FIPS 140-2 Non-proprietary Security Policy

LogRhythm 6.0.4 or 6.3.4 Log Manager

LogRhythm, Inc.
4780 Pearl East Circle
Boulder, CO 80301

April 15, 2016

Document Version 2.1
Module Versions 6.0.4 or 6.3.4

Table of Contents

1. Introduction

LogRhythm is an integrated log management and security information event management (SIEM) solution. It is a distributed system containing several cryptographic modules, which support secure communication between components. A LogRhythm deployment is made up of System Monitor Agents, Log Managers, Advanced Intelligence (AI) Engine Servers, Event Manager, and Consoles. Each System Monitor Agent collects log data from network sources. Each Log Manager aggregates log data from System Monitor Agents, extracts metadata from the logs, and analyzes content of logs and metadata. A Log Manager may forward log metadata to an AI Engine Server and may forward significant events to Event Manager. An AI Engine Server analyzes log metadata for complex events, which it may forward to Event Manager. Event Manager analyzes events and provides notification and reporting. LogRhythm Console provides a graphical user interface (GUI) to view log messages, events, and alerts. Console also is used to manage LogRhythm deployments. LogRhythm relies on Microsoft SQL Server. LogRhythm stores log data in SQL Server databases on Log Manager and Event Manager. It stores configuration information in SQL Server databases on Event Manager. System Monitor Agent, Log Manager, AI Engine Server, Event Manager, and Console each include a cryptographic module.

This document describes the security policy for the LogRhythm Log Manager cryptographic module. It covers the secure operation of the Log Manager cryptographic module including initialization, roles, and responsibilities for operating the product in a secure, FIPS-compliant manner. This module is validated at Security Level 1 as a multi-chip standalone module. The module relies on the Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) (certificate #1336) cryptographic module.

2. Overview

The LogRhythm Log Manager cryptographic module provides cryptographic services to a Log Manager. In particular, these services support secure communication with other LogRhythm components (System Monitor Agents and AI Engine Servers) and SQL Server databases.

A Log Manager is a server running the LogRhythm Mediator Server service and Microsoft SQL Server 2008 R2. The Mediator Server service processes log messages. The Log Manager SQL Server stores log messages as well as metadata the Mediator extracts from logs. Log Manager runs on a general purpose computer (GPC). The Log Manager operating system is Windows Server 2008 R2 SP1. The Log Manager cryptographic module was tested on an x64 processor.

The Log Manager cryptographic module is a software module. Its physical boundary is the enclosure of the standalone GPC on which the Log Manager runs. The software within the logical cryptographic boundary consists of all software assemblies for the Mediator Server service. The Mediator Server software consists of the following files in "C:\Program Files\ LogRhythm\LogRhythm Log Manager":

- lrgeoip.dll
- lrhmcommgr.dll
- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.IPWorksSSL.dll
- nsoftware.IPWorksSSNMP.dll
- nsoftware.System.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll
- sccscomn.dll
- scmedeng.dll
- scmedsvr.exe
- scmedsvr.hsh
- scmessage.dll
- scmpeeng.dll
- scopsec.dll
- scshared.dll
- scvbcomn.dll

Other files and subdirectories of "C:\Program Files\LogRhythm\LogRhythm Log Manager" are outside the logical cryptographic boundary. The excluded files are:

- EULA.rtf
- lrconfig.exe
- lrmedperf.dll
- scmedsvr.exe.config
- sccsuicomn.dll
- Infragistics2.Shared.v9.2.dll
- Infragistics2.Win.Misc.v9.2.dll
- Infragistics2.Win.UltraWinDataSource.v9.2.dll
- Infragistics2.Win.UltraWinEditors.v9.2.dll
- Infragistics2.Win.UltraWinGrid.v9.2.dll
- Infragistics2.Win.UltraWinTabControl.v9.2.dll
- Infragistics2.Win.UltraWinToolbars.v9.2.dll
- Infragistics2.Win.v9.2.dll

The excluded directories (along with their subdirectories) are:

- config
- logs
- state

The Log Manager cryptographic module relies on a cryptographic service provider from the operating system, namely BCRYPTPRIMITIVES.DLL. The cryptographic service provider from the operating system is the following FIPS 140-2 validated cryptographic module:

Microsoft Windows Server 2008 R2 Cryptographic Primitives Library
Certificate #1336

Figure 1 Cryptographic Module Boundaries illustrates the relationship between the Log Manager cryptographic module and the Log Manager as a whole. It shows physical and logical cryptographic boundaries of the module.

