during TLS negotiation **Output**: Output to server encrypted by Public Key	Establish Session	Crypto Officer None User None
Master Secret (48 Bytes)	Used for computing the Session Key	Internal generation by DRBG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

[11] Key establishment mythology provides between 128 and 256 bits of encryption strength

			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
SNMP AES Key	AES CBC 256-bit key for encryption / decryption of SNMP traffic	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**: NA **Entry**: NA **Output**: NA	Encrypt	Crypto Officer R W D User R W D
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**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R W D
DRBG Seed Key	256-bit value to seed the FIPS-approved DRBG	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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None

Entropy Input String	Input value for entropy calculation	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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
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**: NA **Entry**: NA **Output**: NA	Establish Session	Crypto Officer None User None
CTR_DRBG mechanism	V and Key values	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	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**: NA		User None
ECDSA Private Key	Private key for sign / verify operations and key establishment for XGS 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**: NA **Entry**: NA **Output**: None	Establish Session	Crypto Officer R W D User R
ECDSA Public Key	Public key for sign / verify operations and key establishment for XGS 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**: NA **Entry**: NA **Output**: plaintext during TLS negotiation	Establish Session	Crypto Officer R W D User R

R = Read W = Write D = Delete

Table 8 - Key/CSP Management Details

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 to not have write access to modify, change, or delete a public key. Ephemeral CSPs are zeroized by the RAM clearing processes, and static CSPs are zeroized by reimaging the module.

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

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:

- Critical functions test: Checks, identifies, and initializes system devices such as the CPU, RAM, interrupt and DMA controllers and other parts of the chipset, BIOS FW integrity, video display memory, Storage drive, PCIe bus, network cards. System high-level POST issues are reported to the BMC, where the events are logged into the SEL.
- Module integrity check for OpenSSL and components other than GSKit are by digital signature verification based on a 3072-bit CAVS-validated RSA public key using SHA-256 hashing. The signatures are created when the modules are created by IBM. Signature verification is done performed before module initialization (part of system load procedure).
- Module integrity check for the GSKit cryptographic library is via 2048-bit CAVS-validated RSA public key (PKCS#1.5) and a single HMAC SHA-1 digest calculated over the module at the time it is created. This RSA public key is stored inside the static stub and relies on the operating system for protection. Self-test and library verification is performed at library load by hooking the shared library's 'call on load' entry points.

OpenSSL Implementation

Algorithm	Type	Description

SHA	KAT	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
HMAC	KAT	One KAT per SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
AES	KAT	Separate encrypt and decrypt, ECB mode, 128 bit key length
AES CCM	KAT	Separate encrypt and decrypt, 192 key length
AES GCM	KAT	Separate encrypt and decrypt, 256 key length
AES CMAC	KAT	Sign and verify CBC mode, 128, 192, 256 key lengths
Triple-DES	KAT	Separate encrypt and decrypt, ECB mode, 3Key
Triple-DES CMAC	KAT	CMAC generate and verify, CBC mode, 3Key
RSA	KAT	Sign and verify using 2048 bit key, SHA256,PKCS#1, pairwise consistency test
DRBG	KAT	CTR_DRBG: AES, 256 bit with and without derivation function, HASH_DRBG: SHA256, HMAC_DRBG: SHA256
ECDSA	PCT	KeyGen, sign, verify using P224, K233 and SHA512, pairwise consistency test
RSA	PCT	RSA Pairwise consistency test on each generation of a key pair

Table 9 - OpenSSL Self-Tests

GSKIT Implementation

Algorithm	Type	Description
RSA	PCT	Pairwise consistency test
RSA	KAT	signature generation with 2048 modulus
RSA	KAT	signature verification with 2048 modulus
RSA	KAT	encryption with 2048 modulus
RSA	KAT	decryption with 2048 modulus
ECDSA	PCT	pairwise consistency test with P-384
ECDSA	KAT	signature verification with P-384
ECDSA	PCT	pairwise consistency test with B-233
ECDSA	KAT	signature verification with B-233
ECDSA	PCT	pairwise consistency test with K-233
ECDSA	KAT	signature verification with K-233
Triple-DES–CBC	KAT	separate encrypt and decrypt
AES 256–CBC	KAT	separate encrypt and decrypt
AES_GCM	KAT	separate encrypt and decrypt

AES_CCM	KAT	separate encrypt and decrypt
SHA	KAT	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
HMAC	KAT	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
DRBG 800-90A	KAT	CTR_DRBG: AES, 256 bit with and without derivation function, HASH_DRBG: SHA256, HMAC_DRBG: SHA256
DSA	PCT	Sign and verify using 2048 bit key
ECC CDH	KAT	Shared secret calculation per SP 800-56A §5.7.1.2, IG 9.6
DSA	KAT	Signing and signature verification

