IBM® Security QRadar® SIEM Cryptographic Module

Software Version 7.4.3

FIPS 140-2, Level 1

Non-Proprietary Security Policy

Documentation Version 1.1

January 13, 2023

IBM Corporation
1 New Orchard Road
Armonk, New York 10504
USA

Table of Contents

Table of Contents

List of Tables

List of Figures

1 Introduction

This document is the Non-Proprietary Security Policy for the IBM QRadar® SIEM Cryptographic Module version 7.4.3 (QRadar). This Security Policy specifies the security rules under which QRadar shall operate to meet the requirements of FIPS 140-2 Level 1. It describes how QRadar functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of QRadar. The module is referred to in this document as the IBM QRadar® SIEM Cryptographic Module version 7.4.3, or QRadar.

This Security Policy describes the features and design of the module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information. The FIPS 140-2 standard and information on the CMVP can be found at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This Security Policy contains only non-proprietary information. This document may be freely reproduced and distributed whole and intact. All other documentation submitted for FIPS 140-2 conformance testing and validation is “IBM - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The IBM QRadar® SIEM Cryptographic Module meets the overall requirements applicable to Level 1 security for FIPS 140-2 as shown in Table 1.

Table 1: Cryptographic Module Security Requirements

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

Table 2 defines acronyms and abbreviations used in this security policy.

Table 2: Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CBC	Cipher-Block Chaining
CFB	Cipher Feedback
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Keyed-Hashing for Message Authentication
KAT	Known Answer Test
LAN	Local Area Network
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OFB	Output Feedback
OS	Operating System
PKCS	Public Key Cryptography Standards
PSS	Probabilistic Signature Scheme
PUB	Publication
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
TLS	Transport Layer Security
WAN	Wide Area Network

2 IBM Security QRadar® SIEM Cryptographic Module

2.1 Overview

IBM QRadar SIEM Cryptographic Module version 7.4.3 family of products provides a security intelligence platform that integrates critical functions including SIEM, log management, configuration monitoring, network behavior anomaly detection, risk management, vulnerability management, network vulnerability scanning, full packet capture and network forensics into a comprehensive intelligence solution. A typical usage for the module is to provide the core cryptographic services necessary to implement the handshaking, establishment and management of TLS secured connections between IBM appliances over WAN and LAN links. Another is to provide for the symmetric encryption of locally stored secrets.

The module provides security functions for encryption, decryption, random number generation, hashing, getting the status of the integrity test, and running the self-tests. The module is used by the application.

2.2 Module Description

The module is classified by FIPS 140-2 as a Level-1 software module, multi-chip standalone module embodiment. The logical cryptographic boundary of the module includes libcrypto.so and libjgsk8iccs_64.so QRadar object module files. The physical cryptographic boundary is the General-Purpose Computer (GPC) on which the module is installed. The module performs no communication other than with the calling application (the process that invokes the module services). Figure 1 below is the module's block diagram.

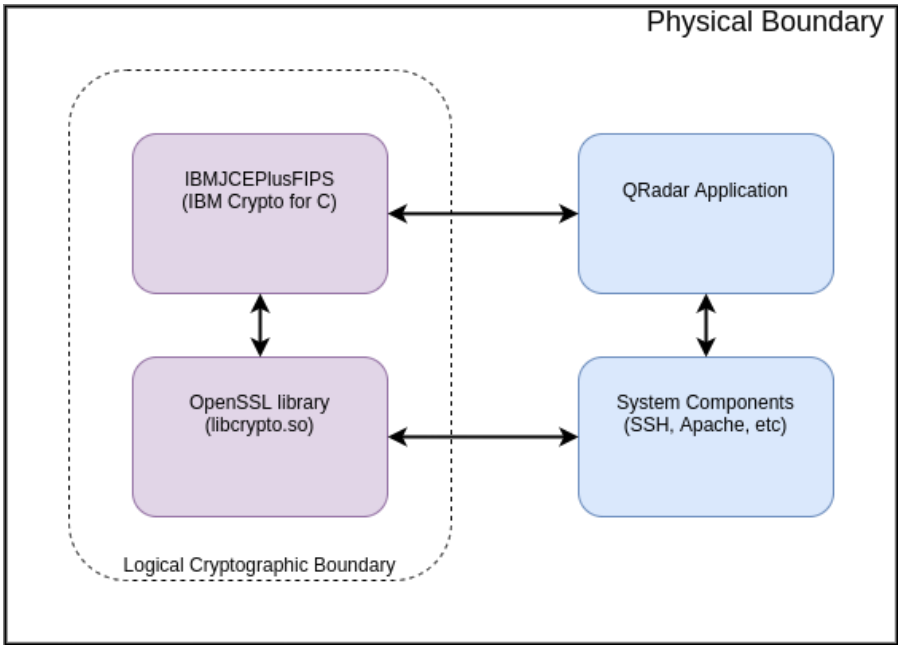

Figure 1 - Module Block Diagram

2.3 Modes of Operation

The module supports the following two modes of operation:

