Forum Systems

Forum FIA Gateway 1504G

(Hardware Version: 1504, Software Version: 4.3, Firmware Version: 4.3)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 0.67

January 2005

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Forum FIA Gateway 1504G from Forum Systems. This security policy describes how the Forum FIA Gateway 1504G meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

In this document, the Forum Systems' Forum FIA Gateway 1504G is referred to as the FIA Gateway 1504G, the Gateway 1504G, the FIA 1504G, the FIA, the Gateway, the 1504G, and the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Forum Systems website (http://www.forumsystems.com) contains information on the full line of products from Forum Systems.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

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

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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Forum Systems. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Forum Systems and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Forum Systems.

FORUM SYSTEMS FORUM FIA GATEWAY 1504G

Overview

In the extended enterprise or governmental entity, the boundaries of partners are blurred with closer coordination of design, development and marketing activities giving way to stable collaborative relationships. Service-Oriented Architectures and XML Web services are allowing enterprises to dynamically integrate their business processes and IT systems using open standards-based specifications.

Forum FIA Gateway provides the foundation infrastructure that drives a return on investment by enabling secure XML and Web services communications for mission critical applications. Forum FIA Gateway industry specific solutions include: government compliance, secure electronic forms, secure partner integration, secure partner collaboration, electronic notary, evidence repository as well as secure Service Oriented Architectures.

The Forum FIA Gateway 1504G is a multi-chip standalone module that meets all level 2 FIPS 140-2 requirements. The module's form factor is a 1U rack-mountable server completely enclosed in a hard metal case with tamper-evident labels.

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

Table 1 – Security Level Per FIPS 140-2 Section

Module Interfaces

The Forum FIA Gateway 1504G is completely enclosed in an opaque, metal case, which surrounds all of the modules internal components and only provides access to the module through well-defined interfaces. This case is defined as the cryptographic boundary for the Forum FIA Gateway 1504G.

The FIA Gateway 1504G has the following physical ports:

- 1 (RJ45 connector with link LED) 10/100 BaseT Ethernet port (management)
  - The link LED (upper left corner of the (RJ45) Ethernet connectors) for each of the ports is only lit when the Ethernet port has an active link, blinking when traffic is flowing over the port.
- 2 (RJ45 connector with link LED) 10/100/1000 BaseT Ethernet ports (LAN, WAN)
  - The link LED (upper left corner of the (RJ45) Ethernet connectors) for each of the ports is only lit when the Ethernet port has an active link, blinking when traffic is flowing over the port.
- 1 (DB9 connector) serial port (CLI)
- 1 (DB9 connector) serial port (smartcard)
- 1 HSM mode selection switch
- 1 HSM reset button
- 1 power connector
- 1 soft power switch (e.g., reset button)
- 1 hard power soft (e.g., on/off switch)
- 3 LEDs (HSM module status, Disk activity, Power)
  - The HSM module status indicates the current operational state of the HSM.
  - The power status LED is lit whenever the module is turned on.
  - The drive activity LED flashes whenever there is hard drive activity.

These physical ports are depicted in the following figures.

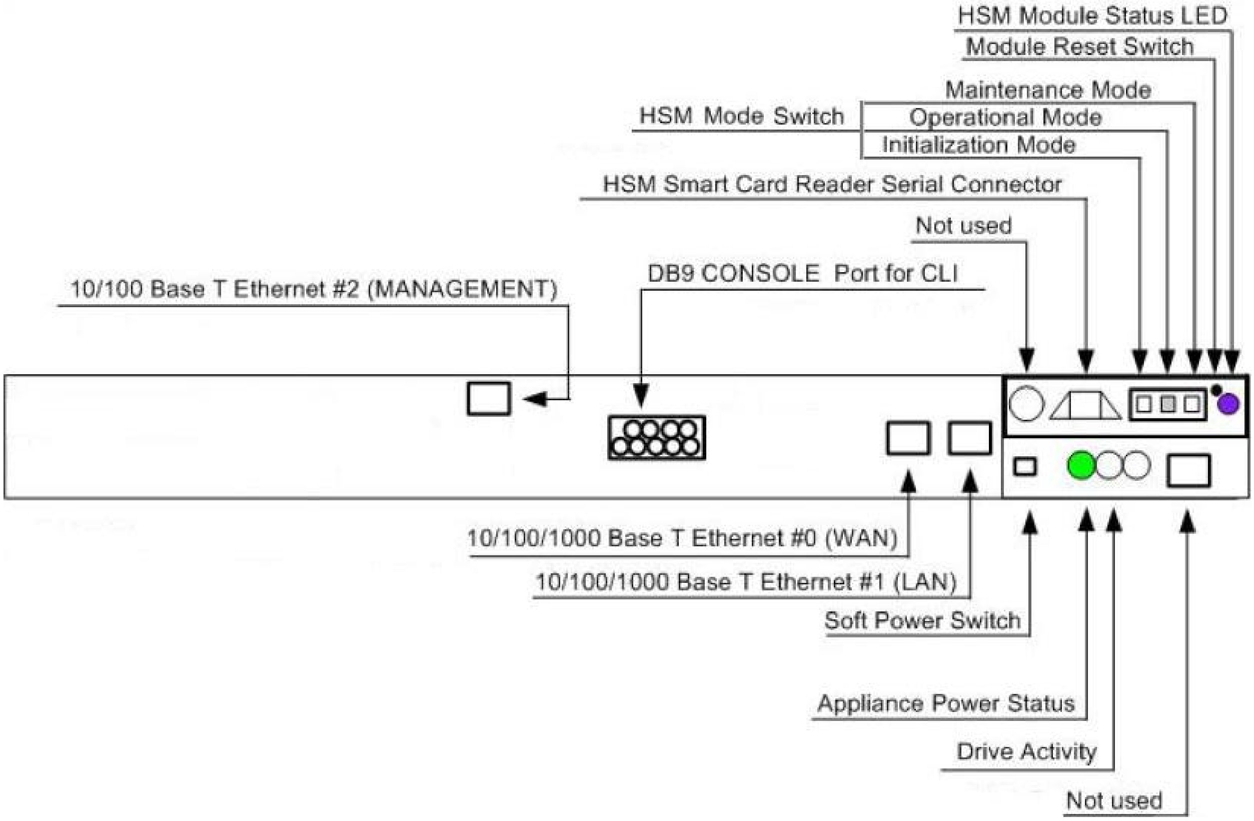


Figure 1 – Front Physical Ports

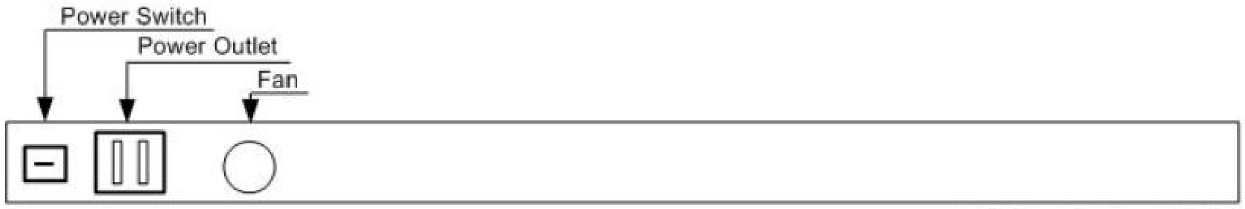


Figure 2 –Rear Physical Ports

All of these physical ports are separated into the logical interfaces defined by FIPS 140-2, as described in the following table:

FIA 1504G Physical Port	FIPS 140-2 Logical Interface
Power connector	Power interface
10/100 BaseT Ethernet port (management)	Data input, data output, control input, status output
10/100/1000 BaseT Ethernet ports (LAN, WAN)	Data input, data output, Control input, status output

DB9 serial port (CLI)	Control input, status output
DB9 serial port (smart card)	Data input, data output
LEDs	Status output
HSM reset button	Control input
HSM mode selection switch	Control input
Soft power button	Control input
Hard power switch	Control input

Table 2 – Physical Ports and Logical Interfaces

Roles and Services

The FIA Gateway 1504G supports four roles: Local Crypto-Officer, Administrative Crypto-Officer, Security Crypto-Officer, and User. The roles use either role-based or identity-based authentication mechanism through digital certificates and/or passwords.