Table 10 - GSKIT Self-Tests

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 test 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
  - DRBG 800-90A
    - Health Tests compliant with SP 800-90A – Section 11.3.
    - The DRBG 800-90A generates a minimum of 8 bytes per request. If less than 8 bytes are requested, the rest of the bytes is discarded and the next request will generate new random data.
    - The first 8 bytes of every request is compared with the last 8 bytes requested, if the bytes match an error is generated.
    - For the first request made to any instantiation of a DRBG 800-90A, two internal 8 byte cycles are performed.
    - The DRBG 800-90A relies on the environment (i.e. proper shutdown of the shared libraries) for resistance to retrospective attacks on data.
    - The DRBG 800-90A performs known answer tests when first instantiated and health checks at intervals as specified in the standard.
  - True Random Number Generator (TRNG)

    - A non-deterministic RNG (NDRNG) is used to seed the DRBG. Every time a new seed or n bytes is required (either to initialize the DRBG, reseed the DRBG periodically or reseed the DRBG by user's demand), the cryptographic module performs a comparison between the SHA-256 message digest using the new seed and the previously calculated digest. If the values match, the TRNG generates a new stream of bytes until the continuous DRBG test passes.
  - DRBG FIPS 140-2 continuous test for stuck fault
  - ECDSA Pairwise consistency test on each generation of a key pair
  - RSA Pairwise consistency test on each generation of a key pair

- GSKIT Implementation
  - Pairwise consistency test for RSA (Signature Generation, Signature Verification, Key Generation, Key Wrapping)
  - Pairwise consistency test for ECDSA (KeyPair Generation, PKV, Signature Generation, Signature Verification)
  - DSA Pairwise consistency test on each generation of a key pair
  - DRBG 800-90A
    - Health Tests compliant with SP 800-90A – Section 11.3.
    - The DRBG 800-90A generates a minimum of 8 bytes per request. If less than 8 bytes are requested, the rest of the bytes is discarded and the next request will generate new random data.
    - The first 8 bytes of every request is compared with the last 8 bytes requested, if the bytes match an error is generated.
    - For the first request made to any instantiation of a DRBG 800-90A, two internal 8 byte cycles are performed.
    - The DRBG 800-90A relies on the environment (i.e. proper shutdown of the shared libraries) for resistance to retrospective attacks on data.
    - The DRBG 800-90A performs known answer tests when first instantiated and health checks at intervals as specified in the standard.
  - True Random Number Generator (TRNG)
    - A non-deterministic RNG (NDRNG) is used to seed the DRBG. Every time a new seed or n bytes is required (either to initialize the DRBG, reseed the DRBG periodically or reseed the DRBG by user's demand), the cryptographic module performs a comparison between the SHA-256 message digest using the new seed and the previously calculated digest. If the values match, the TRNG generates a new stream of bytes until the continuous DRBG test passes.

The module will inhibit data output via the output interface when conditional tests are performed. Once the tests have passed and the keys have been generated, the module will pass the key to the calling daemon.

The modules do not perform a firmware load test because no additional firmware can be loaded in the module while operating in FIPS-approved mode. Please see Section 3 for guidance on configuring and maintaining FIPS mode.

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.

All updates via the My Software | Download menu are signed using SP 800-131a validated algorithms with RSA-3072 key-pair and SHA-256 integrity hash.

3.1 Crypto Officer Guidance

3.1.1 Firmware Installation

To install the appliance firmware, please follow these steps:

1. Log in to the ISS support site at https://ibmss.flexnetoperations.com/,
2. Select **My Software | Download** from the menu
3. Choose **IBM Security Network Protection (XGS)** and then the specific XGS model.
4. Select the appropriate firmware and recovery images from the **New Versions** dropdown menu then select **Go**
5. Accept the End User License and select **Submit**
6. Select the appropriate Recovery image type (USB image)
7. Download the ***.img** image and follow the installation instructions.

3.1.2 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. Additionally, 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.

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

- Verify that the firmware version of the module is Version 5.3.1. No other version can be loaded or used in FIPS mode of operation.
- Apply tamper evidence labels as specified in Section 1.16.4 – Placement of Tamper Evidence Labels. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation.
- Ensure any unused labels are secure at all times.
- Inspect the tamper evidence labels periodically to verify they are intact.
- Do not disclose passwords and store passwords in a safe location and according to his/her organization's systems security policies for password storage.
- Root privilege to the module must be disabled.
- Configure the module to lock accounts after 3 unsuccessful authentication attempts.

3.1.3 Placement of Tamper Evidence Labels

To meet Physical Security Requirements for Level 2, each module enclosure must be protected with tamper evidence labels. The tamper evident labels shall be installed for the module to operate in a FIPS Approved mode of operation. The Crypto Officer is responsible for applying the labels; IBM Security does not apply the labels at time of manufacture. Once applied, the Crypto Officer shall not remove or replace the labels unless the module has shown signs of tampering, in which case the Crypto Officer shall reimage the module and follow all Guidance to place the module in FIPS mode.

Please note that if additional labels need to be ordered, the Crypto Officer shall contact IBM Security support and request part number *00VM255*.

