SECURE IT

FedRAMP Insights

FIPS 140-2 Validation

Greg Kent
Vice President, SecureIT

TECH BULLETIN

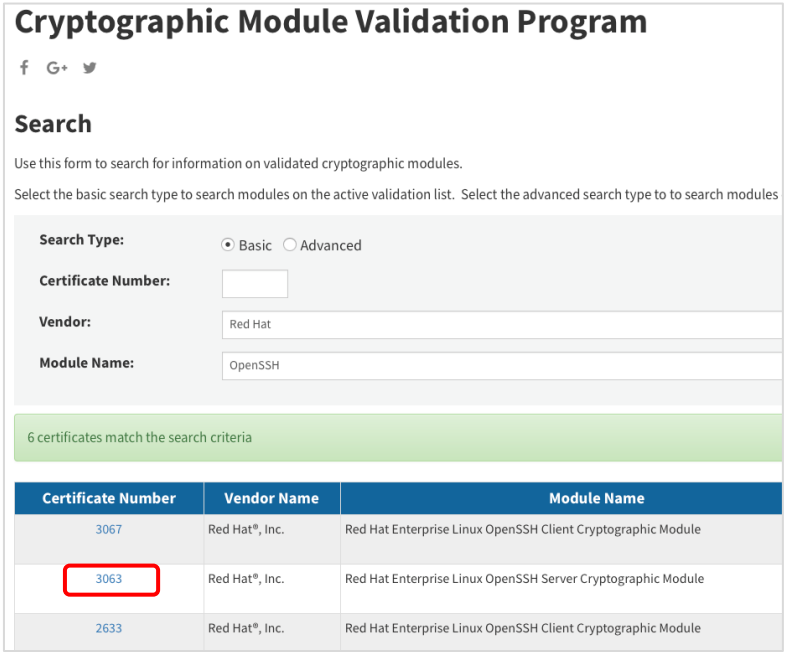
Introduction

Cloud services must use FIPS 140-2 validated encryption modules that have been independently validated and certified by a NIST-specified accredited laboratory in order to obtain FedRAMP authorization. FedRAMP requires that the System Security Plan (SSP) documentation include the FIPS 140-2 certification/validation numbers and dates for all relevant products. Demonstrating ongoing compliance with FIPS 140-2 validated encryption is essential to maintaining FedRAMP authorization, following initial assessment approval.

Below are three examples of how you can confirm FIPS 140-2 validation and demonstrate compliance with Federal requirements to your auditor by leveraging the Security Policy and providing evidence that requirements have been implemented properly. The evidence required for each example illustrates that there is no “one size fits all” list of items that can be provided as evidence. All of the examples are based on a common approach–leveraging the FIPS 140-2 validation certificate and the associated Security Policy to determine the particular items (e.g., versions of modules or RPMs, configuration settings, etc.) that are required to show that the encryption module that is implemented within your cloud service corresponds to the encryption module that NIST validated.

Example 1: RHEL 7.4 OpenSSH

1. Visit the NIST CMVP website to search for RHEL. Review the search results and details for the various RHEL certificates to determine which module applies to the OpenSSH server for RHEL 7.4. Select Certificate #3063 and note that the certificate indicates RHEL version 7.4.



Cryptographic Module Validation Program

Search

Use this form to search for information on validated cryptographic modules.

Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules

Search Type: (•) Basic ( ) Advanced

Certificate Number:

Vendor: Red Hat

Module Name: OpenSSH

6 certificates match the search criteria

Certificate Number	Vendor Name	Module Name
3067	Red Hat®, Inc.	Red Hat Enterprise Linux OpenSSH Client Cryptographic Module
3063	Red Hat®, Inc.	Red Hat Enterprise Linux OpenSSH Server Cryptographic Module
2633	Red Hat®, Inc.	Red Hat Enterprise Linux OpenSSH Client Cryptographic Module