- FIPS mode (the Approved mode of operation): only approved or allowed security functions with sufficient security strength can be used.
- Non-Approved mode (the non-Approved mode of operation): when non-approved security functions are used.

The Module will be in FIPS-approved mode when all power up self-tests have completed successfully and only Approved or Allowed algorithms are invoked. See Tables 3 and 4 below for a list of the supported Approved algorithms and Table 5 for allowed algorithms. The non-Approved mode is entered when a non-Approved algorithm is invoked. See Table 6 for a list of non-Approved algorithms.

2.4 Cryptographic Algorithms

The module implements the FIPS-Approved algorithms listed in the following table and uses these algorithms in FIPS 140-2 Approved mode.

2.4.1 FIPS Approved Algorithms

Table 3: FIPS-Approved Algorithms (IBM QRadar JCE Module)

Algorithm	Certificate Number	Standards	Keys Size
AES (CBC, CTR)	A2425	FIPS 197 SP 800-38A	Keys: 128 and 256 bits
AES-GCM	A2425	SP 800-38D	Keys: 128 and 256 bits
RSA (KeyGen, SigGen, SigVer)	A2425	FIPS 186-4 (PKCS#1 v1.5)	Key Sizes: 2048 bits with SHA-256 and SHA-512
SHS (SHA-1, SHA-256 and SHA-512)	A2425	FIPS 180-4	N/A
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	A2425	FIPS 198-1	Key: 112 bits or larger HMAC Key
ENT (NP)	N/A	SP800-90B	N/A
DRBG	A2425	SP 800-90Arev1	HASH_DRBG (SHA2-256)

KAS-ECC-SSC (Scheme: ephemeralUnified: KAS Role: initiator, responder)	A2425	SP 800-56Arev3	ephemeralUnified; Curves: P-256, P-384, P-521 Key establishment methodology provides between 128 and 256 bits of encryption strength
CKG (Vendor Affirmed) Cryptographic Key Generation. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP 800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.	N/A	SP800-133rev2	N/A

Table 4: FIPS-Approved Algorithm (IBM QRadar OpenSSL Module)

Algorithm	Certificate Number	Standards	Keys Size
AES (CBC, CTR)	A2426	FIPS 197 SP 800-38A	Keys: 128 and 256 bits
AES-GCM	A2426	SP 800-38D	Keys: 128 and 256 bits
RSA PKCS#1 v1.5 (KeyGen, SigGen, SigVer)	A2426	FIPS186-4	Key Sizes: 2048 bits with SHA-256 and SHA-512
SHS (SHA-1, SHA-256 and SHA-512)	A2426	FIPS180-4	N/A
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	A2426	FIPS198-1	Key: 112 bits or larger HMAC Key
ENT (NP)	N/A	SP800-90B	N/A
DRBG	A2426	SP800-90Arev1	CTR_DRBG (AES-256)

KAS-ECC-SSC (Scheme: ephemeralUnified: KAS Role: initiator, responder)	A2426	SP800-56Arev3	Curves: P-256, P-384, P-521 Key establishment methodology provides between 128 and 256 bits of encryption strength
CKG (Vendor Affirmed) Cryptographic Key Generation. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP 800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG.	N/A	SP800-133rev2	N/A

Table 5: FIPS-Approved Algorithm (IBM QRadar Jitterentropy Library used by Entropy Source)

Algorithm	Certificate Number	Standards	Keys Size
SHA-3	A2451	FIPS180-4	SHA3-256

Notes:

1. Not all CAVP tested modes of the algorithms are used in this module.
2. Per the requirements from IG 7.18, SHA-3 (Cert. #2451) implemented by IBM QRadar Jitterentropy Library was validated as a vetted conditioning component (SHA3-256) used by the module's entropy source. No Power-up test was conducted for SHA-3.
3. Per FIPS 198-1 and SP 800-107, keys less than 112 bits in length are not approved for HMAC generation.