The Local Crypto-Officer role has access to the initialization and administrative management functionality of the module through a locally accessible CLI. The Administrative Crypto-Officer role has access to the all of the primary administrative management functionality of the module over the Ethernet ports. The Security Crypto-Officer role can configure the module's User services and enable specific policies based on the higher level configurations put in place by the Administrative Crypto-Officer over the Ethernet ports. The User role has access to the cryptographic services of the module over the Ethernet ports as configured by the Security Crypto-Officer.

Local Crypto-Officer Role

The Local Crypto-Officer accesses the module locally over the serial port using a CLI. The Local Crypto-Officer is responsible for the initialization of the module, including the HSM, the Security World Key, and the Crypto-Officer key, and can perform some administrative configuration of the module, including the creation/deletion of Administrative/Security Crypto-Officers.

The Local Crypto-Officer role is assumed by entering the "enable" command at the CLI and entering the "enable" password. The authenticated Local Crypto-Officer has access to the services listed in the following table.

Service	Description	Input	Output	CSP	CSP Access
Initialization	Initializing the module	Command, configuration information, smart card token, and Crypto-Officer key (if loading from smart card)	Command response, configuration, and Crypto-Officer key (if writing to smart card)	Crypto-Officer key	Read/write

?	Help on enable mode commands	Command	Command response and help information		
access	Access control commands, including user management, group management, and ACL management	Command, sub-command, options (including passwords, if needed)	Command response	Operators	Write
enable	Login to enabled mode (Local Crypto-Officer)	Command and password	Command response	Local Crypto-Officer password	Read
exit	Exit enabled mode	Command	Command response		
log	Configure log parameters	Command, sub-command, and configuration	Command response		
network	Configure network interfaces	Command, sub-command and configuration information	Command response		
reboot	Reboot the module	Command	Command response		
route	Routing commands	Command, sub-command, and configuration information	Command response		
show	Show various configuration settings, including ACLs, users, and system configuration	Command and sub-command	Command response and configuration information		
shutdown	Shutdown the module	Command	Command response		
snmp	SNMP configuration	Command, sub-command, and configuration information	Command response		
syslog	Syslog configuration	Command, sub-command, and configuration information	Command response		
system	System wide settings configuration, including turning on setting the "enable" password (Local Crypto-Officer), performing a factory-reset, and resetting the default TLS key pair	Command, sub-command, and configuration, including turning on FIPS-mode	Command response	Local Crypto-Officer password (when setting password) All (when performing a factory-reset) DSA/RSA private keys; DSA/RSA public keys	Write Write Write

Table 3 – Local Crypto-Officer Services

Administrative Crypto-Officer Role

The Administrative Crypto-Officer accesses the module over the Ethernet ports, with the typical configuration defaulting to only allowing the management Ethernet port for Administrative Crypto-Officer access. Using API calls invoked by applications outside of the cryptographic boundary, including a web-based display, LDAP interface, or the Global Device Management (GDM), the Administrative Crypto-Officer configures the module. The Administrative Crypto-Officer is capable of accessing all of the module's primary configuration functionality, including generating/importing/exporting keys pairs, configuring the cryptographic algorithm allowed by the module (on a global scale), and creating/deleting/permissioning all of the module's operators (except the Local Crypto-Officer).

The Administrative Crypto-Officer accesses the module over an encrypted TLS session. The Administrative Crypto-Officer can be authenticated using digital certificates during the TLS handshake and/or using a username and password over the TLS session. The authenticated Administrative Crypto-Officer has access to the following services.

Service	Description	Input	Output	CSP	CSP Access
Login	Authenticate the Administrative Crypto-Officer role.	Login information	Result of login attempt	Administrative Crypto-Officer password	Read
Logout	Log out the Administrative Crypto-Officer.	Logout call	Call response		
TLS	Establish a TLS session and authenticate an operator with digital certificates, if configured.	TLS handshake parameters, TLS inputs	TLS outputs	TLS session keys DSA/RSA private keys DSA/RSA public keys	Read/Write Read Read/Write
General status	Display system and application memory and enabled Server policies.	API calls	Call response and status information		
General statistics	Display system metrics.	API calls	Call response and status information		
Web services status	Display all WSDL policy activities.	API calls	Call response and status information		
System management	Manage settings for the WebAdmin, Workbench and Global Device Management (GDM) port, IP addresses for NTP time server and	API call and configuration information	Call response and configuration information, if viewing		

	SMTP mail server, and session timeout.				
Network management	Manage network configuration settings.	API call and configuration information	Call response and configuration information, if viewing		
Managed machines management	Manage profiles between the MASTER machine and any managed machines surordinate to the MASTER.	API call and configuration information	Call response and configuration information, if viewing		
Import/Export configurations and keys	Manage Import /Export System configuration files as well as importing and exporting Security Worlds between two HSM-enabled systems.	API call and configuration information, including key pairs, if necessary	Call response and configuration information, including key pairs, if exporting/veiwing	DSA/RSA private keys; DSA/RSA public keys	Read/Write
Log configuration	Manage individual settings for each log category.	API call and configuration information, including key pairs, if necessary	Call response and configuration information, if viewing		
View logs	View System and Audit logs.	API call and configuration information, including key pairs, if necessary	Call response and status information, if viewing		
SysLog configuration	Manage Syslog Logging policies for up to six remote syslog destinations.	API call and configuration information, including key pairs, if necessary	Call response and configuration information, if viewing		
HTTP server policy management	Manage HTTP Server policies.	API call and configuration information	Call response and configuration information, if viewing		
Key management	Manage Key Pairs and Public Certificates (and OpenPGP keys).	API call and configuration information, including key pairs, if necessary	Call response and configuration information, including key pairs, if viewing	DSA/RSA private keys; DSA/RSA public keys	Read/Write
Signer group management	The Signer Groups pane manages Signer Groups.	API call and configuration information	Call response and configuration information, if viewing		
CRL configuration	The CRLs pane handles CRLs with or without LDAP support.	API call and configuration information	Call response and configuration information, if		

			viewing		
SSL/TLS policy management	The SSL Policies pane manages SSL/TLS Termination and SSL/TLS Initiation policies.	API call and configuration information	Call response and configuration information, if viewing		
XML encryption policy management	Manage XML Encryption policies.	API call and configuration information	Call response and configuration information, if viewing		
XML decryption policy management	Manage XML Decryption policies.	API call and configuration information	Call response and configuration information, if viewing		
XML signature policy management	Manage XML Signature policies.	API call and configuration information	Call response and configuration information, if viewing		
XML signature verification policy management	Manage XML Signature Verification policies.	API call and configuration information	Call response and configuration information, if viewing		
LDAP server configuration	Manage authenticating users through a corporate LDAP server and allows LDAP users and groups to be imported to the system.	API call and configuration information	Call response and configuration information, if viewing		
User management	Manage user policies and privileges.	API call and configuration information, including usernames and passwords	Call response and configuration information, including passwords, if viewing	Operator passwords	Read/Write
Group management	Manage groups and sub-groups and their membership privileges.	API call and configuration information	Call response and configuration information, if viewing		
ACL management	Manage Access Control Lists (ACLs) of resources or organizations and membership privileges for to groups and sub-groups in an ACL.	API call and configuration information	Call response and configuration information, if viewing		

