# FIPS 140-2 Non-proprietary Security Policy

# LogRhythm 6.0.4 or 6.3.4 Console

---

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 Console cryptographic module. It covers the secure operation of the Console 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 Console cryptographic module provides cryptographic services to a Console. In particular, these services support secure communication with SQL Server databases in a LogRhythm deployment.

A Console is a Windows application used to access log data collected and processed by a LogRhythm deployment as well as to configure the deployed components. The Console obtains log data from Log Manager SQL Server. It manages deployed components through the Event Manager SQL Server. Console cryptographic module runs on a general purpose computer (GPC). The Console operating system is Windows Server 2008 R2 SP1. The Console cryptographic module was tested on an x64 processor.

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

- ChartFX.WinForms.Adornments.dll
- ChartFX.WinForms.Annotation.dll
- ChartFX.WinForms.Base.dll
- ChartFX.WinForms.Data.dll
- ChartFX.WinForms.dll
- Infragistics2.Shared.v9.2.dll
- Infragistics2.Win.Misc.v9.2.dll
- Infragistics2.Win.UltraWinDataSource.v9.2.dll
- Infragistics2.Win.UltraWinDock.v9.2.dll
- Infragistics2.Win.UltraWinEditors.v9.2.dll
- Infragistics2.Win.UltraWinGauge.v9.2.dll
- Infragistics2.Win.UltraWinGrid.v9.2.dll
- Infragistics2.Win.UltraWinMaskedEdit.v9.2.dll
- Infragistics2.Win.UltraWinStatusBar.v9.2.dll
- Infragistics2.Win.UltraWinTabControl.v9.2.dll
- Infragistics2.Win.UltraWinToolbars.v9.2.dll
- Infragistics2.Win.v9.2.dll
- lrconsole.exe
- lrconsole.hsh
- lrgeoip.dll
- MindFusion.Common.dll
- MindFusion.Diagramming.dll
- MindFusion.Diagramming.WinForms.dll
- MindFusion.Diagramming.WinForms.Overview.dll
- MindFusion.Graphs.dll

- nsoftware.IPWorks.dll
- nsoftware.IPWorksSSH.dll
- nsoftware.System.dll
- scarcstr.dll
- sccscomn.dll
- sccsuicomn.dll
- scmpeeng.dll
- scrpteng.dll
- scshared.dll
- scuicomn.dll
- scvbcomn.dll
- Xceed.Compression.dll
- Xceed.Compression.Formats.dll
- Xceed.FileSystem.dll
- Xceed.GZip.dll
- Xceed.Tar.dll

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

- EULA.rtf
- LogRhythmHelp.chm
- lrautomdneng.dll
- lrconsole.exe.config
- lrhmcommgr.dll

The excluded directories (along with their subdirectories) are:

- config
- css
- html
- images
- js
- prompting

The Console 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 Console cryptographic module and the Console as a whole. It shows physical and logical cryptographic boundaries of the module.