2. Also note the “Caveat” that the module must be operated in FIPS mode.

Cryptographic Module Validation Program

Certificate #3063

Details

Module Name	Red Hat Enterprise Linux OpenSSH Server Cryptographic Module
Standard	FIPS 140-2
Status	Active
Sunset Date	11/13/2022
Validation Dates	11/14/2017 6/15/2018
Overall Level	1
Caveat	When operated in FIPS Mode with module Red Hat Enterprise Linux OpenSSL Module validated to FIPS 140-2 under Cert. #3016 operating in FIPS mode
Security Level Exceptions	• Physical Security: N/A • Mitigation of Other Attacks: N/A
Module Type	Software
Embodiment	Multi-Chip Stand Alone
Description	The OpenSSH Server cryptographic module provides the server-side component for an SSH protocol version 2 protected communication channel. OpenSSH is the standard SSH implementation and shipped with RHEL 7. Its cryptographic mechanisms use the OpenSSL library in FIPS 140-2 mode.
Tested Configuration(s)	• Red Hat Enterprise Linux 7.4 running on Dell PowerEdge R630 with PAA [1] • Red Hat Enterprise Linux 7.4 running on Dell PowerEdge R630 without PAA [1] • Red Hat Enterprise Linux 7.5 running on Dell PowerEdge R630 with PAA [2] • Red Hat Enterprise Linux 7.5 running on Dell PowerEdge R630 without PAA [2] (single-user mode)
FIPS Algorithms	AES Certs. #4644, #4664, #4666, #4667, #4695, #4696, #4697, #4698, #4699, #4700, #5203, #5204, #5205, #5207, #5208, #5209, #5210, #5211, #5212 and #5227 CVL Certs. #1298, #1312, #1318, #1320, #1361, #1687, #1689, #1693, #1700 and #1718 DRBG Certs. #1567, #1576, #1578, #1579, #1593, #1594, #1595, #1596, #1597, #1598, #1975, #1976, #1977, #1979, #1980, #1981, #1982, #1983, #1984 and #1993 ECDSA Certs. #1144, #1148, #1150, #1151, #1347, #1348, #1350 and #1353 HMAC Certs. #3076, #3088, #3090, #3091, #3107, #3108, #3109, #3110, #3111, #3112, #3445, #3446, #3447, #3449, #3450, #3451, #3452, #3453, #3454 and #3459 RSA Certs. #2535, #2544, #2546, #2547, #2786, #2787, #2789 and #2792 SHS Certs. #3807, #3821, #3823, #3824, #3842, #3843, #3844, #3845, #3846, #3847, #4193, #4194, #4195, #4197, #4198, #4199, #4200, #4201, #4202 and #4207 Triple-DES Certs. #2471, #2481, #2483, #2484, #2638, #2639, #2641 and #2642
Allowed Algorithms	Diffie-Hellman (CVL Certs. #1298, #1312, #1318, #1320, #1687, #1689, #1693 and #1700 with CVL Certs. #1361 and #1718, key agreement; key establishment methodology provides 112 or 128 bits of encryption strength); EC Diffie-Hellman (CVL Certs. #1298, #1312, #1318, #1320, #1687, #1689, #1693 and #1700 with CVL Certs. #1361 and #1718, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength); NDRNG
Software Versions	5.0 [1] , 6.0 [2]
Product URL	http://redhat.com/en/technologies/linux-platforms/enterprise-linux

3. Scroll down and open the Security Policy.

4. Review the Security Policy for OpenSSH. Note that Section 2 indicates the required software (including versions) that need to be installed for the module to operate. This includes modules that were validated for OpenSSL (certificate #3016).

The module will use the Red Hat Enterprise Linux OpenSSL Module (FIPS 140-2 Certificate #3016) as a bound module which provides the underlying cryptographic algorithms necessary for establishing and maintaining the SSH session. In addition the integrity check uses the cryptographic services provided by the Red Hat Enterprise Linux OpenSSL Module as used by the utility application of fipscheck using the HMAC-SHA-256 algorithm.

This requires a copy of a Cert. #3016 validated version of the Red Hat Enterprise Linux OpenSSL Module to be installed on the system for the current module to operate.

