FIPS 140-2 Non-Proprietary Security Policy

IBM Internet Security Systems SiteProtector Cryptographic Module (Version 1.0)

Document Version 2.3

August 5, 2010

Prepared For:

IBM Internet Security Systems, Inc.

6303 Barfield Road

Atlanta, GA 30328

www.iss.net

Prepared By:

Apex Assurance Group, LLC

555 Bryant Street, Ste. 804

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides a non-proprietary FIPS 140-2 Security Policy for the SiteProtector Cryptographic Module (Version 1.0).

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP) runs the FIPS 140 program. The CMVP accredits independent testing labs to perform FIPS 140 testing; the CMVP also validates test reports for products meeting FIPS 140 validation. *Validated* is the term given to a product that is documented and tested against the FIPS 140 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 SiteProtector Cryptographic Module (Version 1.0) from IBM Internet Security Systems provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

The IBM Internet Security Systems SiteProtector Cryptographic Module (Version 1.0) may also be referred to as the "module" in this document.

1.3 External Resources

The IBM Internet Security Systems website (http://www.iss.net) contains information on the full line of products from IBM Internet Security Systems, including a detailed overview of the SiteProtector Cryptographic Module (Version 1.0) solution. The Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm) contains links to the FIPS 140-2 certificate and IBM Internet Security Systems 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
CBC	Cipher Block Chaining
CSEC	Communications Security Establishment of Canada
CSP	Critical Security Parameter
DTR	Derived Testing Requirement
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GPOS	General Purpose Operating System
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
IBM	International Business Machines
ISS	Internet Security Systems
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
RSA	Rivest Shamir Adelman
SHA	Secure Hashing Algorithm

Table 1 – Acronyms and Terms

2 IBM Internet Security Systems SiteProtector Cryptographic Module (Version 1.0)

2.1 Product Overview

SiteProtector is a centralized management system that unifies management and analysis for network, server, and desktop protection agents and small networks or appliances. The SiteProtector is used as the central controlling point for IBM ISS appliances deployed on the network. The SiteProtector performs the following functionality:

- Manages and monitors Sensors and SiteProtector sub-components;
- Enables an administrator to view configuration data of a GX series appliance;
- Displays audit and system data records; and
- Monitors the network connection between SiteProtector and the Sensors it is configured to monitor.

2.2 Cryptographic Module Specification

The module is the IBM Internet Security Systems SiteProtector Cryptographic Module (Version 1.0), provides the SiteProtector application with the means to encrypt management session to a managed Sensor. The module is a software-only module installed on a multi-chip standalone device, such as a General Purpose Computer running a General Purpose Operating System and provides cryptographic services to the IBM Internet Security Systems SiteProtector application.

The module is a uniquely identifiable library that is linked into the SiteProtector application. All operations of the module occur via calls from the SiteProtector application, which occur only when an operator is successfully authenticated to the host operating system. As such there are no untrusted services or daemons calling the services of the module. No security functions outside the cryptographic module provide FIPS-relevant functionality to the module.

The module is comprised of the following files:

- \ISS\SiteProtector\Agent Manager\agentmgr.dll
- \ISS\SiteProtector\Agent Manager\issSessionConfigSvcs5.dll

- \ISS\SiteProtector\Application Server\webserver\Apache2\bin\issSessionConfigSvcs5.dll
- \ISS\SiteProtector\Application Server\webserver\Apache2\modules\mod_ssl.so
- \ISS\SiteProtector\Event Collector\issSessionConfigSvcs5.dll
- \ISS\SiteProtector\FIPS Service\FipsService.exe

This module provides no non-FIPS approved mode of operation. Although the module requires no further configuration or compilation, the procedures in the Guidance and Secure Operation must be followed.