Table 4 – Administrative Crypto-Officer Services

Security Crypto-Officer Role

The Security Crypto-Officer accesses the module over the Ethernet ports, with the typical configuration defaulting to only allowing the management Ethernet port for Security Crypto-Officer access. Using API calls invoked through a java-based application (this application is outside of the cryptographic boundary), the Security Crypto-Officer configures the module. The Security Crypto-Officer configures the module's services at a lower level than the Administrative Crypto-Officer, including setting WSDL policies, configuring XML encryption/decryption/signing/verifying policies at a fine-grained level, and configuring authentication methods for Users.

The Security Crypto-Officer accesses the module over an encrypted TLS session. The Security Crypto-Officer can be authenticated using digital certificates during the TLS handshake and/or using a username and password over the TLS session. The authenticated Security Crypto-Officer has access to the following services.

Service	Description	Input	Output	CSP	CSP Access
Login	Authenticate the Administrative Crypto-Officer role.	Login information	Result of login attempt	Administrative Crypto-Officer password	Read
Logout	Log out the Administrative Crypto-Officer.	Logout call	Call response		
TLS	Establish a TLS session and authenticate an operator with digital certificates, if configured.	TLS handshake parameters, TLS inputs	TLS outputs	TLS session keys DSA/RSA private keys DSA/RSA public keys	Read/Write Read Read/Write
WSDL and XML document import	Import WSDL and XML documents.	API call and WSDL/XML documents, if importing	Call response and WSDL/XML documents, if exporting		
WSDL and XML policy management	Create and manage WSDL and XML policies.	API calls and configuration information	Call response and configuration information, if viewing		
Filter and XPath configuration	Set filter priorities and create XPath Expressions to uniquely identify a document.	API calls and configuration information	Call response and configuration information, if viewing		
Process monitoring	Monitor run-time processes.	API calls and configuration information	Call response and status information		
Global/local filter configuration	Set global or local Request Filters on a policy.	API calls and configuration information	Call response and configuration information, if viewing		
Document archiving	Configure/tag individual elements, entire documents and/or both to store to Oracle, MySQL or	API calls and configuration information	Call response and configuration information, if viewing		

	DB2 database during Archive Document task.				
User management	Configure User Identity and Access Control options based on protocol.	API calls and configuration information	Call response and configuration information, if viewing		
XML encryption configuration	Configure XML encryption at the element or content level.	API calls and configuration information	Call response and configuration information, if viewing		
XML decryption configuration	Configure XML decryption at the element or content level.	API calls and configuration information	Call response and configuration information, if viewing		
XML signature generation configuration	Configure XML signatures on the entire document or elements with canonicalization options.	API calls and configuration information	Call response and configuration information, if viewing		
XML signature verification configuration	Configure XML digital signature Verification tasks.	API calls and configuration information	Call response and configuration information, if viewing		
Stylesheet configuration	Configure corporate/customer's requirements using XSLT stylesheets.	API calls and configuration information	Call response and configuration information, if viewing		
Credential mappings	Map credentials from Protocol to document-centric (SSL to SAML).	API calls and configuration information	Call response and configuration information, if viewing		
Credential bindings	Configure dynamic credential binding of private keys for signing.	API calls and configuration information	Call response and configuration information, if viewing		
Access control configuration	Configure Access Control options based on transport, protocol or document content in WSSecurity headers and/or SAML assertions.	API calls and configuration information	Call response and configuration information, if viewing		

Table 5 – Security Crypto-Officer Services

User Role

The User accesses the module over the Ethernet ports. Using standardized mechanism and protocols, such as web services interfaces and TLS, the User access the modules XML document processing, XML filtering, web services processing, and TLS initiation and termination.

Operators utilizing the module's TLS and XML functionality do so over TLS sessions authenticated via digital certificates (during the TLS negotiation), using usernames/passwords (over the TLS session), and/or using digital certificates (during XML document processing). The TLS session state table and the module's internal operator session states maintain separation of the various Users accessing the module concurrently.

Service	Description	Input	Output	CSP	CSP Access
TLS	Establish a TLS session and authenticate an operator with digital certificates, if configured	TLS handshake parameters, TLS inputs	TLS outputs	TLS session keys DSA/RSA private keys DSA/RSA public keys	Read/Write Read Read/Write
WS-Auth or SAML authentication	Authenticate using WS-Authentication mechanism or SAML over TLS session	WS-Auth or SAML credentials, including username/password or digital certificates	Result of login attempt	DSA/RSA public keys Username and passwords	Read/Write Read
WSDL and XML Document Processing	Perform processing of WSDL and XML documents, including encryption/decryption	API calls and documents, including any embedded public keys and RSA transported symmetric keys	API calls, result of processing, and documents, including any embedded public keys and RSA transported symmetric keys, depending on direction	DSA/RSA public keys XML encryption symmetric keys	Read/Write Read/Write

Table 6 – User Services

Authentication Mechanisms

Digital certificates (Administrative Crypto-Officer, Security Crypto-Officer, User) and passwords (Local Crypto-Officer, Administrative Crypto-Officer, Security Crypto-Officer, User) are used to authenticate and authorize users for access to various services based on access control lists and policies.

Authentication Type	Strength
Passwords	Passwords are required to be at least six characters long. Numeric, alphabetic (upper and lowercase), and keyboard and extended characters can be used. Considering only the case-sensitive alphanumeric character set using a password with repetition, the number of potential passwords is 62^6.
Public Key Certificates	RSA and DSA are used for authentication with 1024 bit (DSA, RSA) or 2048 bit (RSA) keys. Considering only 1024 bit key pairs, the strength of authentication

	is roughly equivalent to 2^80.

Table 7 – Estimated Strength of Authentication Mechanisms

Unauthenticated Services

The module provides a limited set of status commands through the serial port using the CLI. Although requiring local access to the module, these commands are still considered unauthenticated.

Service	Description	Input	Output	CSP	CSP Access
?	Help on non-enable mode commands	Command	Command response and help information		
exit	Exit CLI	Command	Command response		
network	View network interfaces (non-security related)	Command and sub-command	Command response		
show	Show some general configuration settings (non-security related)	Command and sub-command	Command response and configuration information		
system	View some general system configuration information (non-security related)	Command and sub-command	Command response and configuration information		

Table 8 – Unauthenticated Services

Physical Security

The FIA Gateway 1504G is a multi-chip standalone cryptographic module. The FIA is encased in an opaque, metal enclosure that encapsulates all the module's internal components. Only the physical ports defined above cross through the module's enclosure, and all vent holes are baffled to prevent viewing of the module's internal components. Additionally, tamper-evident labels are applied to the module's enclosure to provide evidence of physical tampering, and the internal components of the module cannot be viewed without removing the case.