The Crypto Officer is responsible for

- securing and having control at all times of any unused seals, and
- maintaining the direct control and observation of any changes to the module such as reconfigurations where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Important – Do not disturb labels for 10 minutes after application. You must allow labels to set for 24 hours at room temperature to reach full tamper resistance.

3.1.3.1 XGS 3100

Up to five tamper evidence labels are required for XGS FIPS 140-2 Level 2 deployments. (Functional NIMs do not need tamper labels.) Application of the tamper evidence labels is as follows:

Note – Tamper labels are very fragile. Handle with care.

1. Turn off and unplug the system.
2. Clean the enclosure before you apply the tamper evidence labels.
3. Place Label #1 over the top left side of the enclosure, covering the cover screw, as shown in Figure 4 – XGS 3100 Tamper evidence label placement (top left).
4. Place Label #2 over the bottom back side of the enclosure, covering the bottom right corner of the left fan (1), as shown in Figure 5 – XGS 3100 Tamper evidence label placement (bottom back).
5. Place Label #3 over the bottom back side of the enclosure, covering the bottom right corner of the middle fan (2), as shown in Figure 5 – XGS 3100 Tamper evidence label placement (bottom back).
6. Place Label #4 over the bottom back side of the enclosure, covering the bottom right corner of the right fan (3), as shown in Figure 5 – XGS 3100 Tamper evidence label placement (bottom back).

7. Place Label #5 over the top front side of the enclosure, covering the right side of the storage tray (1), as shown in Figure 6 - XGS 3100 Tamper evidence label placement (top front).

Important – Do not disturb labels for 10 minutes after application. You must allow labels to set for 24 hours at room temperature to reach full tamper resistance.

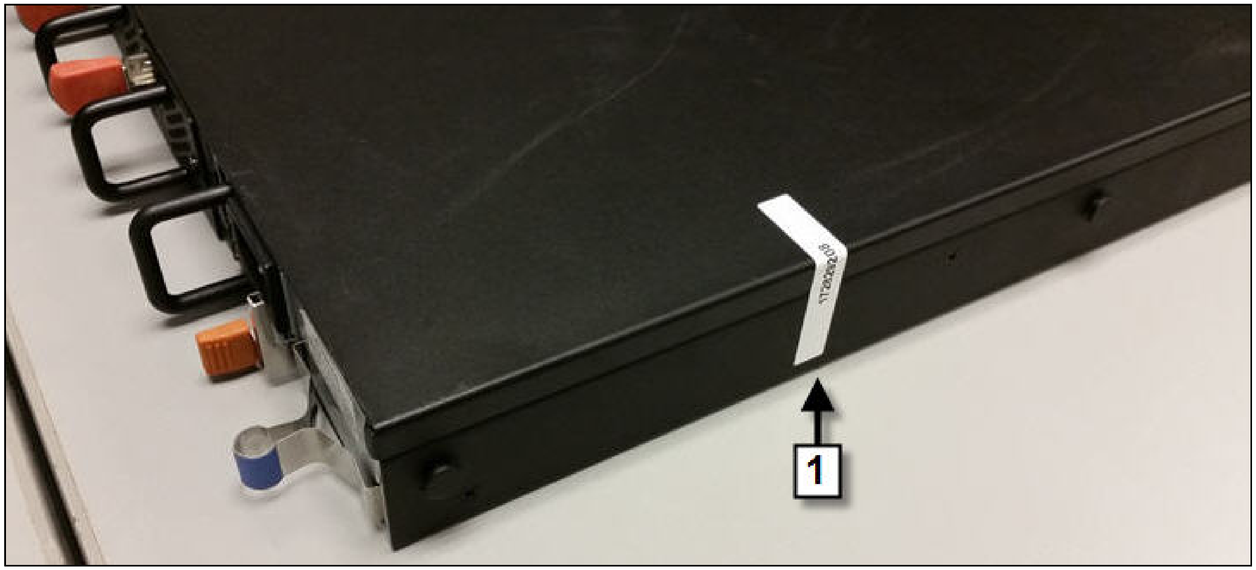

Figure 4 - XGS 3100 Tamper evidence label placement (top left)

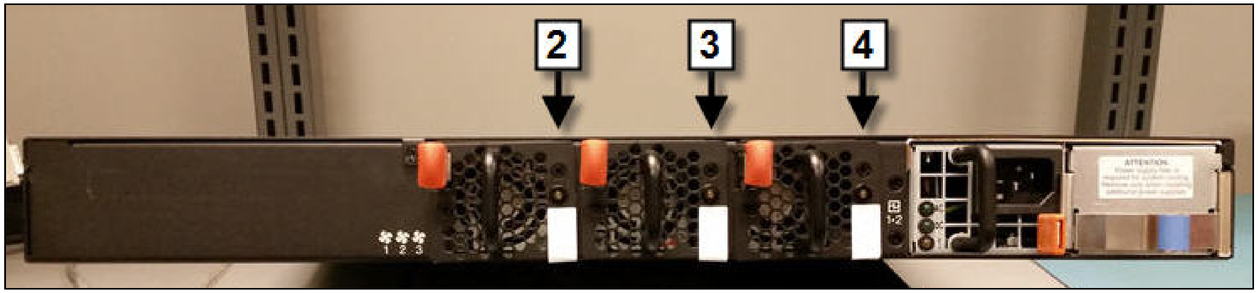

Figure 5 – XGS 3100 Tamper evidence label placement (bottom back)