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

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 Algorithm Implementation Certificates

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

Algorithm Type	Algorithm	Standard	CAVP Certificate	Use
Asymmetric Key	RSA with 1536-bit modulus	RFC2246 (TLS v1.0, PKCS1.5)	562	Sign / verify operations Key establishment
Hashing	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	FIPS 186-3	1090	Message digest in TLS sessions
Keyed Hash	HMAC-SHA1	FIPS 198	681	Message integrity in TLS sessions and module integrity check
Symmetric Key	AES 256 in CBC mode	FIPS 197	1181	Data encryption/ decryption
Random Number Generation	ANSI X9.31	X9.31 (TDES)	652	Random Number Generation

Table 3 – FIPS-Approved Algorithm Certificates

2.4.2 Non-Approved Algorithms

The module implements the following non-FIPS approved algorithms:

- Software-based random number generator (rand_win.c)
    - This RNG is used only as a seeding mechanism to the FIPS-approved PRNG.
- RSA (key agreement; key establishment methodology provides 96 bits of encryption strength)

2.5 Module Interfaces

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

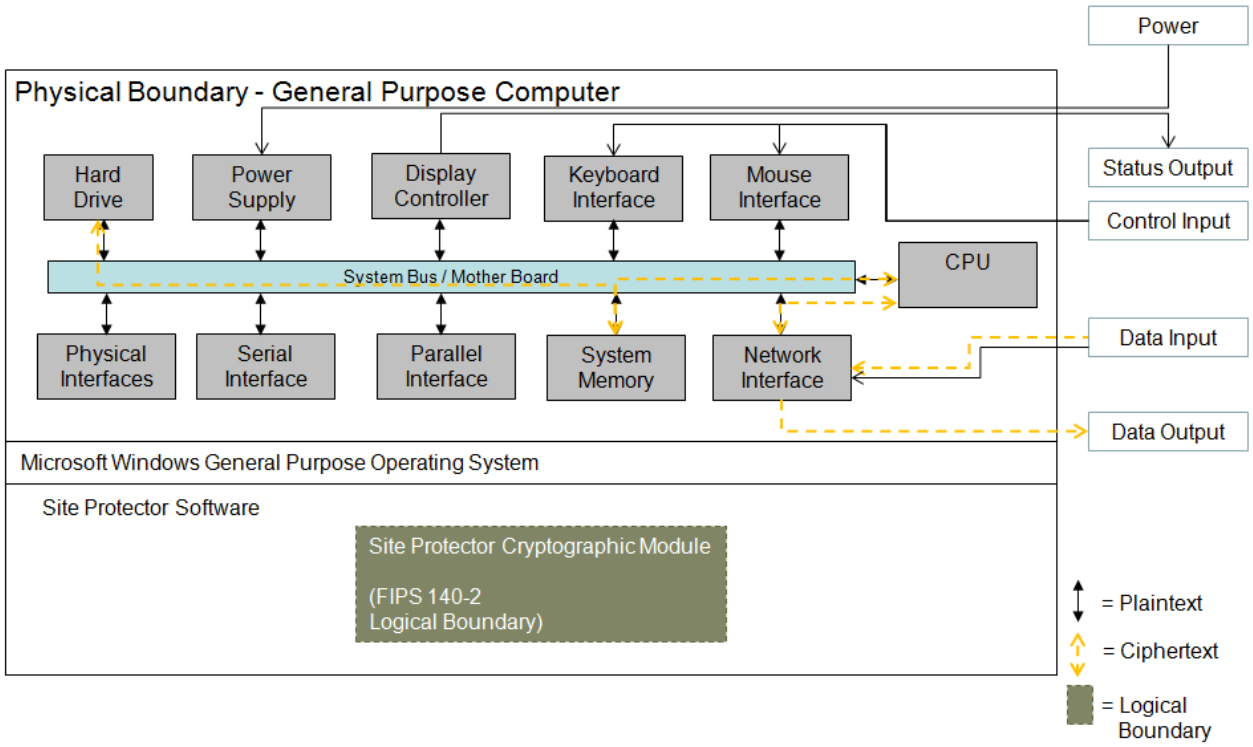

Figure 1 – Module Interfaces Diagram

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

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

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Data Input	Input parameters of API function calls	Ethernet/Network port
Data Output	Output parameters of API function calls	Ethernet/Network port
Control Input	API function calls	Keyboard and mouse