The module was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

Operational Environment

The operational environment requirements do not apply to the FIA Gateway 1504G. The module does not provide a general purpose operating system and does not allow updating of its firmware components.

Cryptographic Key Management

The FIA Gateway 1504G utilizes the nCipher 1600 PCI card (Hardware Version nC3033P-1K6, Build Standard C, Firmware Version: 2.12.8-2) to provide implementations of RSA (PKCS #1) and DSA (FIPS 186-2), and to perform random number and key generation. This HSM has received FIPS 140-2 validation (certificate #402), and the module utilizes the HSM in compliance with the HSM's Security Policy. (Note: The nCipher 1600 PCI card supports additional cryptographic algorithms, which are not used by this module.)

Besides the FIPS 140-2 validated implementations provided by the HSM, the module implements the following FIPS algorithms:

- Symmetric Encryption Algorithms

Algorithm	Modes Implemented	Key Sizes	Algorithm Certificate Number
DES (FIPS 46-3) – for legacy use only	CBC	56 bits	265
Triple DES (FIPS 46-3)	CBC	168 bits (1, 2, and 3 key)	267
AES (FIPS 197)	CBC	128, 192, 256 bits	165

Table 9 – Symmetric Encryption Algorithms

- Hashing and HMAC Algorithms

Algorithm	Hash Sizes	Algorithm Certificate Number
SHA (FIPS 180-2)	160, 256, 384, 512	249
HMAC SHA1 (FIPS 198)		Vendor affirmed; SHA-1 249

Table 10 – Hashing and HMAC Algorithms

The module also implements the following non-Approved algorithms for use in a FIPS mode of operation.

- RSA key transport
- Diffie-Hellman key agreement

The module supports the following critical security parameters and keys:

Key	Key Type	Generation	Storage	Zeroization	Use
Security World Key	Triple-DES (168 bits)	Triple-DES key generated at initialization using the PRNG in the HSM (FIPS-approved nCipher 1600 PCI – certificate #402).	Stored Triple-DES encrypted on the hard drive and in plaintext in NVRAM	Zeroized by re-initializing the HSM.	Used to encrypt all keys stored on the hard drive in the module.

			in the HSM.		
Crypto-Officer Key	Triple-DES (168 bits)	Triple-DES key generated at initialization in the HSM (FIPS-approved nCipher 1600 PCI – certificate #402) or entered into the module through the smartcard serial port.	Not stored - in volatile memory only.	Zeroized in HSM immediately after use.	Used to encrypt the Security World Key stored on the hard drive in the module.
RSA Public Keys	RSA (1024-4096 bit)	RSA public key generated at initialization using the HSM (FIPS-approved nCipher 1600 PCI – certificate #402); or externally generated loaded onto the module in a certificate and/or over a TLS session	Stored Triple-DES encrypted on the hard drive; or not stored - in volatile memory only.	Zeroized using the delete button on the web admin interface for the corresponding key; or zeroized when the tunnel is torn down or when the module reboots.	Used for XML based document processing (signing/verification/key transport) on behalf of the users. Used during TLS session establishment. Used for certificate verification.
RSA Private Keys	RSA (1024-4096 bit)	RSA private key generated at initialization using the HSM (FIPS-approved nCipher 1600 PCI – certificate #402); or externally generated loaded onto the module over a TLS session; or externally generated loaded onto the module over a TLS session.	Stored Triple-DES encrypted on the hard drive.	Zeroized using the delete button on the web admin interface for the corresponding key.	Used for XML based document processing (signing/verification/key transport) on behalf of the users. Used during TLS session establishment.
DSA Public Keys	DSA (1024 bit)	DSA public key generated at initialization using the HSM (FIPS-approved nCipher 1600 PCI – certificate #402); or externally generated loaded onto the module in a certificate and/or over a TLS session	Stored Triple-DES encrypted on the hard drive; or not stored - in volatile memory only.	Zeroized using the delete button on the web admin interface for the corresponding key; or zeroized when the tunnel is torn down or when the module reboots.	Used for XML based document processing (signing/verification) on behalf of the users. Used during TLS session establishment. Used for certificate verification.
DSA Private Keys	DSA (1024 bit)	DSA private key generated at initialization using the HSM (FIPS-approved nCipher 1600 PCI – certificate #402); or externally generated loaded onto the module over a TLS session.	Stored Triple-DES encrypted on the hard drive.	Zeroized using the delete button on the web admin interface for the corresponding key.	Used for XML based document processing (signing/verification) on behalf of the users. Used during TLS session establishment.
TLS session keys	AES (128, 256 bits), Triple-DES (168 bits),	Negotiated during TLS session establishment.	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used to encrypt/MAC the TLS session.

	DES (56 bits) for legacy use only, SHA-1 HMAC (160 bits)				
Diffie-Hellman key pairs	Diffie-Hellman (768, 1024, or 1536 bit)	Generated for TLS session establishment using the PRNG in the HSM (FIPS-approved nCipher 1600 PCI – certificate #402).	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used by the module in establishing a session key during TLS negotiation.
XML encryption symmetric keys	AES (128, 192, or 256 bits), Triple-DES (168 bits), DES (56 bits) for legacy use only	Entered into the module RSA encrypted or generated by the module using the PRNG in the HSM (FIPS-approved nCipher 1600 PCI – certificate #402).	Not stored - in volatile memory only in plaintext.	Zeroized when the module is powered down.	Used to encrypt/decrypt documents during document processing using XML encryption.
Username and passwords	Passwords	Entered by an operator.	Stored on the hard drive in file in plaintext.	Zeroized when the password is updated with a new one or the user is deleted.	Used for authentication of Security Crypto-Officers, Administrative Crypto-Officers, and Users.
Local Crypto-Officer (enable) password for the Serial interface	Password	Entered by an operator.	Stored in the hard drive in configuration files and Triple-DES encrypted.	Zeroized when the password is updated with a new one.	Used for authenticating the Local Crypto-Officer over the serial interface.

Table 11 – Keys and CSPs

Key Generation

The FIA Gateway 1504G uses the FIPS 140-2 validated HSM (certificate #402) to perform all key generation.

Key Entry and Output

All private and secret keys are entered into or output from the module through the administrative interfaces encrypted by virtue of a TLS session using FIPS-approved cipher suites (AES and Triple-DES for encryption). Only the Crypto-Officer key can be entered through the smartcard port, and this is entered using a threshold scheme as defined in the HSM's Security Policy. Keys are never sent out through the data path.

Key Storage

The username/passwords are stored on the module's hard drive in plaintext. The Security World Key is stored on the module's hard drive encrypted by the Crypto-Officer key and is stored within the HSM in plaintext. Ephemeral keys (TLS session keys and Diffie-Hellman key pairs) are only stored in volatile memory in plaintext. The Crypto-Officer key is only stored in volatile memory in plaintext. All other keys and CSPs are stored encrypted on the module's hard drive with the Security World Key.

Key Zeroization

The Security World Key can be zeroized by reinitializing the HSM. Additionally, this zeroizes all keys encrypted with the Security World Key. The username/passwords and Local Crypto-Officer password can be zeroized by changing the passwords. User RSA and DSA key pairs and the System RSA key pair can be zeroized using the delete command through the module's management API. Ephemeral keys can be zeroized by rebooting the module or when the keys usage ends. All keys can be zeroized by returning to a factory state and rebooting.

