Xceedium

FIPS 140-2 Non-Proprietary Security Policy

for the

Xceedium GateKeeper

Level 2 Validation

Document Version: Version 1.3

July 27, 2007

REVISION HISTORY

The table below provides revision history of this document.

Version	Date	Author(s)	Comments
1.0	March 2, 2007	Apex Assurance Group	Initial Draft for submission to EWA
1.1	April 16, 2007	Apex Assurance Group	Revise with comments from EWA
1.2	July 12, 2007	Apex Assurance Group	Address comments from NIST
1.3	July 27, 2007	Apex Assurance Group	Address additional comments from NIST

Table 1 – Security Policy Revision History

TABLE OF CONTENTS

REVISION HISTORY **2**

TABLE OF CONTENTS **3**

INTRODUCTION **4**

BACKGROUND 4
EXTERNAL RESOURCES 4
NOTICES 4

XCEEDIUM GATEKEEPER **5**

PRODUCT OVERVIEW 5
CRYPTOGRAPHIC MODULE SPECIFICATION 5
VALIDATION LEVEL AND ALGORITHM IMPLEMENTATION CERTIFICATES 6
MODULE INTERFACES 7
ROLES AND SERVICES 8
Crypto Officer Role *9*
User Role *10*
Authentication *11*
CRYPTOGRAPHIC KEY MANAGEMENT 12
SELF-TESTS 14
Power-On Self-Tests *15*
Conditional Self-Tests *16*
MITIGATION OF OTHER ATTACKS 16

SECURE OPERATION OF THE GATEKEEPER **17**

CRYPTO OFFICER GUIDANCE 17
Module Initialization and Configuration *17*
Physical Security and Tamper Evidence *18*
USER GUIDANCE 18
APPROVED CRYPTOGRAPHIC ALGORITHMS 19
NON-FIPS APPROVED ALGORITHMS 19

ACRONYM LIST **20**

INTRODUCTION

Background

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic products to be deployed in a Sensitive but Unclassified environment. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/ .

This non-proprietary Cryptographic Module Security Policy for the GateKeeper from Xceedium 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 modules in a FIPS 140-2 mode of operation.

External Resources

The Xceedium website (http://www.xceedium.com) contains information on the full line of products from Xceedium, including a detailed overview of the GateKeeper solution. The NIST Cryptographic Module Validation Program website (http://csrc.ncsl.nist.gov/cryptval/) contains Xceedium contact information for answers to technical or sales-related questions.

Notices

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

XCEEDIUM GATEKEEPER

Product Overview

The GateKeeper provides many of the required day-to-day IT functions for organizations in a 1U, rack-mountable appliance. It provides TLS-secured, in-band and out-of-band management and monitoring of networking equipment, UNIX, Linux, Macintosh and Windows servers and workstations, as well as remote power-management to either turn on, turn off, or reboot any attached device. The GateKeeper offers the following functions:

- All-in-one web-based remote in-band access,
- Web-enabled serial console for remote out-of-band access,
- Web-based Virtual Desktop to bring secure remote management of your UNIX (X-Windows and CDE), Windows, Linux, and Macintosh desktops right to any web-browser without the need to install processor intensive, bandwidth hungry, large applications from other vendors on every desktop and server,
- Web-based Secure Shell (SSH) and Telnet access to all computer desktops and workstations as well as network devices and terminal servers,
- Encrypted connectivity without Virtual Private Networks (VPN) – No expensive VPN tunnels to worry about everywhere your support staff travels – lowers total cost of ownership, and
- Multi-level Authentication.

The GateKeeper features include:

- Web-based access to establish telnet, SSH, and standard operating system specific GUI sessions to devices over TCP/IP,
- IPSec and SSL-VPN support,
- Remote power management – allowing you to turn attached devices on or off, and
- External LCD display for entering initial host connection information without needing access to a laptop of other terminal, as well as checking on system configuration.