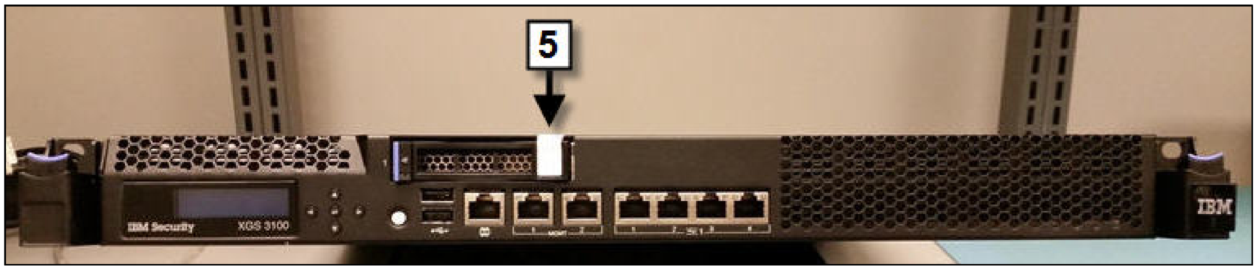

Figure 6 - XGS 3100 Tamper evidence label placement (top front)

3.1.3.2 XGS 4100

Up to seven tamper evidence labels are required for XGS FIPS 140-2 Level 2 deployments. (Functional NIMs do not need tamper labels.) Application of the tamper evidence labels is as follows:

Note – Tamper labels are very fragile. Handle with care.

1. Turn off and unplug the system.
2. Clean the enclosure before you apply the tamper evidence labels.

3. Place Label #1 over the top left side of the enclosure, covering the cover screw, as shown in Figure 7 – XGS 4100 Tamper evidence label placement (top left).
4. Place Label #2 over the bottom back side of the enclosure, covering the bottom right corner of the left fan (1), as shown in Figure 8 – XGS 4100 Tamper evidence label placement (bottom back).
5. Place Label #3 over the bottom back side of the enclosure, covering the bottom right corner of the middle fan (2), as shown in Figure 8 – XGS 4100 Tamper evidence label placement (bottom back).
6. Place Label #4 over the bottom back side of the enclosure, covering the bottom right corner of the right fan (3), as shown in Figure 8 – XGS 4100 Tamper evidence label placement (bottom back).
7. Place Label #5 over the top front side of the enclosure, covering the right side of the left storage (1) tray, as shown in Figure 9 – XGS 4100 Tamper evidence label placement (top and bottom front).
8. Place Label #6 over the top front side of the enclosure, covering the right side of the right storage tray (2), as shown in Figure 9 – XGS 4100 Tamper evidence label placement (top and bottom front).
9. Place Label #7 over the bottom front side of the enclosure, covering the middle of the NIM (2), as shown in Figure 9 – XGS 4100 Tamper evidence label placement (top and bottom front).

Important – Do not disturb labels for 10 minutes after application. You must allow labels to set for 24 hours at room temperature to reach full tamper resistance.