Self-Tests

The module's HSM is already FIPS 140-2 validated (certificate # 402) and performs all of the self-tests required by that validation. More information on the HSM and its self-tests can be found in the nCipher 1600 PCI FIPS 140-2 Security Policy.

Besides the self-tests implemented by the FIPS 140-2 validated HSM, the FIA Gateway 1504G implements the following power-up self-tests. (Note: All of the required conditional self-tests are implemented by the HSM.)

- Power-up Self-tests
    - Software/firmware integrity test
    - DES KAT
    - TDES KAT
    - AES KAT
    - SHA (SHA-1, SHA-256, SHA-384, SHA-512) KAT
    - HMAC SHA1 KAT

The FIA Gateway 1504G performs all the power up self tests automatically every time the module starts. The module inhibits data output while the self-tests are being performed.

If any of the self-tests fails, the module will stop all functionality and the cryptographic functionality will be unavailable. In this error state, the

Crypto-Officer can access the box through the serial interface, but all other interfaces do not respond. The module is not capable of data output or cryptographic processing while in an error state.

The results of all self-tests are logged in the module and output to the console. The Crypto-Officer can also see the current mode of operation of the module in the logs.

Design Assurance

Forum Systems use established software engineering principles and methodologies in all phases of development of the module. The open source configuration management tool Concurrent Versions System (CVS) is used as the repository for source code and documentation.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the module's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

This section is not applicable. The FIA Gateway 1504G does not claim to mitigate any attacks beyond the FIPS 140-2 level 2 requirements for this validation.

SECURE OPERATION

The Forum FIA Gateway 1504G meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Local Crypto-Officer Guidance

This section describes the instructions to the Crypto-Officer to run the module in a FIPS approved mode of operation. Additional guidance for the Crypto-Officer can be found in the FIA administrator manuals.

Additional guidance for the Security Crypto-Officer can be found in the Forum Systems Installation Guide.

Initialization

The Forum FIA is available for shipment from Forum Systems using a bonded carrier or for direct pickup from a Forum facility. Upon receipt of the Forum FIA for Forum Systems, the Local Crypto-Officer must inspect the packing materials for the FIA.

The FIA is shipped in a Forum box sealed with tape. Within the box, the FIA is enclosed in a plastic bag also sealed with tape. The Local Crypto-Officer must check these materials for signs of tampering, including damage to the packaging or the module. If any such evidence is found, the Local Crypto-Officer must not utilize the module and should contact Forum Systems for assistance.

After unpacking the module and verifying there is no evidence of tampering, the module's faceplate must be attached and the tamper-evident labels applied. The following steps described installation of the faceplate and application of the labels.

1. Turn off and unplug the system, and clean the areas of the chassis to which the labels will be applied of any grease, dirt, or oil.

2. Facing the front of the FIA, apply a tamper-evident label across the front panel and bottom of the chassis in the lower left-hand corner of the front of the module as depicted in Figure 3.

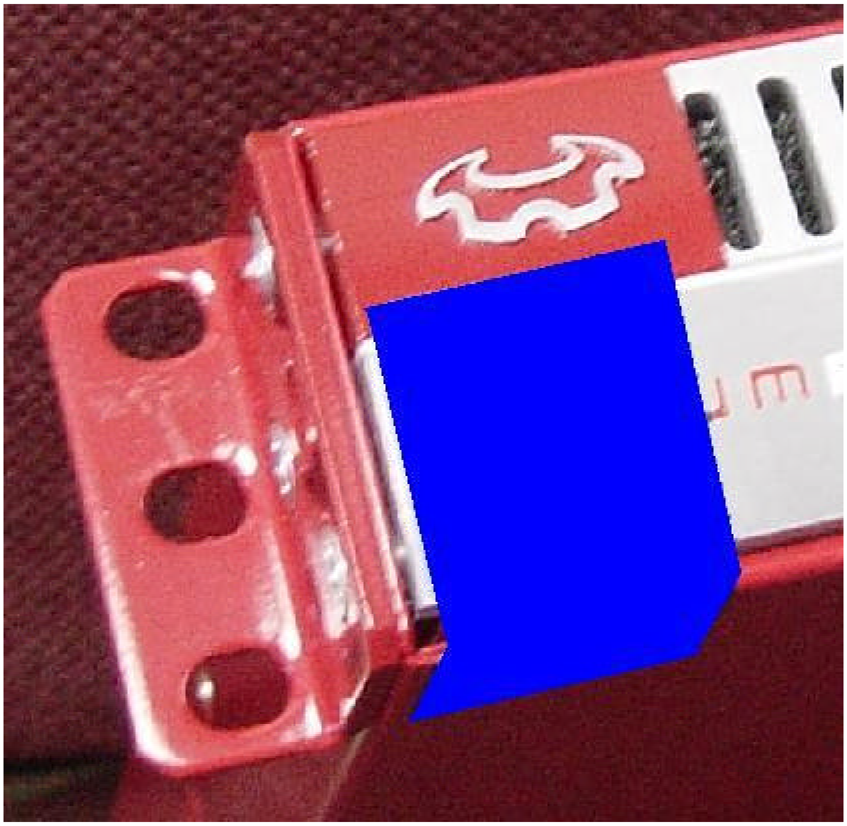


Figure 3 – Apply label to lower left of the front of the FIA

3. Facing the front of the FIA, apply a tamper-evident label across the front panel and top of the chassis in the upper right-hand corner of the front of the module as depicted in Figure 4. The label should cover one of the screws holding the top cover in place.

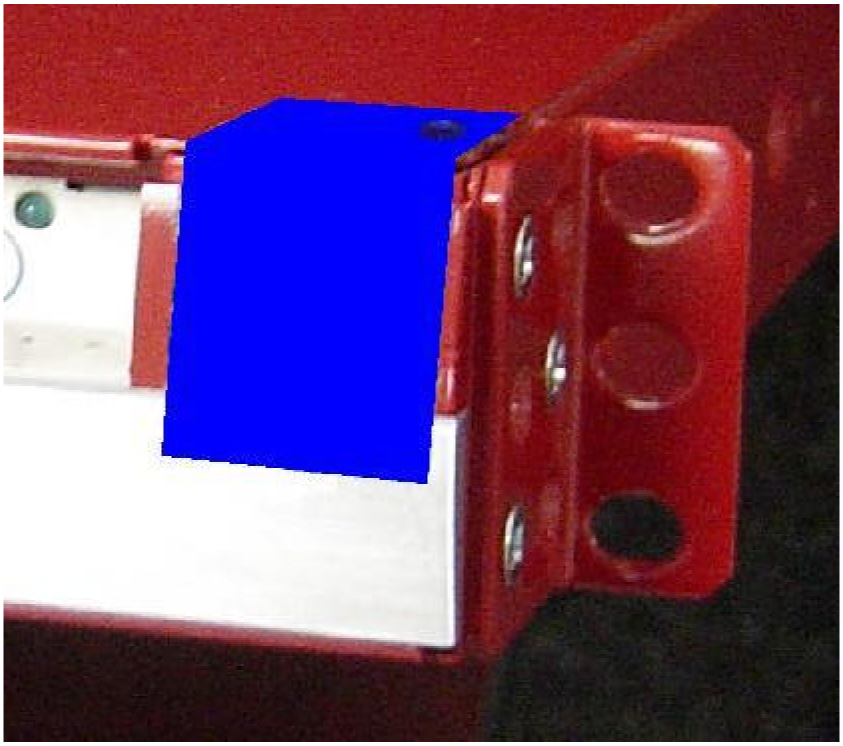


Figure 4 – Apply label to upper right of the front of the FIA

4. Facing the rear of the FIA, apply a tamper-evident label across the front panel and top of the chassis slightly off-center from the middle of the rear of the module as depicted in Figure 5. The label should cover two of the screws holding the second and third fans in place (counting from the right). The label should also cover one of the screws holding the top cover in place.