Cryptographic Module Specification

The module is the Xceedium GateKeeper, running firmware version 4.0.0f on hardware version 4a. The module is classified as a multi-chip standalone cryptographic module. The physical cryptographic boundary is defined as the module's case and all components within the case. No software or firmware is excluded from validation. The physical boundary is pictured in the image below:

Figure 1 – Physical Boundary

Validation Level and Algorithm Implementation Certificates

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

FIPS 140-2 DTR Section	Section Title	Module Validation Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference / Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 2 – Validation Level by DTR Section

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

Algorithm Type	Algorithm	Standard	FIPS Validation Certificate	Use
Asymmetric Key	RSA	PKCS#1 v1.5	197	Sign / verify operations
	RSA	ANSI X9.31	197	Key generation and sign / verify operations
	RSA	PKCS#1 RSASSA-PSS RSA	197	Sign / verify operations
Symmetric Key	TDES – CBC, CFB8, CFB64, ECB, OFB Modes	FIPS 46-3	493	Encrypt / decrypt operations
	AES – CBC, CFB8, CFB128, ECB, OFB each with 128, 192, or 256 bit keys	FIPS 197	480	
HMAC	HMAC SHA-1 HMAC SHA-224 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512	FIPS 198	236	Message integrity
Hashing	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	FIPS 180-2	549	Message digest
RNG	ANSI X9.31 Appendix A.2.4	ANSI X9.31	260	Random number generation

Table 3 – Algorithm Certificates

Module Interfaces

The interfaces for the cryptographic boundary include physical and logical interfaces. 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 mapping of logical interfaces to module physical interfaces is provided in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	6 Gigabit Ethernet Interfaces Modem Port**
Data Output	6 Gigabit Ethernet Interfaces Modem Port**
Control Input	6 Gigabit Ethernet Interfaces Modem Port** LCD Panel Factory Reset Button
Status Output	6 Gigabit Ethernet Interfaces Modem Port** LCD Panel LEDs
Power	Power Plug On/Off Switch
Unused Interface	USB Interfaces DB-9 RS-232 Serial Interface*

* The serial interface and USB interfaces are wired; however, the Xceedium software does not allow any communications through this interface. Driver support for this interface is not compiled into the shipping image.

** The modem port provides the same functionality as the Gigabit Ethernet interfaces; the only difference between the Modem Port and Gigabit Ethernet Interfaces is the physical connection type and data speed.

Table 4 – Logical Interface / Physical Interface Mapping

Roles and Services

In FIPS-approved mode of operation, the module is accessed via Web browser over HTTPS/TLS (see Secure Operation of the GateKeeper section of this document for more details). 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.

The module supports basic management via the LCD panel. This unauthenticated service is used to define basic network configuration to initialize the module for FIPS mode of operation. When in FIPS mode, the LCD Management only allows reboot, power off, and turn off FIPS mode (requiring reboot).

Crypto Officer Role

The Crypto Officer role is responsible for the configuration and maintenance of the module and authenticates via Web browser over HTTPS/TLS[1]. The Crypto Officer services consist of the following:

Service	Description
Authenticate	Allows the Crypto Officer to authenticate to access the services available to the role.
Sessions	Utilize administrative features such as viewing active logins, sessions, logs, and reporting.
Config	Utilize the configuration features, such as setting parameters and conducting maintenance tasks.
Services	Create custom access methods to run either local clients or launch a URL
Users	Utilize user management features, such as create, update, and delete.
Devices	Utilize device management features, such as create, update, and delete.
Associations	Utilize association management features, such as create, update, and delete.
Access	A default setting allowing the user to utilize the assigned access methods. This also allows the Manage features (discussed on the following row) to be available for the user.
Manage	A default setting allowing the user to utilize the power management feature.
Monitoring	A default setting allowing the user to utilize the monitoring feature.

Table 5 – Crypto Officer Services and Descriptions

[1] Except for the initial configuration for FIPS mode of operation, where the Crypto Officer will first use the LCD panel (see *Secure Operation of the GateKeeper* section of this document for more details)

Note that all services are invoked via HTTPS session using the following algorithms in the TLS protocol:

- FIPS-approved PRNG for generation of DH Secret Component
- Diffie Hellman for key agreement with key lengths of 80-bits, 96-bits, or 112-bits
- RSA for:
    - For digital signature generation for self-signing of certificates using 1024-bit and 2048-bit key lengths
    - Key transport with key lengths of 80-bits, 96-bits, 112-bits, 128-bits, or 160-bits
- HMAC SHA (all variants) for message integrity checking
- AES or TDES for data encryption encrypted via symmetric encryption algorithm (AES or TDES).

As part of the initialization procedures, the module also

User Role

The User Role authenticates via Web browser over HTTPS/TLS. The User services available in the module consist of the following:

Service	Description
Access	A default setting allowing the user to utilize the assigned access methods. This also allows the Manage features (discussed on the following row) to be available for the user.
Manage	A default setting allowing the user to utilize the power management feature.
Monitoring	A default setting allowing the user to utilize the monitoring feature.
Authenticate	Allows the user to authenticate to access the services available to the role.
User Account Management	Allows the user to view and change his/her password and contact information.