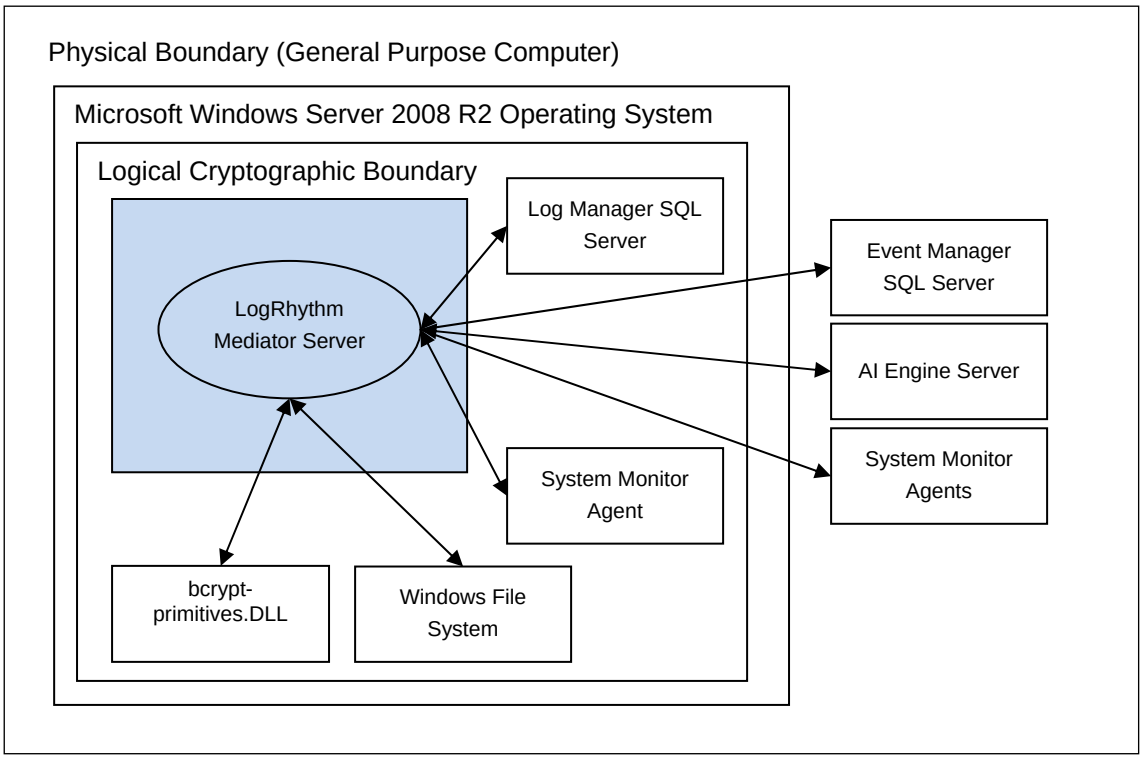

Figure 1 Cryptographic Module Boundaries

2.1. Ports and Interfaces

The Log Manager cryptographic module ports consist of one or more network interface cards (NIC) on the Log Manager GPC. NIC are RJ45 Ethernet adapters, which are connected to IP network(s).

All data enters the Log Manager Server physically through the NIC and logically through the GPC's network driver interface to the module. Hence, the NIC correspond to the data input, data output, control input, and status output interfaces defined in [FIPS 140-2]. Although located on the same GPC as the cryptographic module, the Windows operating system file system and Windows Event Log are outside the logical cryptographic boundary. Hence, the file system and Windows Event Log also present data input, data output, control input, and status output logical interfaces.