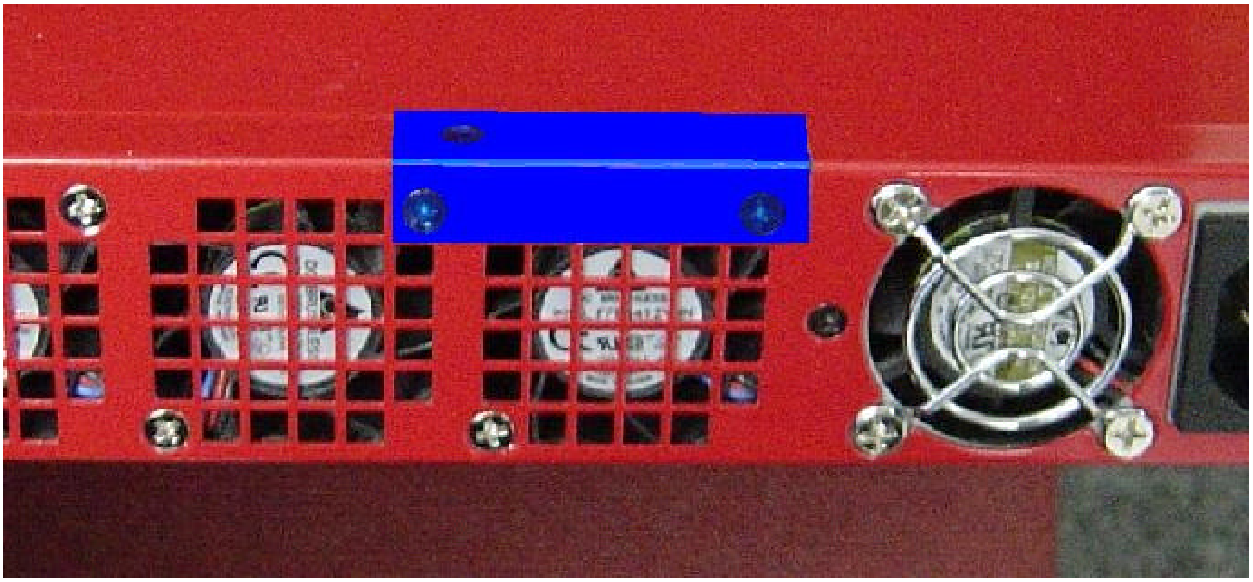


Figure 5 – Apply label to upper off-center of the rear of the FIA

5. Record the serial numbers of the applied labels in a security log.

6. Allow a minimum of 24 hours for the labels to cure.

After the tamper-evident labels have been applied, the Local Crypto-Officer must initialize the module, during which, a Local Crypto-Officer password ("enable" password) must be configured. Until this point, the module does not have any authentication information and must be maintained in the control of the Local Crypto-Officer.

After this initialization, the module must be switched to FIPS mode using the following command.

```
system config fips-mode
```

Enter "Y" when prompted to confirm the switch to FIPS mode, and the module will automatically reboot. After the module has restarted, run the following command to verify the module is in a FIPS mode of operation.

```
show fips-mode
```

Management

The Local Crypto-Officer must check the module's case and tamper-evident labels for signs of tampering, including dents, damage to the labels, or changes in the recorded label serial numbers. If tamper-evidence is found, the Local Crypto-Officer should immediately take the module offline and investigate.

If the module is taken out of FIPS mode into a non-FIPS mode, the Crypto-Officer should delete all CSPs and keys on the module by taking the module back into the factory default state using the following command.

```
system config factory-reset
```

The Crypto-Officer must confirm the factory reset command, and the module will automatically reboot. Since the HSM does not leave its FIPS mode, it is not necessary to zeroize the HSM.

Termination

At the end of the module's usage, the Local Crypto-Officer must zeroize all CSPs and keys on the module using the following command.

```
system config factory-reset
```

The Crypto-Officer must select zeroization of the HSM and confirm the factory reset, and then the module will automatically reboot.

Administrative Crypto-Officer Guidance

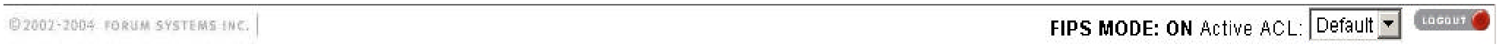
The Administrative Crypto-Officer must configure the module's global policies to be in compliance with FIPS. The guidelines for this configuration are outlined in the following sections.

Additional guidance for the Security Crypto-Officer can be found in the Forum Systems Sentry Web Administration Guide Part 1, Part 2, and Part 3.

Note: All diagrams in this section are the HTML output by the module rendered by an external browser.

Initialization

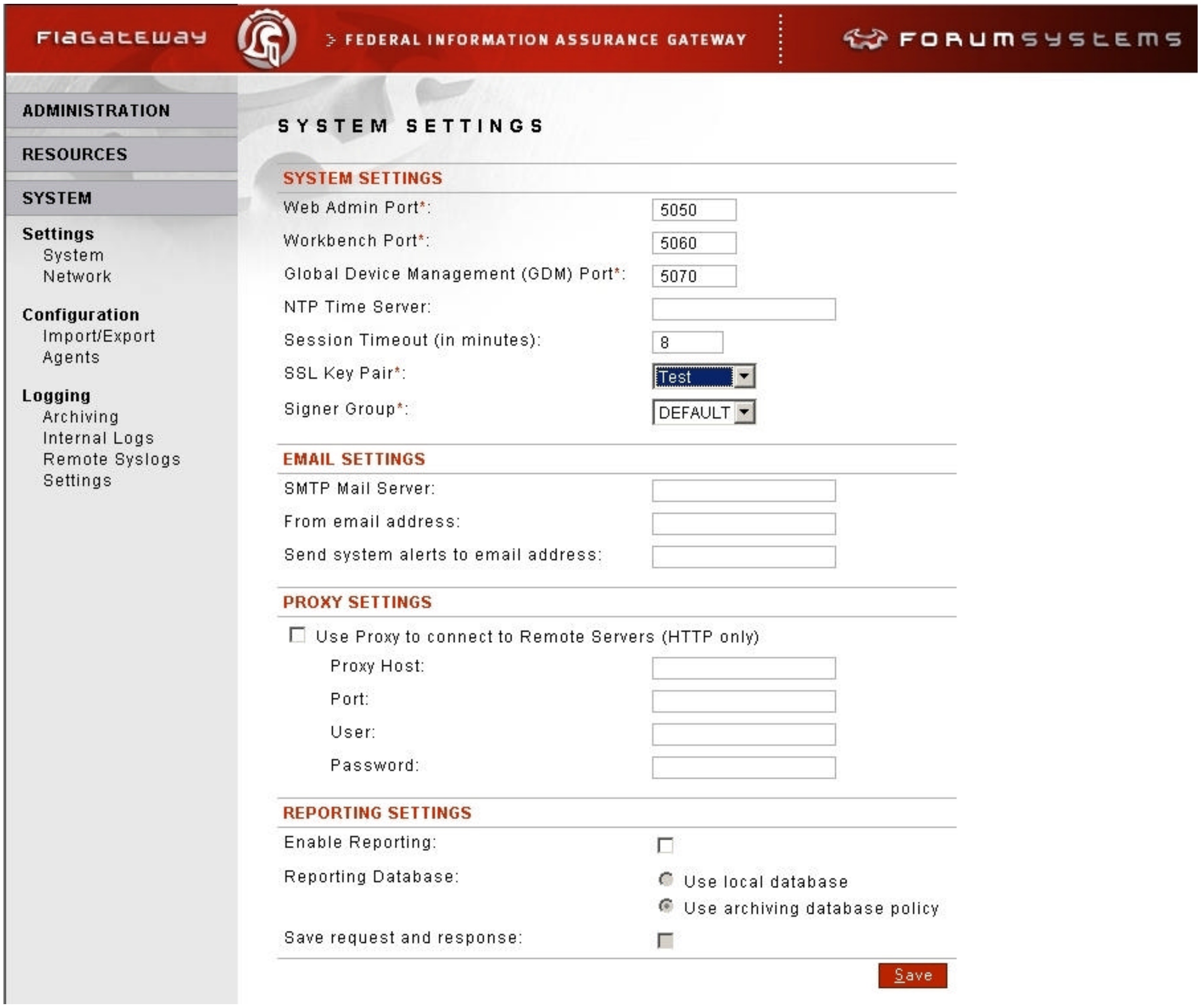
Most of the configuration for FIPS mode is handled when the Local Crypto-Officer runs the "fips-mode" command as detailed above. The Administrative Crypto-Officer can verify the module is in FIPS mode through the WebAdmin interface looking at the lower right-hand corner of the screen.