FIPS 140-2 Interface	Logical Interface	Module Physical Interface
Status Output	For FIPS mode, function calls returning status information and return codes provided by API function calls. FIPS_mode_set returns true or false. False values are logged.	Monitor
Power	None	Power supply/connector

Table 4 – Logical Interface / Physical Interface Mapping

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

As shown in Figure 1 – Module Interfaces Diagram and Table 5 – Module Services and Descriptions , the output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

2.6 Roles, Services, and Authentication

The module supports a Crypto Officer and a User role. The Crypto Officer (i.e., a human operator) can initialize and configure the module while the User role (i.e., SiteProtector) can only access the services of the module. The module does not support a Maintenance role.

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 (API)	Key/CSP Access	Roles
Configure	Initializes the module for FIPS mode of operation	Specified in Section 3 FIPS_check_incore_fingerprint FIPS_check_rsa FIPS_incore_fingerprint FIPS_mode_set FIPS_rand_check ERR_load_FIPS_strings	None	Crypto Officer
Decrypt	Decrypts a block of data Using AES	AES_decrypt	Session Key	User
Encrypt	Encrypts a block of data Using AES	AES_encrypt	Session Key	User
Random Number Generation	Generates random numbers for crypto operations	FIPS_rand_method FIPS_rand_seed FIPS_rand_seeded FIPS_set_prng_key	PRNG Seed PRNG Seed Key	User
Establish Session	Provides a protected session for establishment of AES keys with peers	RSA_generate_key RSA_PKCS1_SSLeay RSA_X931_derive RSA_X931_generate_key SHA1 sha1_block_asm_data_order sha1_block_asm_host_order SHA1_Final SHA1_Init SHA1_Transform SHA1_Update	Private Key Public Key HMAC Key Premaster Secret (48 Bytes) Master Secret (48 Bytes)	User
Self Test	Performs self tests on critical functions of module	FIPS_selftest FIPS_selftest_aes FIPS_selftest_failed FIPS_selftest_hmac FIPS_selftest_rng FIPS_selftest_rsa FIPS_selftest_sha1	None	User
Show Status	Shows status of the module	FIPS_mode FIPS_mode_set	None	User

Service	Description	Service Input/Output (API)	Key/CSP Access	Roles
Zeroization	Zeroizes keys	Ephemeral CSPs are zeroized by the RAM clearing processes, and static CSPs are zeroized by uninstalling the module and formatting the hard drive.	None	User

Table 5 – Module Services and Descriptions

2.6.2 Operator Authentication

Operators authenticate to the module via the General Purpose Operating System, which implements a username/password authentication mechanism and enforces operator authentication prior to the operator utilizing any system services. Further, the GPOS authentication mechanism distinguishes operators that have administrator rights on a computer system. The modules rely on this mechanism to distinguish an operator between the two supported roles. The module itself does not contain authentication data.

The GPOS will allow an operator to change roles only if the User knows the Crypto Officer password and vice versa. The operating system is responsible for ensuring previous authentication data is cleared upon powering off of the module.

Passwords must be a minimum of 8 characters (see Secure Operation section of this document). The password can consist of alphanumeric values, **a-z A-Z 0-9**, yielding 62 choices per character. The probability of a successful random attempt is $1/62^8$, which is less than 1/1,000,000.

The GPOS module will lock an account after 5 failed authentication attempts; thus, the maximum number of attempts in one minute is 5. Therefore, the probability of a success with multiple consecutive attempts in a one minute period is $5/62^8$ which is less than 1/100,000.