Table 6 – User Services and Descriptions

Note that all services are invoked via HTTPS session using the following algorithms in the TLS protocol:

- FIPS-approved PRNG for generation of DH Secret Component
- Diffie Hellman for key agreement with key lengths of 80-bits, 96-bits, or 112-bits
- RSA for:
    - Digital signature generation for self-signing of certificates using 1024-bit and 2048-bit key lengths
    - Key transport with key lengths of 80-bits, 96-bits, 112-bits, 128-bits, or 160-bits
- HMAC SHA (all variants) for message integrity checking

- AES or TDES for data encryption encrypted via symmetric encryption algorithm (AES or TDES).

The services accessing the Critical Security Parameters (CSP)s, the type of access and the role accessing the CSPs are listed in Table 9 – Role and Service Access to Security Relevant Data Items.

Authentication

The module supports either a username and password or digital certificates for authenticating operators. The table below provides estimated strength of the authentication mechanisms:

Authentication Type	Strength
Username and Password mechanism	Passwords must be a minimum of 6 characters (see 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. For the Super and Config accounts, 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. For accounts other than the Super account, 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.
Certificate-based authentication	The module supports a public key based authentication with 512, 768, 1024, and 2048 (for RSA) bit keys[2]. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is 1/2^80, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one minute period is 60/2^80 which is less than 1/100,000. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000. Assuming the module can support 60 authentication attempts in one minute, the probability of a success with multiple consecutive attempts in a one minute period is 60/2^112 which is less than 1/100,000.

[2] As described in the *Secure Operation of the GateKeeper* section, 512-bit and 768-bit RSA keys must not be used in FIPS mode of operation.

Table 7 – Estimated Strength of Authentication Mechanisms

To authenticate to the module for management purposes (i.e., accessing available services defined in the Crypto Officer Role and User role sections), an operator must connect to the module via a Web browser and provide a username and password. A user name and password is required for all services accessed through a browser.

Note that all services are available when accessing the module via certificate-based authentication.

Cryptographic Key Management

Table 8 provides a complete list of critical security parameters[3] used within the module:

IDENTIFIER	KEY / CSP NAME	DESCRIPTION	STORAGE (FORMAT)	DELETION
1	PRNG Seed	Generated from non-FIPS approved PRNG in OpenSSL code implemented in module; used in 2-key TDES ANSI X9.31 Appendix A.2.4 FIPS-approved PRNG	RAM (plaintext)	Generating a new seed
2	Public keys	Public keys of peers	RAM (plaintext)	Resetting or rebooting the module
3	RSA public/private keys	Identity certificates for the module itself and also used in TLS negotiations. The module supports 1024 and 2048 bit key sizes.	NVRAM (plaintext)	Deleting the certificate or certificate request; The keys are overwritten with dashes via command sent by the Crypto Officer over the web interface.
4	TLS Traffic Keys	Used in HTTPS connections	RAM (plaintext)	Resetting or rebooting the module
5	User Passwords	Secret	NVRAM/Flash Memory (plaintext) and	Overwriting the passwords with new ones

[3] Public keys are not considered to be critical security parameters.

			RAM (plaintext)	
6	Crypto Officer Passwords	Secret	NVRAM/Flash Memory (plaintext) and RAM (plaintext)	Overwriting the passwords with new ones
7	Xceedium default certificate and private key	Used in HTTPS connections	NVRAM (plaintext)	Deleting the certificate or certificate request; The private key is overwritten with dashes via command sent by the Crypto Officer over the web interface.
8	Diffie-Hellman Key Pairs[4]	Key agreement for TLS sessions	RAM (plaintext)	Resetting or rebooting the module
9	IPSec Traffic Keys	Used to encrypt IPSec sessions	RAM (plaintext)	Resetting or rebooting the module
10	Client Certificates	Authenticate PKI peers	RAM (plaintext)	Resetting or rebooting the module

Table 8 – Critical Security Parameters

The services accessing the Critical Security Parameters (CSP)s, the type of access and the role accessing the CSPs are listed in the following table:

[4] DH groups 2 (1024 bits), 5 (1536 bits) and 7 (2048 bits) are supported.