FIPS MODE: ON Active ACL: Default

Figure 6 – FIPS Mode Indicator

The Administrative Crypto-Officer must change the default key pair. This can be performed through the WebAdmin interface as follows.



SYSTEM SETTINGS

SYSTEM SETTINGS

Web Admin Port*: 5050

Workbench Port*: 5060

Global Device Management (GDM) Port*: 5070

NTP Time Server:

Session Timeout (in minutes): 8

SSL Key Pair*: Test

Signer Group*: DEFAULT

EMAIL SETTINGS

SMTP Mail Server:

From email address:

Send system alerts to email address:

PROXY SETTINGS

□ Use Proxy to connect to Remote Servers (HTTP only)

Proxy Host:

Port:

User:

Password:

REPORTING SETTINGS

Enable Reporting: □

Reporting Database: ○ Use local database ● Use archiving database policy

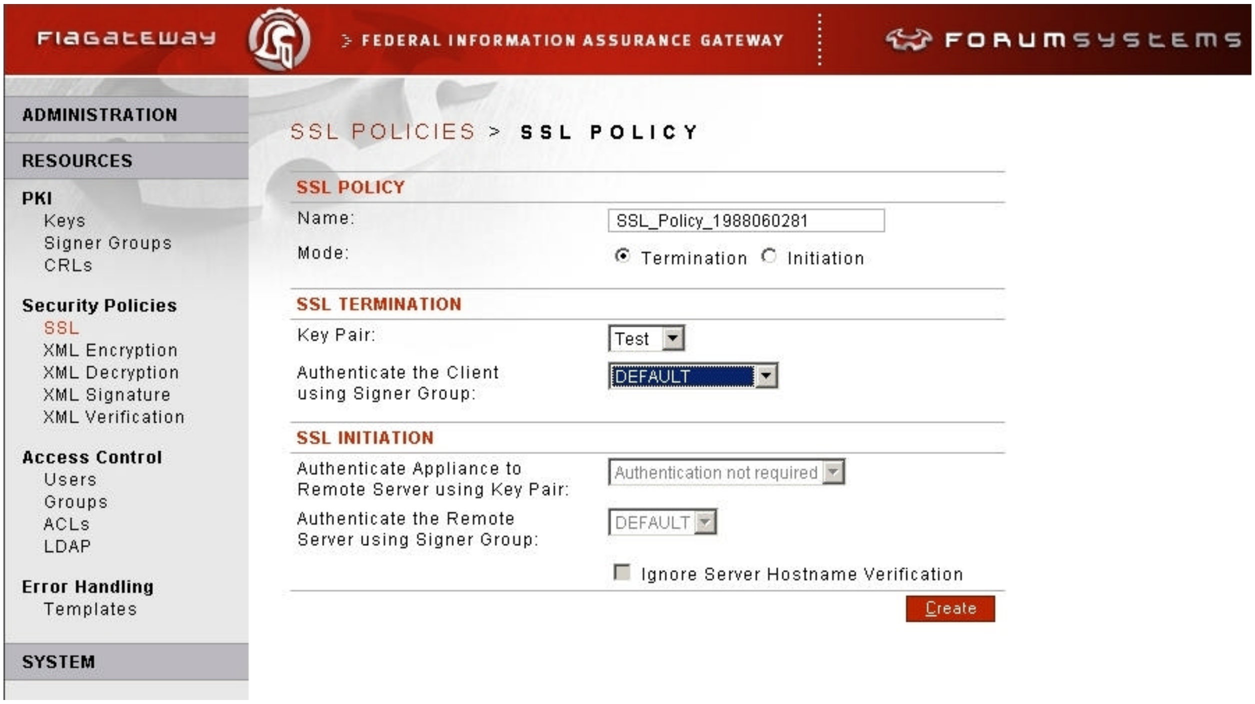
Save request and response: □

Figure 7 – Change SSL Key Pair

Management

In FIPS mode, the module only provides a subset of its supported algorithms and services. When generating key pairs, only RSA keys pairs greater than or equal to 1024 bits in size and DSA key pairs equal to 1024 bits in size may be generated. XML encryption and decryption policies only allow the support of FIPS-approved algorithms. FTP and OpenPGP cannot be enabled. SSLv2 and SSLv3 are disabled, and only TLSv1 with FIPS-approved algorithms is allowed. Administrator Crypto-Officer access must only be over a TLSv1 session that uses cipher suites requiring AES and Triple-DES encryption.

The module’s SSL policies must be configured to require authentication. For the SSL initiation policy, this is configured by setting the “Authenticate the Remote Server using Signer Group” parameter to a particular signer group (i.e., a particular set of accepted certificates). For the SSL initiation policy, this either configured by setting the “Authenticate the Client using Signer Group” parameter to a particular signer group (i.e., a particular set of accepted certificates) or by configuring the HTTP listener policy to “Basic Auth.”