2.4.2 Non-Approved Cryptographic Algorithms

The module implements the following services which are Non-Approved per the FIPS 140-2 and SP 800-131Ar1 transition.

Table 6 - Non-FIPS Approved Algorithms

Algorithm	Notes
RSA with keys < 2048 bits	Signing, verification and generation are not approved and not allowed for key sizes < 2048 bits
DSA with key sizes not listed in tables 3 and 4	DSA signing, verification and key gen not allowed except as approved.
DES	Symmetric encryption with DES not permitted
Blowfish	Symmetric encryption with Blowfish not permitted
Camellia	Symmetric encryption with Camellia not permitted
MD4	MD4 digests not permitted
MD5	MD5 digests not permitted
RC4	RC4 symmetric encryption not permitted
RIPEMD	RIPEMD digests not permitted
Whirlpool	Whirlpool digests are not permitted

2.5 Module Interfaces

The module's interfaces are provided by the logical application programming interface (API), which provides the data input, data output, control input, and status output logical interfaces defined by FIPS 140-2. The module is installed on a GPC with physical ports consistent with that of a GPC. All the physical components are standard electronic components; there are not any custom integrated circuits or components dedicated to FIPS 140-2 functionality. Table 7 below demonstrates a mapping between the FIPS logical interfaces and the module's interfaces.

Table 7 - FIPS 140-2 Logical Interface Mappings

Logical Interface	Module Interface Description
Data input	API input parameters
Data output	API output parameters
Control input	API Control/Command parameters input.
Status output	API return codes, API output parameters for status.
Power	N/A

2.6 Roles, Services, and Authentication

The module supports the Crypto Officer (CO) role and User role, which meets all FIPS 140-2 level 1 requirements for Roles and Services. The module does not support a Maintenance role. The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the module. No further authentication is required. The module does not allow concurrent operators.

2.6.1 Crypto Officer Role

The Crypto Officer role has the ability to install the module, to query the module for status information, and to force the module to perform startup self-tests.

Table 8 – Crypto Officer Services

Service	Notes	Algorithm Information	Access	CSPs
Installing the module	Installation tasks include loading the software components onto the system and configuring the module to ensure proper operation.	N/A	N/A	None
Configure QRadar processes	File editing	N/A	N/A	None
Reboot	Restarts a FIPS enabled appliance (terminates all processes zeroizing all keys).	N/A	W	All keys and CSPs
Start, stop, or restart a QRadar service	Changes the status of a service on your QRadar appliance.	N/A	R, X W	None
Perform self-test	Process restart triggers a power-on self-test.	HMAC or RSA signature verification	R	None
Show status	Process output and exit codes	N/A	N/A	None
Shutdown appliance	Power off appliance (and all modules)	N/A	W	All keys and CSPs
Zeroize	Zeroize all CSPs	N/A	Z	All CSPs

2.6.2 User Role

The User role has the ability to perform basic cryptographic operations, typically mediated by the application processes. Descriptions of the services available to the User role are provided in Table 9 below.

Table 9 - User Services

Service	Notes	Algorithm Information	Access	CSPs
Generate random bits	Returns the specified number of random bits to calling application	SP-800-90Arev1	R	CTR_DRBG CSPs

Service	Notes	Algorithm Information	Access	CSPs
Generate Keyed Hash (HMAC)	Compute and return a message authentication code	HMAC	R, X	HMAC key
Symmetric Encrypt/Decrypt	Encrypt/decrypt the data using supplied key	AES-CBC/CTR, AES-GCM	R, X	AES Key, AES GCM Key
Generate RSA Asymmetric Keypair	Generate and return an RSA asymmetric keypair	RSA with approved key size	W	RSA SGK, RSA SVK
ECDH key agreement	Perform KAS-ECC-SSC (SP800-56Ar3) key agreement	ECDH with approved parameters and key size	W	KAS-ECC-SSC Private Key, KAS-ECC-SSC Public Key, KAS-ECC-SSC Shared Secret
RSA Signature Generation	Generate a signature for the supplied message	RSA with approved key size	R, X	RSA SGK
RSA Signature Verification	Verify the signature on the supplied message	RSA with approved key size	R, X	RSA SVK
Zeroize	Zeroize all CSPs	N/A	Z	All CSPs

Please note that the keys and critical security parameters (CSPs) listed in tables 8 and 9 indicate the type of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within a FIPS-Approved or Allowed security function or authentication mechanism.
- Z or Zeroize: The Module zeroizes the CSP.