2.7 Physical Security

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

2.8 Operational Environment

The cryptographic module were tested and validated on the following hardware platform:

- IBM eServer 326m 2.0 GHz AMD Opteron Processor 270 (1 Dual-Core 32-bit CPU)

The module runs on Microsoft Windows Server 2003 R2 Standard, Version 5.2 SP2, which has met Common Criteria EAL 4+ certification. The module's software is entirely encapsulated by the cryptographic boundary shown in Figure 1. Please note that this operating system must meet installation and configuration requirements specified in the operating system's Common Criteria Security Target (http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf).

The GPC(s) used during testing are assumed to have met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

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
Session Key	AES CBC 256-bit key for encryption / decryption of session 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 Session Key Certificate and the SiteProtector management of the session.	**Agreement**: Via secure TLS tunnel **Entry**: NA **Output**: Key handle from API request is output only to the SiteProtector application	Decrypt Encrypt	Crypto Officer R W D User R
PRNG Seed	System Entropy to seed the X9.31 PRNG	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

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privileges
Private Key	RSA Private 1536-bit for sign / verify operations and key establishment[1] for SiteProtector to GX appliances over TLS	Internal generation by X9.31 PRNG	**Storage**: RAM plaintext **Type:** Static **Association**: The system is the one and only owner. elationship is maintained by the operating system via protected memory.	**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
Public Key	RSA Public 1536-bit for sign / verify operations and key establishment[2] for SiteProtector to GX appliances over TLS. Encryption/Decryption of the Premaster Secret for entry/output	Internal generation by X9.31 PRNG	**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
PRNG Seed Key	256-bit value to seed the FIPS-approved ANSI X9.31 PRNG	Generated internally by non-Approved RNG	**Storage**: RAM plaintext **Type:** Ephemeral	**Agreement**: NA **Entry**: NA	Establish Session	Crypto Officer None

[1] Key establishment methodology provides at least 96-bits of encryption strength
[2] Key establishment methodology provides at least 96-bits of encryption strength

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privileges
			Association: The system is the one and only owner. Relationship is maintained by the operating system via protected memory.	**Output**: NA		User None
HMAC key	160-bit HMAC-SHA1 for message verification in TLS sessions	Partitioned from 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**: 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
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 D

Key/CSP Name	Description / Use	Generation	Storage	Establishment / Export	Interface	Privileges
Premaster Secret (48 Bytes)	RSA-Encrypted Premaster Secret Message	Internal generation by X9.31 PRNG	**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 X9.31 PRNG	**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

R = Read W = Write D = Delete

Table 6 – Module Keys/CSPs

Secret keys, public/private keys, and CSPs are protected from unauthorized disclosure, unauthorized modification, and unauthorized substitution because only authorized users are allowed access to the GPOS and SiteProtector application. The SiteProtector application ensures that no keys or CSPs leave the physical boundary of the module in plaintext. The module does not output intermediate key values, nor does it generate keys with non-Approved key generation methods.

Ephemeral CSPs are zeroized by the RAM clearing processes, and static CSPs are zeroized by uninstalling the module and formatting the hard drive. All keys and CSPs are stored in memory, and zeroization has been implemented to ensure no

traces are left of any CSPs upon termination of the service using the CSP. Zeroization has been implemented by overwriting the allocated memory buffer with zeros before freeing the memory to other uses. Any service using a CSP will zeroize the CSP upon normal termination and when transitioning into error states. Zeroization is initiated by terminating the process and powering off the module. Zeroization will complete before any other malicious command could compromise the keys currently being zeroized because the module will not process additional commands until it finishes executing the current command.

2.10 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. In the event of any self-test failure, the module/SiteProtector application will output an error to the audit log and will shutdown. In addition to self-test failures, successful loading of the module is also logged. To access status of self-tests, success or failure, the application provides access to the audit log. Status is viewable via operating environment's audit mechanism and by verifying proper loading and operation of the SiteProtector application. While the module is running self-tests, the module will not output data. The SiteProtector application makes calls to the SiteProtector Cryptographic Module (Version 1.0), and data will not be returned until the self-tests complete.