Identifier / Services by Role	1	2	3	4	5	6	7	8	9	10
User Role										
Access				R					R	
Authenticate		R W	R	R W	R		R	R W	R W	R
Manage				R			R W		R	R W
Monitoring				R					R	
User Account Management					R W D					
Crypto Officer Role										
Authenticate		R W	R	R W		R	R	R W	R W	R
Sessions				R					R	
Config	R W D	R W D	R W D	R W D	D	R W D	R W D	R W D	R W D	R W D
Services				R					R	
Users				R	W D	R W D	R W		R	R W
Devices				R					R	
Associations				R					R	
LCD Management										

R = Read W = Write D = Delete

Table 9 – Role and Service Access to Security Relevant Data Items

The module supports entry of usernames and passwords for authentication, but these parameters are not distributed outside the cryptographic boundary. The module supports electronic key entry; the Crypto Officer may load RSA private keys and certificates to replace the default Xceedium private key and certificate for the module identity. The parameters are loaded via the secured Web interface. The public key, private key, and certificate associated with the default Xceedium certificate is output if the certificate is downloaded by the Crypto Officer via the secure Web interface.

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. The module supports OpenSSL for all IPSec and SSL-VPN operations as well as HTTPS communications. The following sections discuss the module's self-tests in more detail:

Power-On Self-Tests

The module implements the following power-on self-tests:

- Module integrity check via SHA-1
- RSA KAT (signing and signature verification)
- AES KAT (encryption and decryption)
- Triple DES KAT (encryption and decryption)
- SHA-1 KAT
- HMAC SHA-1 KAT
- HMAC SHA-224 KAT
- HMAC SHA-256 KAT
- HMAC SHA-384 KAT
- HMAC SHA-512 KAT
- PRNG KAT

The module performs all power-on self-tests automatically at boot when FIPS mode is enabled. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the Gigabit Ethernet ports, which prevents the module from passing any data during a power-on self-test failure.

An operator can discern that all power-on self-tests have passed via normal operation of the module, which is indicated with the following text on the LCD panel:

```
""""""""""""""
GateKeeper
In FIPS mode
""""""""""""""
```

For OpenSSL self-test failure: *spfd*[5] will not run, and an error status is sent by *spfd* to the log table. When *spfd* stops, there will be no connections to the module because no process is listening on port 443 (Port 443 is the only way to connect to the module). The module will also provide the following indication of a self-test failure via the LCD: `FIPS mode failed / System halted`, and the user will reboot manually. When rebooted, the module is not running in FIPS mode, and `Network Setup` is displayed on the LCD panel.

[5] *spfd* is a Sender Policy Framework (SPF) query proxy server that receives and answers SPF query requests on a TCP/IP socket.

The module will indicate a failure of the integrity test via the LCD; the message `GK SI failure / System halted` is displayed on the LCD. The module writes a log entry to the log table only if the database is initialized prior to the failure.

Conditional Self-Tests

The module performs the following conditional self-tests:

- Pairwise consistency test for RSA
- Continuous Random Number Generator Test for the FIPS-approved PRNG
- Continuous Random Number Generator Test for the non-approved PRNG in the OpenSSL code portion of the cryptographic module

The module will provide the following indication of a conditional self-test failure via the LCD: `FIPS mode failed / System halted`, and the user will reboot manually. A log entry is written to the module database.

The module does not support a bypass function because it only transmits encrypted data.

Mitigation of Other Attacks

The module does not mitigate other attacks in a FIPS-approved mode of operation.

SECURE OPERATION OF THE GATEKEEPER

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.

Crypto Officer Guidance

Module Initialization and Configuration

Crypto Officer must configure and enforce the following initialization procedures:

1. Verify that the firmware version is 4.0.0f. No other version is allowed to be used in FIPS mode of operation.
2. Configure the minimum password length for all accounts to 6 characters.

   Note: Stronger, more secure passwords should have a combination of letters and numbers and should not contain any recognizable words that may be found in a dictionary. The module does not enforce this; the Crypto Officer must follow his/her organization's systems security policies and adhere to the password policies set forth therein.

3. Change the default password of the Crypto Officer.
4. Ensure that 768-bit RSA keys are not used in FIPS mode of operation.
5. Ensure that RADIUS is not used in FIPS mode of operation.
6. Ensure that DSA is not used in FIPS mode of operation.
7. Ensure that FIPS-allowed algorithms and key sizes are used when configuring TLS.
8. Ensure all Telnet sessions are conducted via a TLS session.
9. Turn on FIPS mode via the Web interface or LCD panel.
10. Configure the Password Failures Limit to 3. This ensures that accounts are locked after 3 unsuccessful authentication attempts.
11. Reboot the module.

The Crypto Officer should consider replacing the default Xceedium certificate with another certificate. Additionally, the Crypto Officer must not disclose passwords and must store passwords in a safe location and according to his/her organization's systems security policies for password storage.