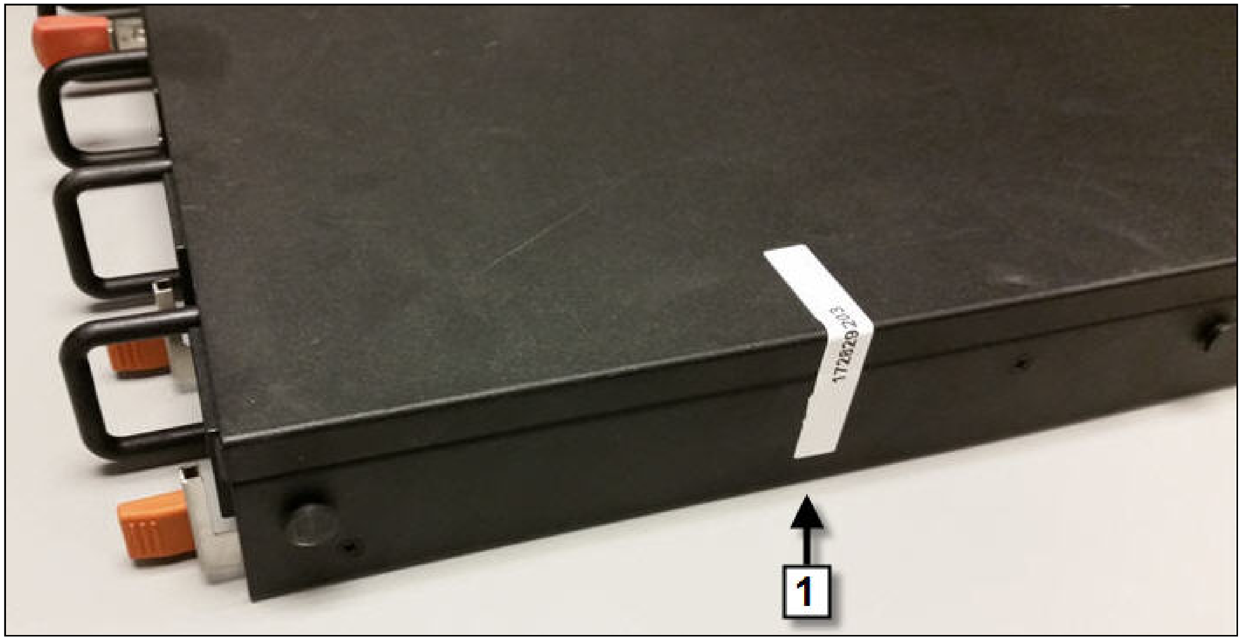

Figure 7 - XGS 4100 Tamper evidence label placement (top left).

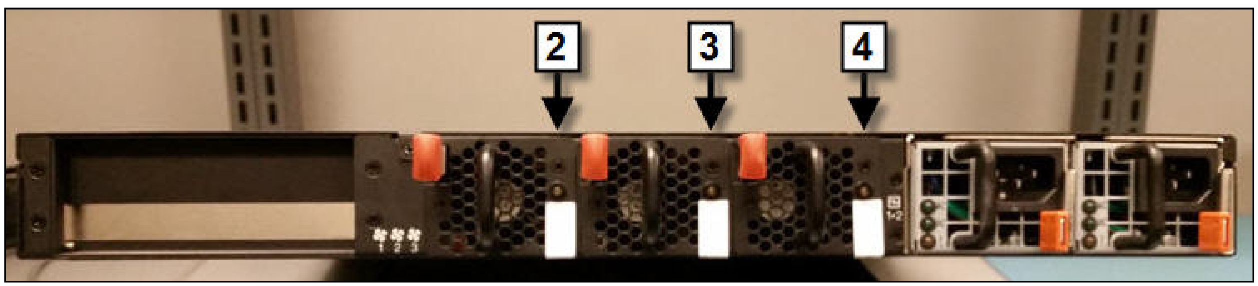

Figure 8 – XGS 4100 Tamper evidence label placement (bottom back)

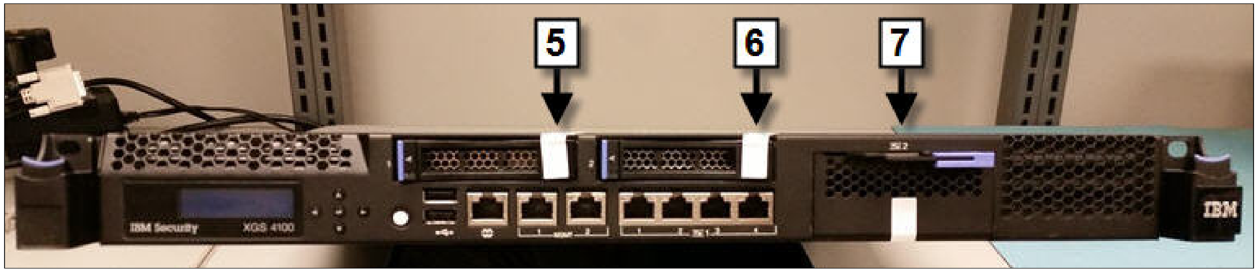

Figure 9 – XGS 4100 Tamper evidence label placement (top and bottom front)

3.1.3.3 XGS 5100

Up to eight tamper evidence labels are required for XGS FIPS 140-2 Level 2 deployments. (Functional NIMs do not need tamper labels.) Application of the tamper evidence labels is as follows:

Note – Tamper labels are very fragile. Handle with care.

1. Turn off and unplug the system.
2. Clean the enclosure before you apply the tamper evidence labels.
3. Place Label #1 over the top left side of the enclosure, covering the cover screw, as shown in Figure 10– XGS 5100 Tamper evidence label placement (top left).
4. Place Label #2 over the bottom back side of the enclosure, covering the bottom left corner of the left fan (1), as shown in Figure 11 – XGS 5100 Tamper evidence label placement (bottom back).
5. Place Label #3 over the bottom back side of the enclosure, covering the bottom left corner of the middle fan (2), as shown in Figure 11 – XGS 5100 Tamper evidence label placement (bottom back).
6. Place Label #4 over the bottom back side of the enclosure, covering the bottom left corner of the right fan (3), as shown in Figure 11 – XGS 5100 Tamper evidence label placement (bottom back).