The complete services supported by the module are available at IBM QRadar SIEM 7.4.3 documentation, Copyright IBM Corp. 2012, 2021.

https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/c_qradar_pdfs.html

2.6.3 Non-FIPS Mode Services

The Module also provides the following non-Approved services available in non-FIPS mode. By selecting non-Approved services listed in Table 10, the Crypto Officer is placing the module into a non-FIPS mode of operation. The Keys/CSPs used in FIPS mode cannot be used in non-approved FIPS mode, and vice versa. Prior to using any of the Non-Approved services in Table 10, the Crypto Officer must zeroize all CSPs used in FIPS mode of operation. Neither the User nor the Crypto Officer are allowed to operate any of these services in Table 10 while in FIPS mode of operation.

Table 10 - Non-FIPS Services

Service	Role	Access
Asymmetric encryption/decryption using non-approved key sizes	User	R, X
Symmetric encryption/decryption using non-approved key sizes	User	R, X
Signature generation (RSA) using non-approved key sizes	User	R, X
Generate keyed hash (HMAC) using non-approved algorithms	User	R, X

2.6.4 Operator Authentication

The module is a software-only cryptographic module. No authentication is required at security level 1, and the authentication is implicit by assumption of the role.

2.7 Physical Security

The module is a software entity only and thus does not claim any physical security.

2.8 Operational Environment

This module operates in a modifiable operational environment per the FIPS 140-2 definition. The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded). The external application that makes calls to the cryptographic module is the single user of the module, even when the application is serving multiple clients. All cryptographic keys and CSPs are under the control of the OS or calling applications, which is responsible for protection of the CSPs against unauthorized disclosure, modification, and substitution.

The module has been tested on the following platforms.

Table 11 - Tested Platforms

#	Operating System	Processor	Platform
1	Red Hat Enterprise Linux (RHEL) 7	Intel Xeon Gold 5118 with PAA	Dell PowerEdge R740XD
2	Red Hat Enterprise Linux (RHEL) 7	Intel Xeon Gold 5118 without PAA	Dell PowerEdge R740XD

2.9 Cryptographic Key Management

The module supports the critical security parameters (CSPs) listed Tables 8 and 9 and cryptographic keys listed in Table 12.

All CSPs used by the module are described in this section. The CSP names are generic, corresponding to the API parameter data structure.

Table 12 - CSPs

#	CSP/Key Name	Description	Generated/Input	Output
1	AES Key	AES-CBC/CTR (128/256 bits) key for data encryption and decryption	Input via API in plaintext	N/A
2	AES GCM Key	AES (128/256 bits) key for authenticated encryption and decryption	Input via API in plaintext	N/A
3	HMAC Key	Keyed hash key (160/256/512 bits)	Input via API in plaintext	N/A
4	CTR_DRBG CSPs	V (128 bits), Seed (256/320/384 bits) and Key (AES 128/256 bits), Entropy input (384 bits from entropy source)	Internally generated per SP800-90Arev1	N/A
5	RSA SGK	RSA (2048 bits) signature generation key.	Internally generated or input via API in plaintext	N/A
7	KAS-ECC-SSC Private Key	KAS-ECC-SSC (ECDH) Private Key with Curves: P-256, P-384 and P-521	Internally generated per SP800-56Arev3	N/A
8	KAS-ECC-SSC Shared Secret	KAS-ECC-SSC (ECDH) Shared Secret with Curves: P-256, P-384 and P-521	Internally derived per SP800-56Arev3	N/A

Below is the table listing all public keys used within the module.

Table 13. Public Keys

#	CSP Name	Description
1	RSA SVK	RSA (2048 bits) signature verification public key
2	KAS-ECC-SSC Public Key	KAS-ECC-SSC (ECDH) Public Key with Curves: P-256, P-384 and P-521

2.9.1 Key/CSP Storage, Generation, Entry, Output and Zeroization

Storage: RAM, associated to entities by memory location. The module stores DRBG state values for the lifetime of the DRBG instance. The module uses CSPs passed in by the calling application on the stack or registers. The module does not store any CSP

persistently (beyond the lifetime of an API call), with the exception of DRBG state values used for the module's default key generation service.