SSL POLICIES > SSL POLICY

SSL POLICY

Name: SSL_Policy_1988060281

Mode: ● Termination ○ Initiation

SSL TERMINATION

Key Pair: Test

Authenticate the Client using Signer Group: DEFAULT

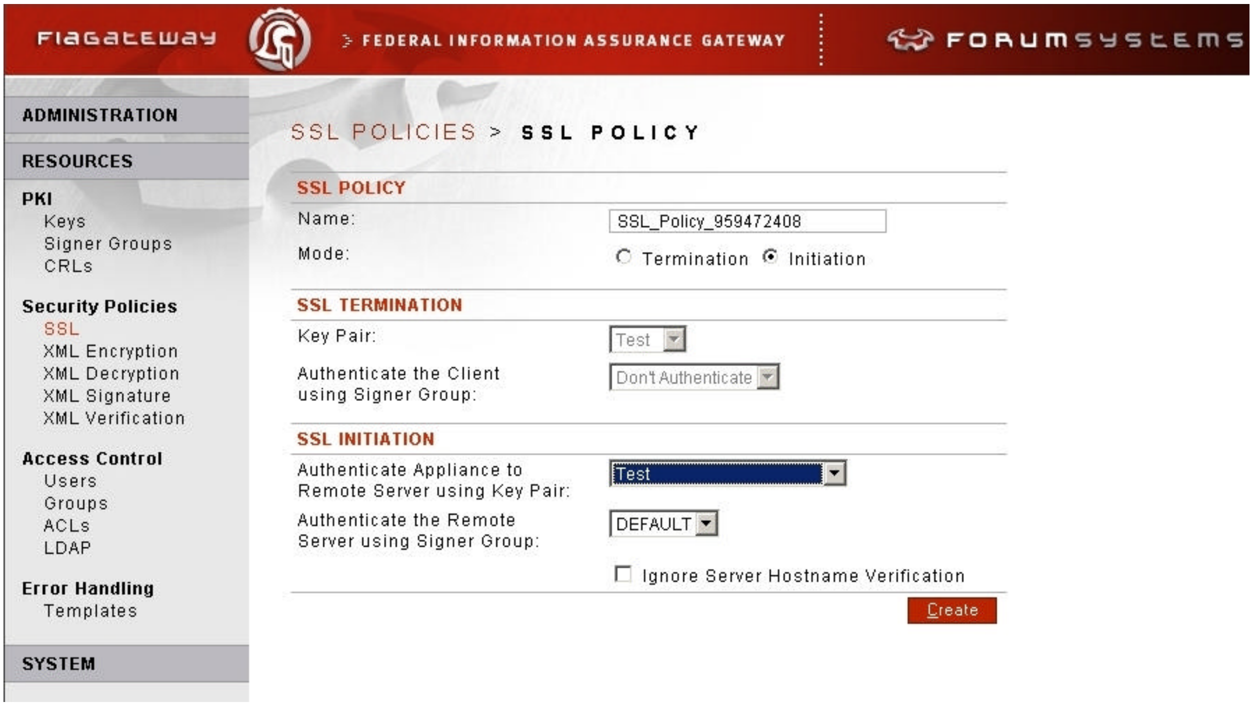
SSL INITIATION

Authenticate Appliance to Remote Server using Key Pair: Authentication not required

Authenticate the Remote Server using Signer Group: DEFAULT

□ Ignore Server Hostname Verification

Figure 8 – Change Setting to Authenticate Remote Server



SSL POLICIES > SSL POLICY

SSL POLICY

Name: SSL_Policy_959472408

Mode: ○ Termination ● Initiation

SSL TERMINATION

Key Pair: Test

Authenticate the Client using Signer Group: Don't Authenticate

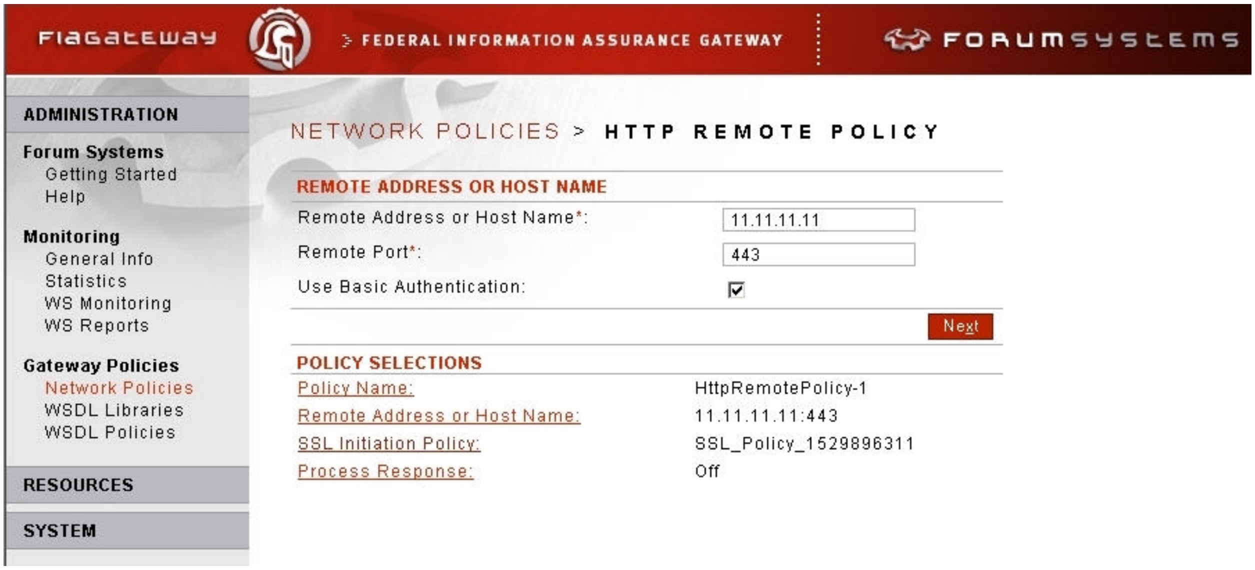
SSL INITIATION

Authenticate Appliance to Remote Server using Key Pair: Test

Authenticate the Remote Server using Signer Group: DEFAULT

□ Ignore Server Hostname Verification

Figure 9 – Change Setting to Authenticate Client



NETWORK POLICIES > HTTP REMOTE POLICY

REMOTE ADDRESS OR HOST NAME

Remote Address or Host Name*: 11.11.11.11

Remote Port*: 443

Use Basic Authentication: ☑

POLICY SELECTIONS

Policy Name: HttpRemotePolicy-1

Remote Address or Host Name: 11.11.11.11:443

SSL Initiation Policy: SSL_Policy_1529896311

Process Response: Off

Figure 10 – Change Setting to Authenticate Remote Server

The Crypto-Officer must routinely check the logs for any indicators of problems or suspicious activity. If an error is indicated, the Administrative Crypto-Officer should immediately take the module offline and investigate.

Security Crypto-Officer Guidance

The Security Crypto-Officer's ability to configure the module is primarily governed by the configuration put in place by the Administrative Crypto-Officer. Thus, the Security Crypto-Officer does not have many rules to follow to operate the module properly.

Additional guidance for the Security Crypto-Officer can be found in the Forum Systems Sentry XIP Guide Part 1 and Part 2.

Management

The Security Crypto-Officer must configure all users to authenticate. With the restriction established by the Administrative Crypto-Officer requiring all communications to be over a TLS session, the Security Crypto-Officer is permitted to configure Users to authenticate using any of the supported mechanisms.

User Guidance

There is no special guidance for the User with regards to operating the module as the User does not have any ability to modify the configuration of the module. However, the User must take care not to disclose any passwords or secret/private keys. Additionally, unless the User requires DES encryption for legacy purposes, only AES and Triple-DES are to be used for data encryption.

.

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
CVS	Concurrent Versions System
DES	Data Encryption Standard
DSA	Digital Signature Standard
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GDM	Global Device Management
HMAC	(Keyed-) Hash MAC
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standards
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SAML	Security Associations Markup Language
SHA	Secure Hash Algorithm
WAN	Wide Area Network
WSDL	Web Services Description Language
XML	eXtensible Markup Language
VSS	Visual Source Safe