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

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

2.10.1 Power-On Self-Tests

Power-on self-tests are run upon every initialization of the module and if any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the users. The module implements the following power-on self-tests:

- Module integrity check[3] via HMAC-SHA1
- RSA pairwise consistency key (signing and signature verification)
- AES KAT (encryption and decryption)
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT
- HMAC-SHA1 KAT
- KAT for Approved PRNG

[3] The integrity of the FIPS module (i.e., all files within the cryptographic boundary listed in Section 2.2) is protected by a single HMAC SHA-1 digest that is calculated over the module at the time it is created. This digest is verified when the module is initialized.

- KAT for non-approved software RNG

The module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by reinitializing the module in FIPS approved Mode of Operation. Upon passing the power-on self-tests, the module will log the success and will continue to boot normally; successful loading of the SiteProtector application will indicate that all self-tests have passed. If a self-test fails, the module will not load and the SiteProtector application will halt.

2.10.2 Conditional Self-Tests

Conditional self-tests are on-demand tests and tests run continuously during operation of the module. If any of these tests fail, the module will enter an error state and no services can be accessed by the users. The module can be re-initialized to clear the error and resume FIPS mode of operation. The module performs the following conditional self-tests:

- Pairwise consistency test for RSA
- Continuous RNG test run on output of ANSI X9.31 PRNG
- Continuous test on output of ANSI X9.31 PRNG seed mechanism
- Test to ensure ANSI X9.31 PRNG output and seed do not match

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.

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 module for FIPS-approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

3.1.1 Software Packaging

The module is included with SiteProtector Version 2.0 Service Pack 8.0 and is not available for direct download. The SiteProtector application (and subsequently the module) is to be installed on a Microsoft Windows Server 2003 R2 Standard, Version 5.2 SP2 operating system. Please note that this operating system must meet installation and configuration requirements specified in the operating system's Common Criteria Security Target (http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf). This includes configuring the General Purpose Operating System to lock an account after 5 failed authentication attempts.

3.1.2 Enabling FIPS Mode

To meet the cryptographic security requirements, especially for secure communication, certain restrictions on the installation and use of SiteProtector must be followed. The steps below will ensure that the module implements all required self-tests and uses only approved algorithms.

3.1.2.1 Installation

1. Only the Express install package is supported. Other installation options are not valid. To install SiteProtector, please follow these steps:
    - Log in to the ISS support site at https://webapp.iss.net/myiss/login.jsp
    - Select **Downloads** from the menu
    - Choose **FIPS enabled systems** from the **Select a Product** dropdown menu and then select **Go**
    - Select **GX6116 FW 3.1 and SiteProtector 2.0 SP 8.0** from the **Version** dropdown menu then select **Go**

- Select **Other Updates** and select **Continue** next to the bundle listing for the **Proventia Management SiteProtector 2.0 Service Pack 8.0 FIPS 140-2 service** software
- Accept the End User License and select **Submit**
- Download **FIPSService-Setup.exe** (SiteProtector Installation) and install on the machine intended to run SiteProtector.

2. All SiteProtector components must be installed on a single hardware / OS platform. The only exception to this rule is that the management Console may be installed and used remotely.
3. The installation must be a new install. Upgrading from a previous version of SiteProtector is not valid.
4. The Update Server's XPU Settings policy must be modified to disable Install of automatic Product Updates.
5. The optional Event Archiver package must not be installed.
6. The following keys must be deleted from the platform hosting SiteProtector after installation:
   - \rs_eng_siteprotector_1024.Pubkey
   - \sp_con_siteprotector_1024.Pubkey

   These files can be found in the *ISS\SiteProtector\AgentManger\Keys\RSA* directory.

3.1.3 Additional Rules of Operation

1. All host system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.
2. The writable memory areas of the Module (data and stack segments) are accessible only by the SiteProtector application so that the Module is in "single user" mode, i.e. only the SiteProtector application has access to that instance of the Module.
3. The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the Module.

3.2 User Guidance

3.2.1 General Guidance

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

1. The end user of the operating system is responsible for zeroizing CSPs by via wipe/secure delete procedures.