Generation: In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP800-133rev2. The resulting generated seed used in the asymmetric key generation is the unmodified output from SP800-90Arev1 DRBG. The calling application is responsible for storage of generated keys returned by the Module.

The module is a software module that contains an approved DRBG that is seeded exclusively from a known entropy source (0.829800 bits/sample bit) located within the operational environment inside the module's physical boundary but outside the logical boundary, which is compliant with FIPS 140-2 IG 7.14 #1 (b). The minimum number of bits of entropy requested per each GET function call is at least 256 bits.

Entry: All CSPs enter the Module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

Output: The Module does not output CSPs, other than as explicit results of key generation services. However, none cross the physical boundary.

Destruction: Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. In addition, the module provides functions to explicitly destroy CSPs related to random number generation services. The calling application is responsible for parameters passed in and out of the module.

Private and secret keys as well as seeds are provided to the module by the calling application and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the module defined API. The operating system protects memory and process space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An authorized application as the Crypto Officer role or User role has access to all key data generated during the operation of the module.

2.9.2 Use of AES-GCM

In approved mode, users of the module must not utilize GCM with an externally generated IV unless the source of the IV is also FIPS approved for GCM IV generation. The module's implementation of AES-GCM is used together with an application that executes outside of the module's cryptographic boundary. The application negotiates the protocol session's keys and the value of the IV.

The Module also supports internal IV generation using the module's Approved DRBG. The IV is at least 96-bits in length per NIST SP 800-38D, Section 8.2.2. Per FIPS 140-2 IG A.5 Scenario 2 and NIST SP 800-38D, the approved DRBG generates outputs such that the (key, IV) pair

collision probability is less than 2^{-32}. Per IG A.5, in the event module power is lost and restored the consuming application must ensure that any of its AES-GCM keys used for encryption or decryption are re-distributed.

The Module also supports importing of GCM IVs when an IV is not generated within the Module. In the FIPS approved mode, an IV must not be imported for encryption from outside the cryptographic boundary of the Module as this will result in a non-conformance.

2.10 EMI/EMC

The Cryptographic Security Kernel is a software module. Therefore, the only electromagnetic interference produced is that of the host platform on which the module resides and executes. FIPS 140-2 requires that the host systems on which FIPS 140-2 testing is performed meet the Federal Communications Commission (FCC) EMI and EMC requirements for business use as defined in Subpart B, Class A of FCC 47 Code of Federal Regulations Part 15. However, all systems sold in the United States must meet these applicable FCC requirements.

2.11 Self-Tests

This section describes the power-up and conditional self-tests performed by the module. If any of the tests listed below fails to complete successfully, the module enters into a critical error state where all cryptographic operations and output of any data is prohibited. An error message is logged for the CO to review and requires action on the CO's part to clear the error state.

2.11.1 Power-Up Self-Tests

At start-up, Known Answer Tests (KATs) and software integrity check are performed. These tests are automatic and do not need operator intervention. If the value calculated and the known answer do not match, the module immediately enters into an error state. Once the module is in the error state, it becomes unusable via any interface.

The module implements the following Power-On Self-Tests (POSTs):

- Software Integrity Checks:
  - HMAC-SHA-256 (IBM QRadar OpenSSL Module)
  - RSA 2048 with SHA-256 (IBM QRadar JCE Module)
- IBM QRadar OpenSSL Module Known Answer Tests (KATs):
  - AES-CBC Encrypt/Decrypt KATs
  - AES-GCM Encrypt/Decrypt KATs
  - DRBG KAT (Note: CTR_DRBG health tests as specified in SP800-90Arev1 Section 11.3 are performed)
  - HMAC KATs (HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512)
  - KAS-ECC-SSC primitive Z KAT
  - RSA KATs (separate KAT for signing; separate KAT for verification)

- IBM QRadar JCE Module Known Answer Tests (KATs):
  - AES-CBC Encrypt/Decrypt KATs
  - AES-GCM Encrypt/Decrypt KATs
  - DRBG KAT (Note: HASH_DRBG health tests as specified in SP800-90Arev1 Section 11.3 are performed)
  - HMAC KATs (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)
  - KAS-ECC-SSC primitive Z KAT
  - RSA KATs (separate KAT for signing; separate KAT for verification)

Each module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by power-cycling the host platform.