Data input to Log Manager is made up of log messages. System Monitor Agents collect log messages and send them to the Log Manager over a TLS socket connection. Log Manager can archive log data to the Windows file system. Data output from Log Manager comprises log data sent to AI Engine Server and to SQL Servers as well as data written to the local file system. Log Manager sends log data to the AI Engine Server over a TLS socket connection.

Log Manager sends raw log data to the Log Manager SQL Server and event data to the Event Manager SQL Server using TLS connections. Log data output to the local file system consists of archive plain text log data, suspense log files, and unprocessed logs. The Console provides a graphical interface to configure the Log Manager cryptographic module, but configuration information reaches the module indirectly through the Event Manager SQL Server. (The Console is a separate and distinct component of a LogRhythm deployment.) The Console connects to Event Manager SQL Server and stores configurations in a database. The Mediator service retrieves the configuration information from the database. Hence, the TLS connection to the Event Manager SQL Server serves as the control input interface. The status output interface comprises the TLS connection to the Event Manager SQL Server, the local file system, and the Windows Event Log. The Log Manager sends status information to Event Manager SQL Server using TLS, which makes it available to the Console. The Log Manager writes status information to log files in the file system and the Windows Event Log.

2.2. Modes of Operation

The Log Manager cryptographic module has two modes of operation: Approved and non-Approved. Approved mode is a FIPS-compliant mode of operation. The module provides the cryptographic functions listed in Table 1 and Table 2 below. While the functions in Table 2 are not FIPS Approved, they are allowed in Approved mode of operation when used as part of an approved key transport scheme where no security is provided by the algorithm.

Table 1 FIPS Approved Cryptographic Functions

Label	Approved Cryptographic Function	Standard
AES	Advanced Encryption Algorithm	FIPS 197
HMAC-SHA-1	Keyed-Hash Message Authentication Code SHA-1	FIPS 198-1
DRBG	Deterministic Random Bit Generator	SP 800-90A
RSA	Rivest Shamir Adleman Signature Algorithm	FIPS 186-2 (PKCS#1 v2.1 and ANSI X9.31-1998)
SHS	Secure Hash Algorithm	FIPS 180-4

Table 2 FIPS Non-Approved Cryptographic Functions

Label	Non-Approved Cryptographic Function
MD5	Message-Digest Algorithm 5
HMAC-MD5	Keyed Hash Message Authentication Code MD5

The Log Manager cryptographic module does not implement a bypass capability.

2.3. Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 1.

Table 3 FIPS 140-2 Non-proprietary Security Policy

LogRhythm 6.0.4 or 6.3.4 Log Manager Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	N/A
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Operational Environment	1

3. Roles

In Approved mode, Log Manager cryptographic module supports two roles: User and Crypto Officer. Roles are assumed implicitly, since the module does not provide user authentication.

1. User Role: Operators with the User role are other components of a LogRhythm deployment configured to interact with the Log Manager. These are: System Monitor Agents, AI Engine Server, Log Manager SQL Server, and Event Manager SQL Server.

2. Crypto Officer Role: Operators with the Crypto Officer role have direct access to the cryptographic module. Responsibilities of the Crypto Officer role include initial configuration, on-demand self test, and status review.

4. Services

In Approved mode, the services available to an operator depend on the operator's role. Roles are assumed implicitly.

4.1. User Services

4.1.1. Agent Write Log Data

This service provides a protected communication channel to transfer log data collected by the System Monitor Agent to a Log Manager. The channel is established in accordance with the Log Manager configuration. (See service Write Log Manager Configuration.) The connection uses TLS 1.0 with cipher suite based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES _128_CBC_SHA).

4.1.2. Read Agent Configuration

This service provides a protected communication channel to transfer configuration data from a Log Manager to the System Monitor Agent. The channel is established in accordance with the Log Manager configuration. (See service Write Log Manager Configuration.) The connection uses TLS 1.0 with cipher suite based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES _128_CBC_SHA).