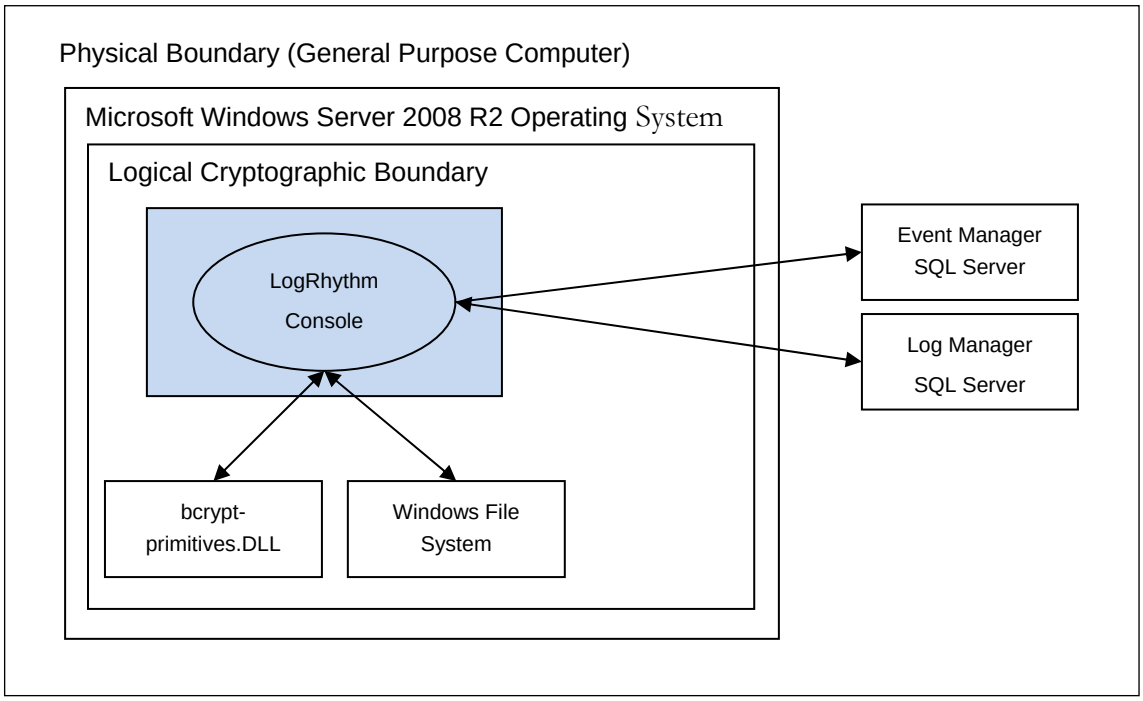


**Figure 1 Cryptographic Module Boundaries**

## 2.1. Ports and Interfaces

The Console cryptographic module ports consist of one or more network interface cards (NIC) on the Console GPC, a keyboard, a mouse, and video output. NICs are RJ45 Ethernet adapters, which are connected to IP network(s).

All data enters the Console application through the NIC, keyboard, and mouse. Data enters physically through the NIC and logically through the GPC's network driver interfaces to the module. All data exits the Console through the NIC and video output. Hence, the NIC, keyboard, mouse, and video 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 Console is made up of log data (such as raw log messages and alarms). The Log Manager SQL Server and Event Manager SQL Server transfer log data (raw log messages and alarms, respectively) to the Console over TLS socket connections. Console can restore log data that Log Manager has archived in the Windows file system. Data output from the Console comprises log data presented to an operator as well as data written to the local file system (for example, reports). Console presents log data to an operator through the

graphical user interface described in [Help]. Console writes reports and state information to files in the local file system. The Console graphical interface also serves as the control interface. At application startup, Console reads preferences and state information from the Windows file system and prompts the operator for session control settings: "Login with Windows account" and "Encrypt all communications." The status output interface comprises the Console "About LogRhythm" dialog box and the Windows Event Log. The Console displays mode and encryption status information in the "About LogRhythm" dialog box. The Console writes status information to the graphical user interface and the Windows Event Log.

## 2.2. Modes of Operation

The Console 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 Console 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 Console 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, Console 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 have read-only access to the configuration of the LogRhythm deployment. They have read-only access to the data LogRhythm collects. The User role corresponds to the LogRhythm Global Analyst and Restricted Analyst user profiles. A Global Analyst can read all data the LogRhythm deployment collects while Restricted Analyst user profiles limit access by Log Source and Log Manager.

2. Crypto Officer Role: Operators with the Crypto Officer role have complete access to the cryptographic module. The Crypto Officer role corresponds to the LogRhythm Global Admin user profile.

# 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. Read/Export Log Data

This service provides an operator with a protected communication channel for reading log data. An operator reads log data from a Log Manager SQL Server with the Console application. The Console displays log data to the operator and can export the data to the Windows file system as a report. The Console cryptographic module provides the cryptographic functions for a TLS connection between the Console and the SQL Server. The connection uses TLS 1.0 with cipher suites 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 LogRhythm Configuration

This service provides an operator with a protected communication channel for reading configuration information for each of the LogRhythm components. The Console connects to the Event Manager SQL Server database using TLS and reads configuration information. The connection uses TLS 1.0 with cipher suites 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. Perform Self-Tests

Console module performs a (start-up) power-on software integrity self 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 Console will not be able to receive input 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.

### 4.1.4. Show FIPS Status

LogRhythm provides status information about the cryptographic module mode of operation through the Console itself. To determine whether the LogRhythm Console is running in FIPS mode, click Console Help menu item About LogRhythm and view the FIPS mode message.

Similarly, LogRhythm provides information about communication encryption through the Console. To determine whether the LogRhythm Console is encrypting Console communication, click Console Help menu item About LogRhythm and view the encryption message. The Console cryptographic module must be encrypting communication in order to be considered operating in Approved mode

The Console cryptographic module may enter an error state and stop (for example, when a self test fails). The Console displays an error dialog box when it stops. To determine the cause of a Console failure, an operator checks the Console error dialog box for error messages to determine the cause of the cryptographic module's error state.