7. Place Label #5 over the top front side of the enclosure, covering the right side of the left storage tray (1), as shown in Figure 12 – XGS 5100 Tamper evidence label placement (top and bottom front).

8. Place Label #6 over the top front side of the enclosure, covering the right side of the right storage tray (2), as shown in Figure 12 – XGS 5100 Tamper evidence label placement (top and bottom front).

9. Place Label #7 over the bottom front side of the enclosure, covering the middle of the left NIM (2), as shown in Figure 12 – XGS 5100 Tamper evidence label placement (top and bottom front).

10. Place Label #8 over the bottom front side of the enclosure, covering the middle of the right NIM (3), as shown in Figure 12 – XGS 5100 Tamper evidence label placement (top and bottom front).

Important – Do not disturb labels for 10 minutes after application. You must allow labels to set for 24 hours at room temperature to reach full tamper resistance.

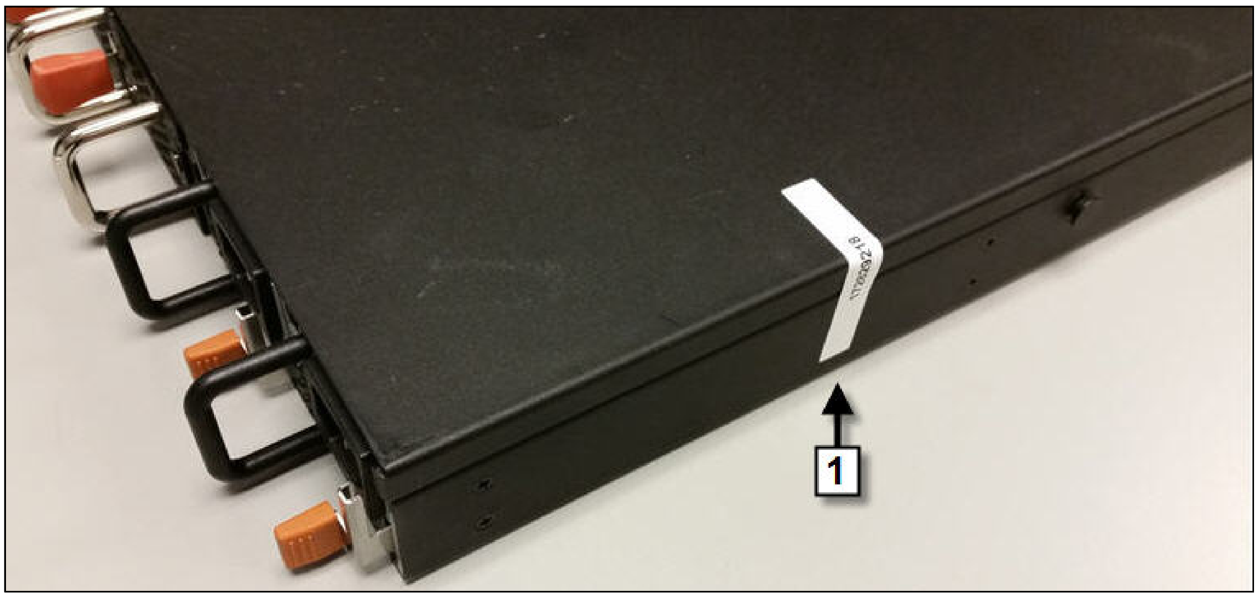

Figure 10 – XGS 5100 Tamper evidence label placement (top left)

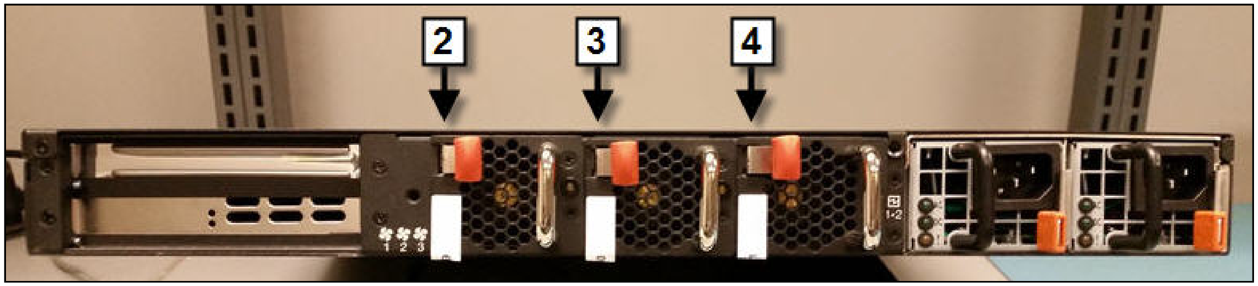

Figure 11 – XGS 5100 Tamper evidence label placement (bottom back)