4.1.1. AI Engine Server Read Log Data

This service provides a protected communication channel to transfer log data from Log Manager to an AI Engine Server. The channel is established in accordance with the Log Manager configuration set. (See service Write Log Manager Configuration.) The connection uses TLS 1.0 with cipher suite based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC _SHA).

4.1.2. Event Manager Read Log Data

This service provides a protected communication channel to transfer log data from the Log Manager to Event Manager SQL Server. An operator in the Crypto Officer role sets up communication between the Log Manager and the Event Manager SQL Server. (See service Configure Log Manager Communication.) The channel is established in accordance with the Log Manager configuration. (See service Write Log Manager Configuration.) The connection uses TLS 1.0 with cipher suite based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC _SHA).

4.1.3. Log Manager Read/Write Log Data

The Mediator Server service stores log data and metadata in Log Manager SQL Server databases. This service provides a protected communication channel to transfer log data between the Log Manager and Log Manager SQL Server. The channel is established in accordance with the Log Manager configuration. (See service Write Log Manager Configuration.) The connection uses TLS 1.0 with cipher suite based on RSA key agreement

with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC_SHA).

4.1.4. Write Log Manager Configuration

This service provides a protected communication channel to transfer configuration information from the Event Manager SQL Server to the Log Manager. An operator in the Crypto Officer role sets up communication between the Log Manager and the Event Manager SQL Server. (See service Configure Log Manager Communication.) After set up, an operator in the User role (that is, the Event Manager SQL Server) uses this service to propagate configuration changes to the Log Manager. The connection uses TLS 1.0 with cipher suite based on RSA key agreement with AES 128-bit encryption for confidentiality and SHA-1 for integrity protection (TLS_RSA_WITH_AES_128_CBC_SHA).

Note that a Log Manager's configuration originates from the Console. The Console transfers the configuration information to the Event Manager SQL Server.

4.1.5. Seal Archive File

The Log Manager can archive log data to a file in the file system. In a process called sealing, the Log Manager computes and stores a cryptographic hash of an archive file. Log Manager uses SHA-1 for the cryptographic hash. It stores the hash value in an Event Manager SQL Server database. The Log Manager performs the Archive Sealing service in accordance with the Log Manager configuration. (See service Write Log Manager Configuration.)

4.2. Crypto Officer Services

4.2.1. Configure Log Manager Communication

After the Log Manager has been installed, this service provides an operator in the Crypto Officer role with the capability to configure the Log Manager to communicate with Event Manager. This consists of setting the IP address for the Event Manager. Log Manager authenticates the AI Engine Server for TLS sessions. Optionally, a Crypto Officer may pre-place a user-provided certificate on the Log Manager for mutual authentication of TLS sessions with the AI Engine Server. The Event Manager SQL Server provides all other configuration information. (See service Write Log Manager Configuration.)

4.2.2. Perform Self-Tests

Log Manager module performs a (start-up) power-on software integrity test to verify the integrity of the component software. If the module fails a software integrity test, it reports status indicating which failure occurred and transitions to an error state, in which the module ceases to continue processing. The Log Manager will not be able to receive logs and cannot output data to SQL Server databases when it is in an error state.

An operator can run the software integrity test on demand by stopping and starting the module. The system integrity test will always run at startup regardless of FIPS Mode.

4.2.3. Show FIPS Status

Log Manager provides status information about the cryptographic module mode of operation through Log Manager log file. When the Log Manager component is started, the Mediator service writes a message to the log indicating the mode of operation, for example:

Mediator running in FIPS mode: YES

To determine whether Log Manager is in Approved mode, an operator in the Crypto Officer role checks the Mediator Server service log, scmedsvr.log.

Similarly, LogRhythm provides information about communication encryption through Log Manager log files. When the Log Manager component is started, the Mediator service writes a message to the log file indicating whether encryption is being used, for example.

Mediator using encryption for SQL Server communications: YES

To determine whether Log Manager is encrypting communication, check the Mediator Server service log, scmedsvr.log. The Log Manager cryptographic module must be encrypting communication in order to be considered operating in Approved mode.