Physical Security and Tamper Evidence

A single tamper evidence label is placed on the GateKeeper at the time of manufacture. This security label is very fragile and cannot be removed without clear signs of damage to the label; any attempt to open the device will damage the tamper evidence label or the material of the module cover. The label is placed on the back of the module next to the power switch, as shown in Figure 2 – Tamper Evidence Label Placement below:

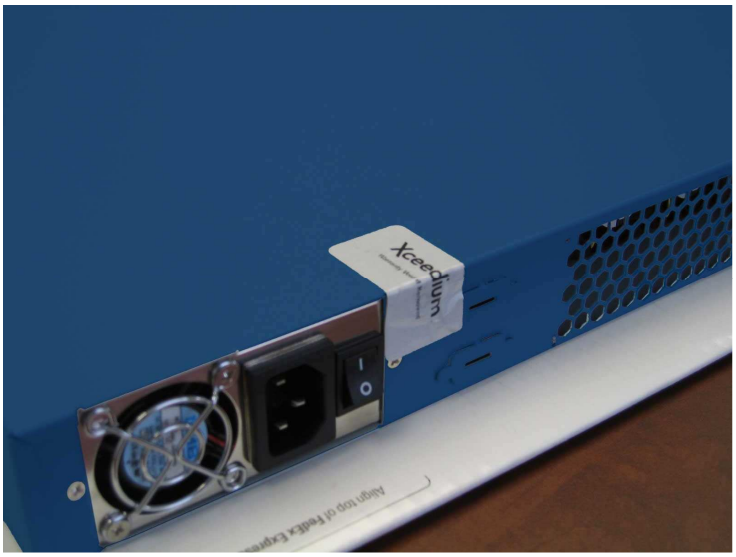

Figure 2 – Tamper Evidence Label Placement

The Crypto Officer should inspect the tamper evidence label periodically according to his/her organization's systems security policies to verify it is not damaged.

User Guidance

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

Approved Cryptographic Algorithms

In FIPS mode of operation, only the following FIPS approved algorithms are to be used:

- AES encryption/decryption
- Triple DES encryption/decryption
- RSA signing and verifying
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hashing
- HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, and HMAC SHA-512 for hashed message authentication
- ANSI X9.31 Appendix A.2.4 for PRNG

Non-FIPS Approved Algorithms

The module implements the following non-FIPS-approved cryptographic algorithms:

- Diffie-Hellman (allowed for use in FIPS mode / key establishment methodology provides 80-bits, 96-bits, or 112-bits of key establishing strength; non-compliant less than 80-bits of key establishing strength)
- DSA (non-compliant)
- RSA encryption/decryption (allowed for key transport in FIPS mode / key establishment methodology provides 80-bits, 96-bits, 112-bits, 128-bits, or 160-bits of encryption strength; non-compliant less than 80-bits of key establishing strength)
- PRNG included in the OpenSSL code for the cryptographic module

ACRONYM LIST

AES ..... Advanced Encryption Standard
ANSI ..... American National Standards Institute
CBC ..... Cipher Block Chaining
CDE ..... Common Desktop Environment
CFB ..... Cipher Feedback
CSP ..... Critical Security Parameter
DES ..... Data Encryption Standard
DH ..... Diffie-Hellman
DSA ..... Digital Signature Algorithm
DTR ..... Derived Test Requirements
ECB ..... Electronic Codebook
FIPS ..... Federal Information Processing Standard
GUI ..... Graphical User Interface
HMAC ..... Hashed Message Authentication Code
HTTPS ..... Secure Hypertext Transfer Protocol
IP ..... Internet Protocol
KAT ..... Known Answer Test
LCD ..... Liquid Crystal Display
MAC ..... Message Authentication Code
NIST ..... National Institute of Standards and Technology
NVRAM ..... Non-Volatile Random Access Memory
OFB ..... Output Feedback
PRNG ..... Pseudo-Random Number Generator
RADIUS ..... Remote Authentication Dial In User Service
RAM ..... Random Access Memory
RNG ..... Random Number Generator
RSA ..... Rivest, Shamir, Adleman
SHA ..... Secure Hash Algorithm
SPFD ..... Sender Policy Framework Daemon
SSH ..... Secure Shell
SSL ..... Secure Sockets Layer
TCP ..... Transmission Control Protocol
TDES ..... Triple DES
TLS ..... Transport Layer Security
VPN ..... Virtual Private Network