## *4.2. Crypto Officer Services*

### 4.2.1. Read/Export Log Data

An operator in the Crypto Officer role has access to the User role Read/Export Log Data service described above.

### 4.2.2. Read LogRhythm Configuration

An operator in the Crypto Officer role has access to the User role Read LogRhythm Configuration service described above.

### 4.2.3. Perform Self-Tests

An operator in the Crypto Officer role has access to the User role Perform Self-Tests service described above.

### 4.2.4. Show FIPS Status

An operator in the Crypto Officer role has access to the User role Show FIPS Status service described above.

### 4.2.5. Write LogRhythm Configuration

This service provides an operator in the Crypto Officer role with a protected communication channel for writing configuration information for each of the LogRhythm components. The Console connects to the Event Manager SQL Server database using TLS and writes configuration information. The connection uses TLS 1.0 with cipher suites 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).

### 4.2.6. Verify Archive File Seal

An operator in the Crypto Officer role can restore a previously archived log data from a file. Archive files reside on the Log Manager and are restored to a Log Manager SQL Server database. This service provides the capability to validate the integrity of an archive file. Console uses SHA-1 for the cryptographic hash. It recalls the original hash value from the Event Manager SQL database.

# 5. Policies

## 5.1. Security Rules

In order to operate the Console 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 Console 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 Console 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 Console 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 communicating with other LogRhythm components in Approved mode, the Console encrypts communication including:

   - Module to Log Manager SQL Server and

   - Module to Event Manager SQL Server.

5. In accordance with [SP 800-57 P3] and [SP 800-131A] (key length transition recommendations), the size of TLS public/private keys provided for SQL Servers shall be at least 2048 bits.

6. In accordance with [SP 800-57 P3] (key length transition recommendations), the size of public/private keys for the CA issuing SQL Server certificates shall be at least 2048 bits.

## 5.2. Identification and Authentication Policy

The Console 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 Console's Security Relevant Data Items (SRDIs) 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 Console contains the following security relevant data items:

| ID | Key type | Size | Description | Origin | Storage | Zeroization Method |
|---|---|---|---|---|---|---|
| Secret and Private Keys | | | | | | |
| 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] |
| 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 | | | | | | |
| CA public key | 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 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 Console 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 Console in a given role performing a specific Console 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<br><br>[Key:<br>r: read<br>w: write<br>x: execute<br>d: delete] | Security Relevant Data Item | CA public key | SQL Server public keys | TLS session encryption keys | TLS session integrity keys | Power-up integrity test key |
|---|---|---|---|---|---|---|
| Role/Service | | | | | | |
| User Role | | | | | | |
| Read/Export Log Data | | x | w,x,d | w,x,d | w,x,d | |
| Read LogRhythm Configuration | | x | w,x,d | w,x,d | w,x,d | |
| Perform Self Tests | | | | | | x |
| Show FIPS Status | | | | | | |
| Crypto-officer Role | | | | | | |
| Read/Export Log Data | | x | w,x,d | w,x,d | w,x,d | |
| Read LogRhythm Configuration | | x | w,x,d | w,x,d | w,x,d | |
| Perform Self Tests | | | | | | x |
| Show FIPS Status | | | | | | |
| Write LogRhythm Configuration | | x | w,x,d | w,x,d | w,x,d | |
| Verify Archive Seal | | x | w,x,d | w,x,d | w,x,d | |

## *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 Console. Once Console is installed, enable Approve mode as described below. See the LogRhythm Solution Software Installation Guide for more details.

The LogRhythm Console 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<br>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 Console,
2. Using a Windows account to login to Console, and
3. Encrypting all Console communication.

Enabling Windows FIPS security policy affects other LogRhythm components installed on the same GPC as the Console. Hence, Approved mode 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 Approved mode across a LogRhythm deployment, including the Console cryptographic module.

See section "Starting and Stopping the Cryptographic Module" below for instructions for using a Windows account to login to Console and for encrypting all Console communication.

### 6.2.2. Starting and Stopping the Cryptographic Module

The Console is a Windows application. To start the Console:

1. Go to Start > All Programs > LogRhythm > LogRhythm Console.

The LogRhythm log in window is displayed.

2. Select 'Login with Windows account'
3. Select 'Encrypt all communications'
4. Complete other local options as described in [Help] section "Logging in."
5. Click OK.

The Console application starts.

See [Help] section "Open Console" for additional instructions for the first time Console starts.

To stop the Console, select File menu option Exit.

# 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 |
| 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