The Log Manager cryptographic module may enter an error state and stop (for example, when a power-up integrity test fails). An operator in the Crypto Officer role checks the Mediator log file (scmedsvr.log) and the Windows Event Log for error messages to determine the cause of the cryptographic module's error state.

5. Policies

5.1. Security Rules

In order to operate the Log Manager cryptographic module securely, the operator should be aware of the security rules enforced by the module. Operators should adhere to rules required for physical security of the module and for secure operation.

The Log Manager cryptographic module enforces the following security rules when operating in Approved mode (its FIPS compliant mode of operation). These rules include both security rules that result from the security requirements of FIPS 140-2 and security rules that LogRhythm has imposed.

1. Approved mode is supported on Window Server 2008 R2 SP1 in a single-user environment.

2. The Log Manager cryptographic module operates in Approved mode only when used with the FIPS approved version of Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) validated to FIPS 140-2 under certificate #1336 operating in FIPS mode.

3. The Log Manager cryptographic module is in Approved mode only when it operates in the environment of BCRYPTPRIMITIVES, namely:

   i) FIPS approved security functions are used and Windows is booted normally, meaning Debug mode is disabled and Driver Signing enforcement is enabled;

   ii) One of the following DWORD registry values is set to 1:

      (1) HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled

      (2) HKLM\SYSTEM\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration\SelfTestAlgorithms

4. When installed on a system where FIPS is enabled, Log Manager runs in a FIPS-compliant mode of operation. When communicating with other LogRhythm components, the Log Manager encrypts communication including:

   - Module to System Monitor Agent
   - Module to Log Manager SQL Server
   - Module to Event Manager SQL Server
   - Module to AI Engine Server

5. The Log Manager cryptographic module operates in Approved mode only when using pre-placed, user-provided certificates for TLS communication with the Mediator service. Dynamically-generated, self-signed certificate for the Mediator

service shall not be used in Approved mode. See [Help] section "Configure LogRhythm to use Specific User Provided TLS Certificates" for detailed configuration instructions. [Help] section "Common Access Card (CAC) Use" covers operational requirements for user-provided certificates (for example, extended key usage values).

6. In accordance with [SP 800-57 P3] and [SP 800-131A] (key length transition recommendations), the size of TLS public/private keys provided for Log Manager, Windows System Monitor Agents, AI Engine Server, and SQL Servers shall be at least 2048 bits.

7. In accordance with [SP 800-57 P3] (key length transition recommendations), the size of public/private keys for the CA issuing Log Manager, Windows System Monitor Agents, AI Engine Server, and SQL Server certificates shall be at least 2048 bits.

8. The module does not support unidirectional System Monitor Agents in Approved mode.

5.2. Identification and Authentication Policy

The Log Manager cryptographic module does not provide operator authentication. Roles are assumed implicitly. Operating system and SQL Server authentication mechanisms were not within the scope of the validation.

5.3. Access Control Policy and SRDIs

This section specifies the LogRhythm Log Manager's Security Relevant Data Items (SRDI) as well as the access control policy enforced by the LogRhythm.

5.3.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a FIPS-compliant manner, the LogRhythm Log Manager contains the following security relevant data items:

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
Secret and Private Keys						
TLS private key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS session establishment	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance
TLS session encryption keys	AES	128 bits	Used for TLS communication	Generated through TLS handshake	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]

ID	Key type	Size	Description	Origin	Storage	Zeroization Method
TLS session integrity keys	HMAC-SHA1	160 bits	Used for TLS communication	Generated through TLS handshake	Plaintext in volatile memory	As per guidance for bound module [Win BCRYPT]
Public Keys						
TLS public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with AI Engine Server, Windows System Monitor Agents, and SQL Servers	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance
Windows System Monitor Agent public keys	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Windows System Monitor Agents	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
AI Engine Server public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with AI Engine Server	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
CA public key	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with AI Engine Server, Windows System Monitor Agents, and SQL Servers	N/A (entered through Windows operating system)	Volatile memory and the operating system	As per guidance for bound module [Win BCRYPT] and Windows operating system guidance
SQL Server public keys	RSA	2048-bits, 3072-bits, 4096-bits	Used for TLS communication with Log Manager SQL Server and Event Manager SQL Server	N/A (entered through TLS handshake)	Volatile memory	As per guidance for bound module [Win BCRYPT]
Other Keys/CSPs						
Power-up integrity test key	HMAC-SHA1	160 bits	Used to verify integrity of cryptographic module image on power up	Preplaced in module by LogRhythm	Obscured in volatile memory	Re-initialize module