The cryptographic module combines a vertical stack of Linux components intended to limit the external interface each separate component may provide. The following software need to be installed for the module to operate:

- Red Hat Enterprise Linux OpenSSH Server Cryptographic Module with the version of the OpenSSH server RPM file 7.4p1-11.el7 [1] and 7.4p1-16.el7 [2]
- The bound module of OpenSSL with FIPS 140-2 Certificate #3016
- The contents of the fipscheck RPM package (version 1.4.1-6.el7)
- The contents of the fipscheck-lib RPM package (version 1.4.1-6.el7).

In addition, note that section 10.1 of the Security Policy indicates that a “fips_enabled” setting should be configured and that section 10.1.1 places restrictions on the ciphers and hmacs that can be enabled within fips mode.

The next step is to check the presence of the configuration file /proc/sys/crypto/fips_enabled and make sure it contains value 1.

10.1.1 OpenSSH Configuration

The user must not use DSA keys for performing key-based authentication as OpenSSH only allows DSA keys with 1024 bit size which are disallowed as per SP800-131A.

The user must not accept DSA host keys potentially offered during the first contact of an SSH server as OpenSSH only allows DSA keys with 1024 bit size which are disallowed as per SP800- 131A.

When re-generating RSA host keys, the crypto officer should generate RSA keys with a size of 2048 bit or higher according to [SP800-131A]. The crypto officer should inform the user base to not use RSA keys with key sizes smaller than 2048 bits.

In FIPS 140-2 mode, the following restrictions are applicable. When these restrictions are violated by configuration options or command line options, the module will not be in the FIPS mode of operation:

- SSH protocol version 1 is not allowed
- GSSAPI is not allowed
- Only the following ciphers are allowed:
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - aes128-cbc
  - aes192-cbc
  - aes256-cbc
  - 3des-cbc
  - rijndael-cbc@lysator.liu.se

Only the following message authentication codes are allowed:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com

Any use of other ciphers or algorithms will results in the module entering the non-FIPS mode of operation.

5. Review the Security Policy for the referenced OpenSSL certificate #3016. Notice that the section 1.3 lists the module's RPM version.

The Red Hat Enterprise Linux OpenSSL Cryptographic Module v6.0 logical cryptographic boundary is the shared library files and their integrity check HMAC files, which are delivered through Red Hat Package Manager (RPM) as listed below.

The openssl-libs-1.0.2k-12.el7.x86_64.rpm (64 bits) and openssl-libs-1.0.2k-12.el7.i686.rpm (32 bits) file contains the following files that are part of the module boundary:

- /usr/lib{64,}/.libcrypto.so.1.0.2k.hmac
- /usr/lib{64,}/.libssl.so.1.0.2k.hmac
- /usr/lib{64,}/libcrypto.so.1.0.2k
- /usr/lib{64,}/libssl.so.1.0.2k

Also note that section 9.1 of the Security Policy, similar to the Security Policy for OpenSSH, identifies a required configuration for the “fips_enabled” setting.

> The next step is to check the presence of the configuration file /proc/sys/crypto/fips_enabled and make sure it contains value 1.

6. To demonstrate the Red Hat OpenSSH (and the associated OpenSSL module) is FIPS 140-2 validated, provide your auditor the following artifacts:

   A) FIPS 140-2 Certificate #3063
   B) The associated Security Policy PDF file for certificate #3063
   C) FIPS 140-2 Certificate #3016 (for the OpenSSL module)
   D) The associated Security Policy PDF file for certificate #3016 (for the OpenSSL module)
   E) Evidence that the installed OpenSSH and OpenSSL modules correspond to the versions listed in the respective Security Policy documents

```
[root@ip  ]# rpm --last -q -a | grep fips
dracut-fips-033-502.el7.x86_64                Tue 02 Jan 2018 02:26:55 PM UTC
fipscheck-lib-1.4.1-6.el7.x86_64              Tue 02 Jan 2018 02:25:19 PM UTC
fipscheck-1.4.1-6.el7.x86_64                  Tue 02 Jan 2018 02:25:19 PM UTC
[root@i  ]# rpm --last -q -a | grep ssh
openssh-server-7.4p1-16.el7.x86_64            Tue 01 May 2018 01:18:25 PM UTC
openssh-clients-7.4p1-16.el7.x86_64           Tue 01 May 2018 01:18:24 PM UTC
openssh-7.4p1-16.el7.x86_64                   Tue 01 May 2018 01:18:03 PM UTC
sshpass-1.06-2.el7.x86_64                     Tue 02 Jan 2018 02:17:58 PM UTC
libssh2-1.4.3-10.el7_2.1.x86_64               Thu 13 Jul 2017 05:26:02 PM UTC
[root@  ]# rpm --last -q -a | grep openssl
openssl-1.0.2k-12.el7.x86_64                  Tue 01 May 2018 01:18:25 PM UTC
openssl-devel-1.0.2k-12.el7.x86_64            Tue 01 May 2018 01:18:24 PM UTC
openssl-libs-1.0.2k-12.el7.x86_64             Tue 01 May 2018 01:18:02 PM UTC
```