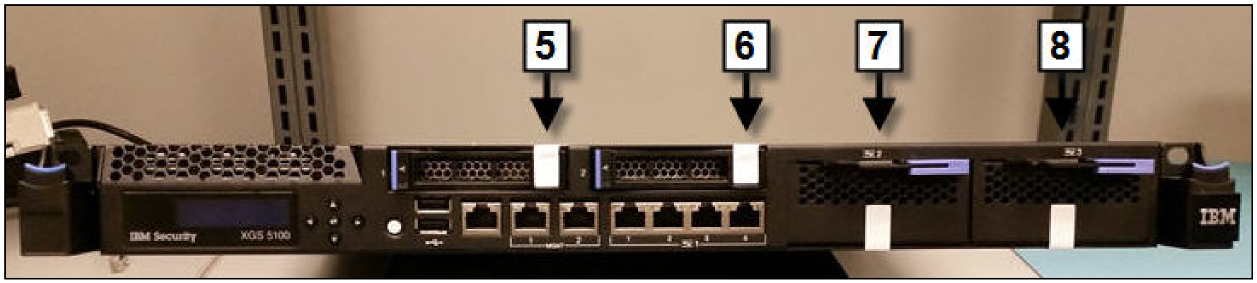

Figure 12 – XGS 5100 Tamper evidence label placement (top and bottom front)

3.1.3.4 XGS 7100

Up to 10 tamper evidence labels are required for XGS FIPS 140-2 Level 2 deployments. (Functional NIMs do not need tamper labels.) Application of the tamper evidence labels is as follows:

Note – Tamper labels are very fragile. Handle with care.

1. Turn off and unplug the system.
2. Clean the enclosure before you apply the tamper evidence labels.
3. Place Label #1 over the top left side of the enclosure, covering the cover screw, as shown in Figure 13 – XGS 7100 Tamper evidence label placement (top left).

4. Place Label #2 over the bottom back side of the enclosure, covering the bottom left corner of the left fan (1), as shown in Figure 14 – XGS 7100 Tamper evidence label placement (bottom back).

5. Place Label #3 over the bottom back side of the enclosure, covering the bottom left corner of the middle fan (2), as shown in Figure 14 – XGS 7100 Tamper evidence label placement (bottom back).

6. Place Label #4 over the bottom back side of the enclosure, covering the bottom left corner of the right fan (3), as shown in Figure 14 – XGS 7100 Tamper evidence label placement (bottom back).

7. Remove left NIM (1), place Label #5 in the middle of the bottom of the left storage tray (1), and then wrap the label up over the storage tray so that it covers the middle of the storage tray, as shown in Figure 15 – XGS 7100 Tamper evidence label placement (top and bottom front). Replace the left NIM.

8. Remove second from the left NIM (2), place Label #6 on the middle of the bottom the left storage tray (2), and then wrap the label up over the storage tray so that it covers the middle of the storage tray, as shown in Figure 15 – XGS 7100 Tamper evidence label placement (top and bottom front). Replace the second from the left NIM.

9. Place Label #7 over the bottom front side of the enclosure, covering the middle of the left NIM (1), as shown in Figure 15 – XGS 7100 Tamper evidence label placement (top and bottom front).

10. Place Label #8 over the bottom front side of the enclosure, covering the middle of the second from the left NIM (2), as shown in Figure15 – XGS 7100 Tamper evidence label placement (top and bottom front).

11. Place Label #9 over the bottom front side of the enclosure, covering the middle of the third from the left NIM (3), as shown in Figure 14 – XGS 7100 Tamper evidence label placement (top and bottom front).

12. Place Label #10 over the bottom front side of the enclosure, covering the middle of the fourth from the left NIM (4), as shown in Figure 15 – XGS 7100 Tamper evidence label placement (top and bottom front).

Important – Do not disturb labels for 10 minutes after application. You must allow labels to set for 24 hours at room temperature to reach full tamper resistance.