5.3.2. Access Control Policy

The Log Manager allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SRDI while operating the Log Manager in a given role performing a specific Log Manager service. The permissions are categorized as a set of four separate permissions: read, write, execute, delete (r, w, x, and d, respectively, in the table). If no permission is listed, then an operator outside the Log Manager has no access to the SRDI.

LogRhythm Log Manager Server Access Policy [Key: r: read w: write x: execute d: delete]	Security Relevant Data Item	TLS private key	TLS public key	Windows System Monitor Agent public keys	AI Engine Server public key	CA public key	SQL Server public keys	TLS Session encryption keys	TLS Session Integrity seys	Power-up integrity test key
Role/Service										
User Role										
Agent Write Log Data		x	x	w,x,d		x		w,x,d	w,x,d	
Read Agent Configuration		x	x	w,x,d		x		w,x,d	w,x,d	
AI Engine Server Read Log Data		x	x		w,x,d	x		w,x,d	w,x,d	
Event Manager Read Log Data		x	x			x	w,x,d	w,x,d	w,x,d	
Log Manager Read/Write Log Data		x	x			x	w,x,d	w,x,d	w,x,d	
Write Log Manager Configuration		x	x			x	w,x,d	w,x,d	w,x,d	
Seal Archive File		x	x			x	w,x,d	w,x,d	w,x,d	
Crypto-officer Role										
Configure Log Manager Communication		r,w,d	r,w,d			r,w,d				
Perform Self Tests										x
Show FIPS Status										

5.4. Physical Security

This section is not applicable.

6. Crypto Officer Guidance

6.1. Secure Operation Initialization Rules

The LogRhythm software is delivered with the LogRhythm Appliance or standalone as part of the LogRhythm Solution Software (LRSS).

LRSS is the software-only solution for installation and configuration on your own dedicated custom hardware or a supported virtualization platform. Follow the instructions in [Help] section "Installing the Components" to install LogRhythm, including a Log Manager. Once Log Manager is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Log Manager provides the cryptographic functions listed in section Modes of Operation above. The following table identifies the FIPS algorithm certificates for the Approved cryptographic functions along with modes and sizes.

Algorithm Type	Modes/Mod sizes	Cert No.
BCRYPTPRIMITIVES.DLL Algorithms		
AES	CBC, 128 and 256-bit keys	Cert. #1168
HMAC	SHA-1	Cert. #686
SHS	SHA-1/256/384/512	Cert. #1081
DRBG	SP 800-90A CTR_DRBG (AES-256)	Cert. #23
RSA	FIPS186-2: ALG[ANSIX9.31]: Key(gen), MOD: 2048 , 3072 and 4096 bits modulus	Cert. #559
RSA	ALG [RSASSA-PKCS1_V1_5]: SIG(gen) 2048, 3072 and 4096 bits modulus, SHS: SHA-256, SHA-384 and SHA-512 SIG (ver): 1024 , 1536 , 2048 , 3072 and 4096 bits modulus , SHS: SHA-1, SHA-256, SHA-384 and SHA-512	Cert. #567

6.2. Approved Mode

6.2.1. Establishing Approved Mode

Establishing Approved mode entails:

1. Enabling Windows FIPS security policy on the GPC hosting the Log Manager.
2. Providing public key certificate for the Mediator service to support encrypted communication.
3. Enabling encrypted communication between LogRhythm components.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Log Manager. Hence, Windows FIPS security policy should be configured initially for all LogRhythm cryptographic modules in a deployment at the same time. [Help] sections "Running FIPS" and "Enabling FIPS Security Policy" cover the procedures for establishing Windows FIPS security policy across a LogRhythm deployment, including the Log Manager cryptographic module.