   F) Evidence that the fips_enabled setting is configured properly.

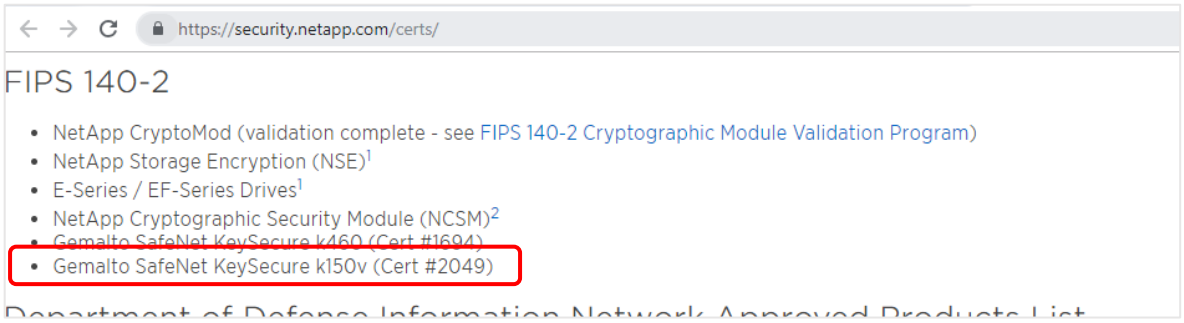
```
[root@  ]#cat /proc/sys/crypto/fips_enabled
1
```

G) Evidence that sshd_config does not enable prohibited ciphers or algorithms.

```
root@[redacted]# cat /etc/ssh/sshd_config | grep ^# -v | grep ^$ -v
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile .ssh/authorized_keys
HostbasedAuthentication no
IgnoreRhosts yes
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication no
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
UsePrivilegeSeparation yes
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY
LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem sftp          /usr/libexec/openssh/sftp-server
UseDNS no
PermitRootLogin no
Protocol 2
KerberosAuthentication no
StrictModes yes
Compression no
PrintLastLog yes
ClientAliveInterval 600
ClientAliveCountMax 0
IgnoreUserKnownHosts yes
RhostsRSAAuthentication no
PermitEmptyPasswords no
Banner /etc/issue
PermitUserEnvironment no
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha2-256,hmac-sha2-512
```

Example 2: Gemalto SafeNet KeySecure k150v

1. Visit the vendor website to learn which FIPS 140-2 certificate is associated with the product: https://security.netapp.com/certs/



Note that KeySecure k150v is validated under Certificate #2049.

2. Visit the NIST CMVP website to view Certificate #2049 for any “Caveat” that is noted. The “Caveat” indicates that the module must be operated in FIPS mode.