2.11.2 Conditional Self-Tests

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

- IBM QRadar OpenSSL Module:
  - RSA PWCT (RSA Sign/Verify)
- IBM QRadar JCE Module:
  - RSA PWCT (RSA Sign/Verify)

In addition, the module's entropy source also conducted following Self-Tests:

1. ENT (NP) SP800-90B Start-Up Health Tests:
   - Repetition Count Test (RCT)
   - Adaptive Proportion Test (APT)

Note: Please refer to SP800-90B, sections 4.4.1 and 4.4.2 for more information about the RCT and APT.

2. ENT (NP) SP800-90B Continuous Health Tests:
   - Repetition Count Test (RCT)
   - Adaptive Proportion Test (APT)

2.12 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

2.13 Secure Operation

The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

The Crypto Officer role is responsible for installing the module as part of its host application. During the power-up self-tests phase, the signatures are verified over the stored module instances. If the stored signatures are verified, then the test is passed. Otherwise, the test is failed and the module enters an error state where no cryptographic functionality is allowed.

2.13.1 Initial Setup

To install a module in a FIPS-approved mode of operation, the following steps must be completed:

1. Add the following to the end of the vmlinuz line at the boot menu during installation of Red Hat Enterprise Linux 7.7:
    a. qradar.fips=1
2. Continue with the installation of the module as per the installation documentation.

If there are circumstances where Red Hat Enterprise Linux must be installed in FIPS mode separately, this can be accomplished with the following steps:

1. Create a bootable USB flash drive with Red Hat Enterprise Linux 7.7 or otherwise map the ISO using the Integrated Management Module (IMM) or the Integrated Dell Remote Access Controller (iDRAC).
2. Restart the appliance and boot into the bootable USB or ISO install. At the boot menu, add the following to the end of the vmlinuz line:
    a. fips=1
3. Continue with the installation of Red Hat Enterprise Linux 7.7.
4. Once installation is complete, copy the QRadar ISO to either /root or /storetmp.
5. Create a /media/cdrom directory and mount the ISO to the newly created directory.
6. Start the QRadar setup using the following command:
    a. /media/cdrom/setup –fips
    b. When the Red Hat Enterprise Linux and QRadar systems are installed separately, the QRadar setup command used during installation will first verify that the operating system is FIPS enabled before it can proceed with the installation. If FIPS is not enabled, an error message will be reported and the QRadar setup will fail.
7. Continue with the QRadar setup.
8. Once the setup is complete. Ensure that the HTTPd server does not enable any non-approved algorithms. In /etc/httpd/conf.d/ssl.conf the SSLCipherSuite line should contain only:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384

9. Ensure that Java processes cannot enable cipher suites with non-approved algorithms. In /usr/java/j2sdk/jre/lib/security/java.security find the jdk.tls.disabledAlgorithms line and make sure ECDH are included.

2.13.2 Use of AES-GCM

In approved mode, users of the module must not utilize GCM with an externally generated IV unless the source of the IV is also FIPS approved for GCM IV generation.

The module's implementation of AES-GCM is used together with an application that executes outside of the module's logical cryptographic boundary. The application negotiates the protocol session's keys and the value of the IV. The IV generation method will conform to the requirements specified in Provision 1 of IG A.5.

Per IG A.5, in the event module power is lost and restored, the consuming application must ensure that any of its AES-GCM keys used for encryption or decryption are re-distributed.

2.13.3 Secure Management

The Crypto Officer shall monitor the module's status regularly and make sure only the services listed in Tables 8 and 9 are being used. If any irregular activity is noticed or the module is consistently reporting errors, then IBM customer support should be contacted.

2.13.4 Permitted Applications

The Crypto Officer must monitor the system and ensure that only software packages provided by IBM, expressly for use with QRadar are installed on the system. The installation of software packages from any other source implicitly places the system in non-FIPS mode.

3 References

The IBM website www.ibm.com contains information on the full line of solutions from IBM.

The following National Institute of Standards and Technology publications are available at URL csrc.nist.gov/groups/STM/cmvp/index.html:

- *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*
- *FIPS 140-2 Annex A: Approved Security Functions*
- *FIPS 140-2 Annex B: Approved Protection Profiles*
- *FIPS 140-2 Annex C: Approved Random Number Generators*
- *FIPS 140-2 Annex D: Approved Key Establishment Techniques*
- *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* (a joint publication of the National Institute of Standards and Technology and Communications Security Establishment)
- *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197

- *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-3