[Help] section "Public Key Enabled (PKE)" covers providing public key certificates as well as configuring Log Manager to use the certificate.

Section "When FIPS mode is enabled on a host, all LogRhythm services will connect to SQL Server using Windows Integrated Security regardless of what is configured in their INI files. See [Help] section "Using Integrated Security 6.0" for steps to enable Integrated Security.

TLS Configuration" below describes how to enable encrypted communication

When FIPS mode is enabled on a host, all LogRhythm services will connect to SQL Server using Windows Integrated Security regardless of what is configured in their INI files. See [Help] section "Using Integrated Security 6.0" for steps to enable Integrated Security.

6.2.2. TLS Configuration

The cryptographic module supports protected communication between the Log Manager and other LogRhythm components. Protection is provided by TLS. In particular, the Log Manager module supports TLS between itself and the following external components:

- System Monitor Agents,
- AI Engine Server ,
- Log Manager SQL Server, and
- Event Manager SQL Server.

In Approved mode, TLS communication is required between all components. Enable TLS communication for the Log Manager cryptographic module:

1. Open the Log Manager Local Configuration Manager from where the Log Manager resides by clicking Start > All Programs > LogRhythm > Log Manager Configuration Manager.
2. Select the General tab and check 'Encrypt all communication.'
3. To restart the Log Manager when the Local Configuration Manager exits, select the Windows Service tab and check 'Start (or restart) the service when the configuration is saved.'
4. Click OK to save the settings and exit.

The TLS communication is not enabled and the module is not in Approved mode until the module is restarted.

6.2.3. Starting and Stopping the Cryptographic Module

The Log Manager cryptographic module runs as a Windows service *scmedsvr*. Starting service *scmedsvr* starts the Log Manager cryptographic module. Similarly, stopping service *scmedsvr* stops the cryptographic module. Use the LogRhythm Console, Windows Service Control Manager (SCM), or Windows command line to start or stop the cryptographic module. [Help] section "Starting, Stopping, and Restarting Log Manager Services" describes Console operation. The Windows commands for starting and stopping the module are 'net start' and 'net stop,' respectively.

7. Mitigation of Other Attacks

This section is not applicable.

8. Terminology and Acronyms

Term/Acronym	Description
AIE	Advanced Intelligence Engine
CSP	Critical Security Parameter
EM	Event Manager
GPC	General Purpose Computer
GUI	Graphical User Interface
LM	Log Manager
Mediator Server service	System Monitor Agents collect logs and send them to a Mediator Server service, which processes the logs
SIEM	Security Information Event Management
SRDI	Security Relevant Data Item
TLS [1]	Transport Layer Security

[1] This protocol has not been reviewed or tested by the CAVP and CMVP.

9. References

[FIPS 198-1] *Federal Information Processing Standards Publication: The Keyed-Hash Message Authentication Code (HMAC),* Information Technology Laboratory National Institute of Standards and Technology, July 2008.

[FIPS 140-2] *Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules,* Information Technology Laboratory National Institute of Standards and Technology, 25 May 2001.

[FIPS 140-2 IG] *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, National Institute of Standards and Technology Communications Security Establishment Canada, 11 January 2016.

[Help] LogRhythm Help, Version 6.0.4, March 2012.
LogRhythm Help, Version 6.3.4, February 2015

[SP 800-57 P3] *NIST Special Publication 800-57 Part 3, Revision 1*
Recommendation for Key Management Part 3: Application-Specific Key Management Guidance, National Institute of Standards and Technology, January 2015

[SP 800-131A] *NIST Special Publication 800-131A, Revision 1*
Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, National Institute of Standards and Technology, November 2015

[Win BCRYPT] *Microsoft Windows Server 2008 R2 Cryptographic Primitives Library (bcryptprimitives.dll) Security Policy Document,* Document Version 2.3, 8 June 2011