Cryptographic Module Validation Program

Certificate #2049

Details

Module Name	SafeNet Software Cryptographic Library
Standard	FIPS 140-2
Status	Active
Sunset Date	1/9/2022
Validation Dates	11/27/2013 12/15/2015 1/10/2017
Overall Level	1
Caveat	When operated in FIPS mode and when installed, initialized and configured as specified in Section 4 of the provided Security Policy. The module generates cryptographic keys whose strengths are modified by available entropy; No assurance of the minimum strength of generated keys.
Security Level Exceptions	• Design Assurance: Level 3
Module Type	Software
Embodiment	Multi-chip standalone
Description	The SafeNet Software Cryptographic Library is SafeNet's cryptographic service provider that provides extended high performance cryptographic services for SafeNet's broad range of Data Protection products.
Tested Configuration(s)	• Android 4.0 running on Beagleboard xM with PAA • CentOS 5.6 32-bit running on a Dell PowerEdge 860 (Single User Mode) • NetBSD 4.0 32-bit on Vmware ESX running on Dell PowerEdge R210II with PAA • RHEL 6.2 64-bit running on a Dell PowerEdge R210II with PAA • Windows 7 32-bit running on a Acer Aspire AS5750 • Windows 7 64-bit running on a Acer Aspire AS5750 with PAA • Windows Server 2008 64-bit running on Dell PowerEdge R210II • Windows Server 2008R2 64-bit running on Dell PowerEdge R210II with PAA
FIPS Algorithms	AES — Cert. #2286 CVL — Cert. #45 DRBG — Cert. #283 DSA — Cert. #714 ECDSA — Cert. #370 HMAC — Cert. #1402 RSA — Cert. #1176 SHS — Cert. #1967 Triple-DES — Cert. #1434
Other Algorithms	RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength); EC Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength); RNG (non-compliant); DRBG (non-compliant)
Software Versions	1.0

3. Scroll down and open the Security Policy.

4. Read the Security Policy to confirm the KeySecure k150v is configured in accordance with the Security Policy. Note that Section 4 indicates that the module supports only FIPS 140-2 approved mode, and requires that the FIPS_mode_set parameter be true.

> **4 Modes of Operation and Cryptographic Functionality**
>
> The Module supports only a FIPS 140-2 Approved mode. These algorithms shall not be used when operating in the FIPS Approved mode of operation.
>
> The Module requires an initialization sequence (see IG 9.5): the calling application invokes FIPS_mode_set()[3], which returns a "1" for success and "0" for failure. If FIPS_mode_set() fails then all cryptographic services fail from then on. The application can test to see if FIPS mode has been

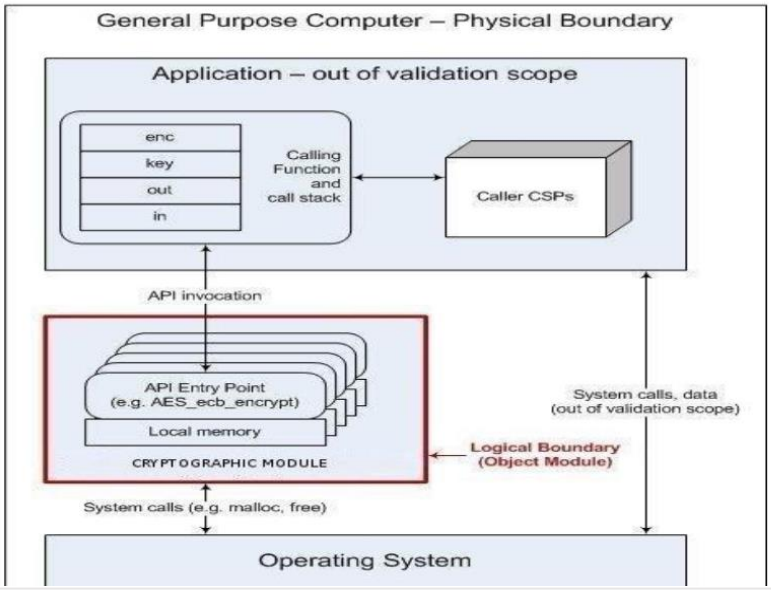
Section 8.2 describes how the cryptographic library is embedded within KeySecure and is not configurable.

> ***8.2 Delivery and Operation***
>
> The SafeNet Software Cryptographic Library is never released outside of SafeNet as a source code distribution. It is contained within our source code management repository that can be accessed by engineering to download a copy of the code. It is not possible to make changes to the code and replace it within this repository. When a developer downloads code for integration into a SafeNet product, the code gets integrated into the configuration management structure for that product. The module code is then linked as part of an application build process that is configured to operate in FIPS Approved Mode.

Based on this security policy, no specific configuration is required in order to enable FIPS mode within the module itself, as it is automatically enabled. FIPS mode would need to be enabled in the application that calls the validation. However, section 1 of the Security Policy (as shown below) indicates that the application is out of scope, as the FIPS validation focused strictly on the module itself.