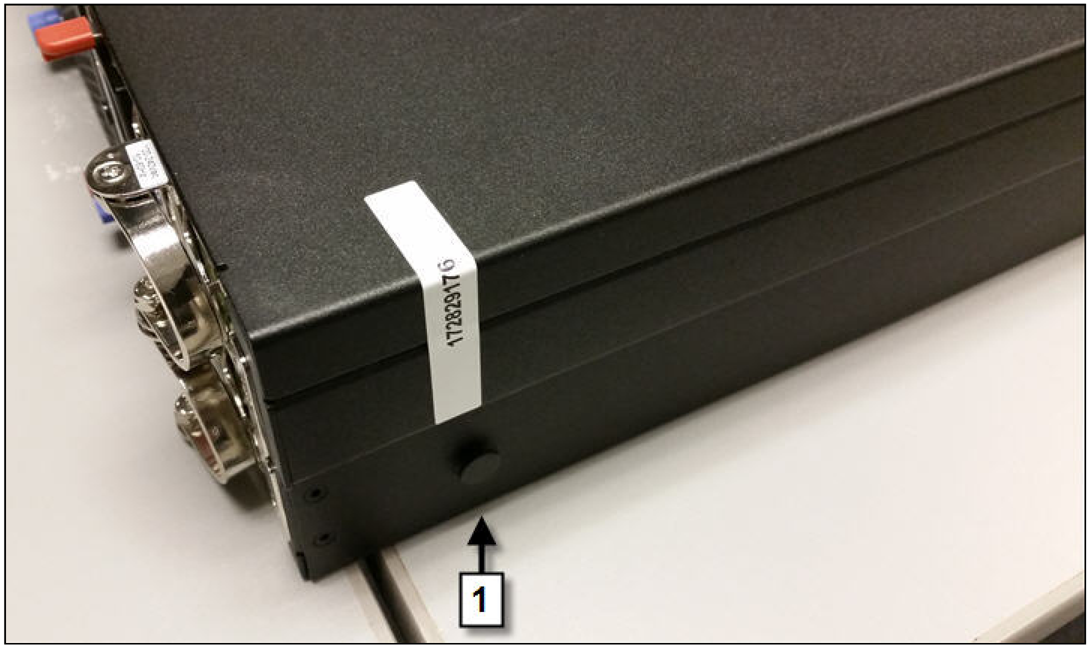

Figure 13 – XGS 7100 Tamper evidence label placement (top left)

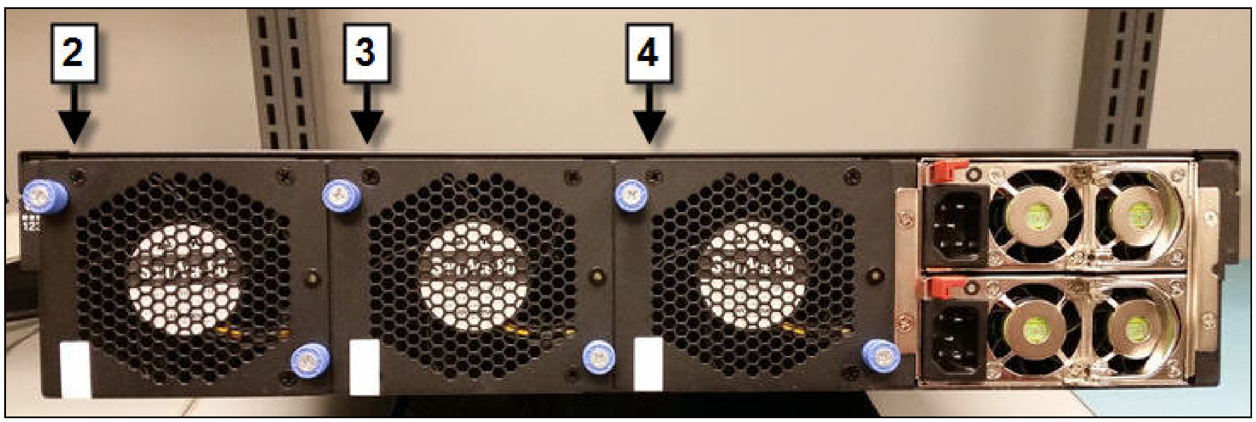

Figure 14 – XGS 7100 Tamper evidence label placement (bottom back)

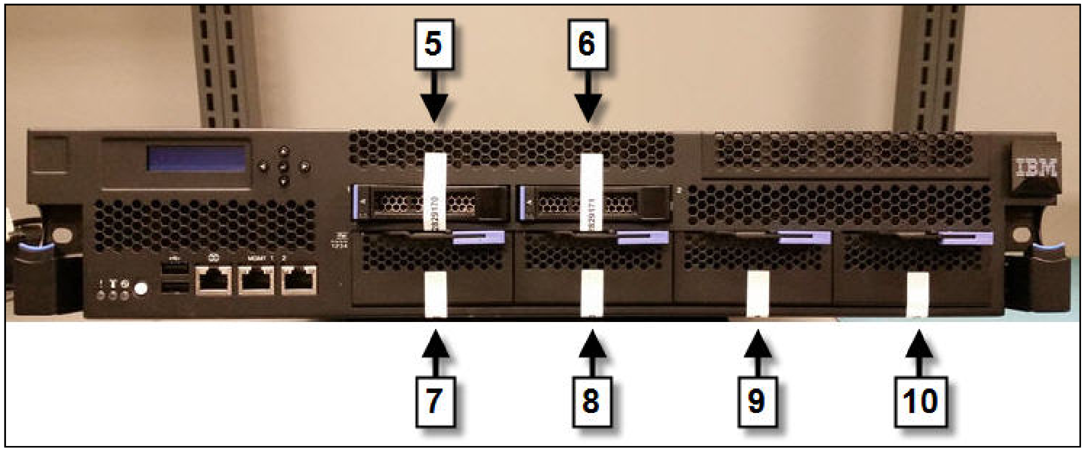

Figure 15 – XGS 7100 Tamper evidence label placement (top and bottom front)

3.2 User Guidance

3.2.1 General Guidance

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

End of Document