1 Introduction

This document comprises the non-proprietary FIPS 140-2 Security Policy for the SafeNet Software Cryptographic Library v1.0, hereafter referred to as the Module.



Based on review of the Security Policy, it is necessary to look beyond the module itself and consult the application's system documentation to determine if the application properly enables FIPS mode when calling the module.

5. Review the product's configuration guide to determine how the device must be configured to comply with FIPS 140-2 by invoking the validated module. Note that Section 31 of the *SafeNet KeySecure Appliance Administrator Guide* describes how the appliance must be configured to operate in accordance with FIPS 140-2.

31

High Security Features

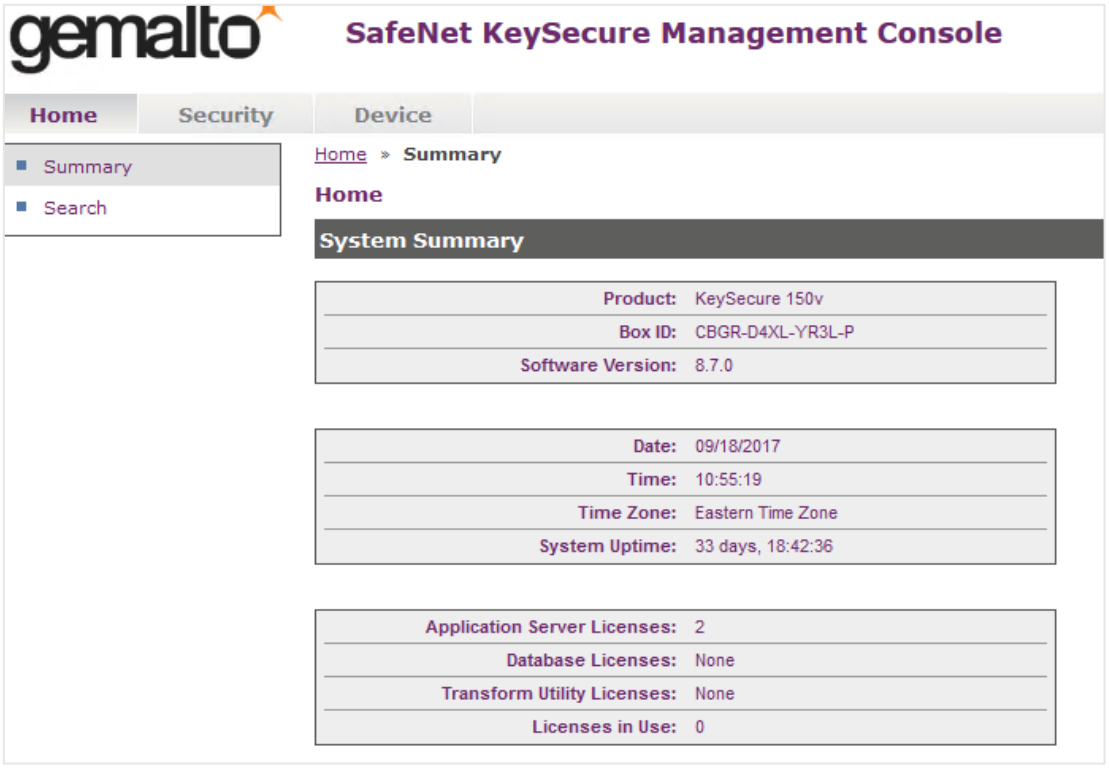
Use the High Security settings on the SafeNet KeySecure to set the highest level of security for administrative and cryptographic operations on the device. Depending on the SafeNet KeySecure in use, the advanced security settings may be configurable to comply with the Federal Information Processing Standard (FIPS) 140-2 for key generation. Some SafeNet KeySecure platforms include a K-6 Luna PCI-E HSM card which has also been evaluated to FIPS 140-2 Level 3. If you use a non-FIPS compliant SafeNet KeySecure, you can still use high security settings.

The following models are capable of operating in accordance with FIPS 140-2, Level 1:

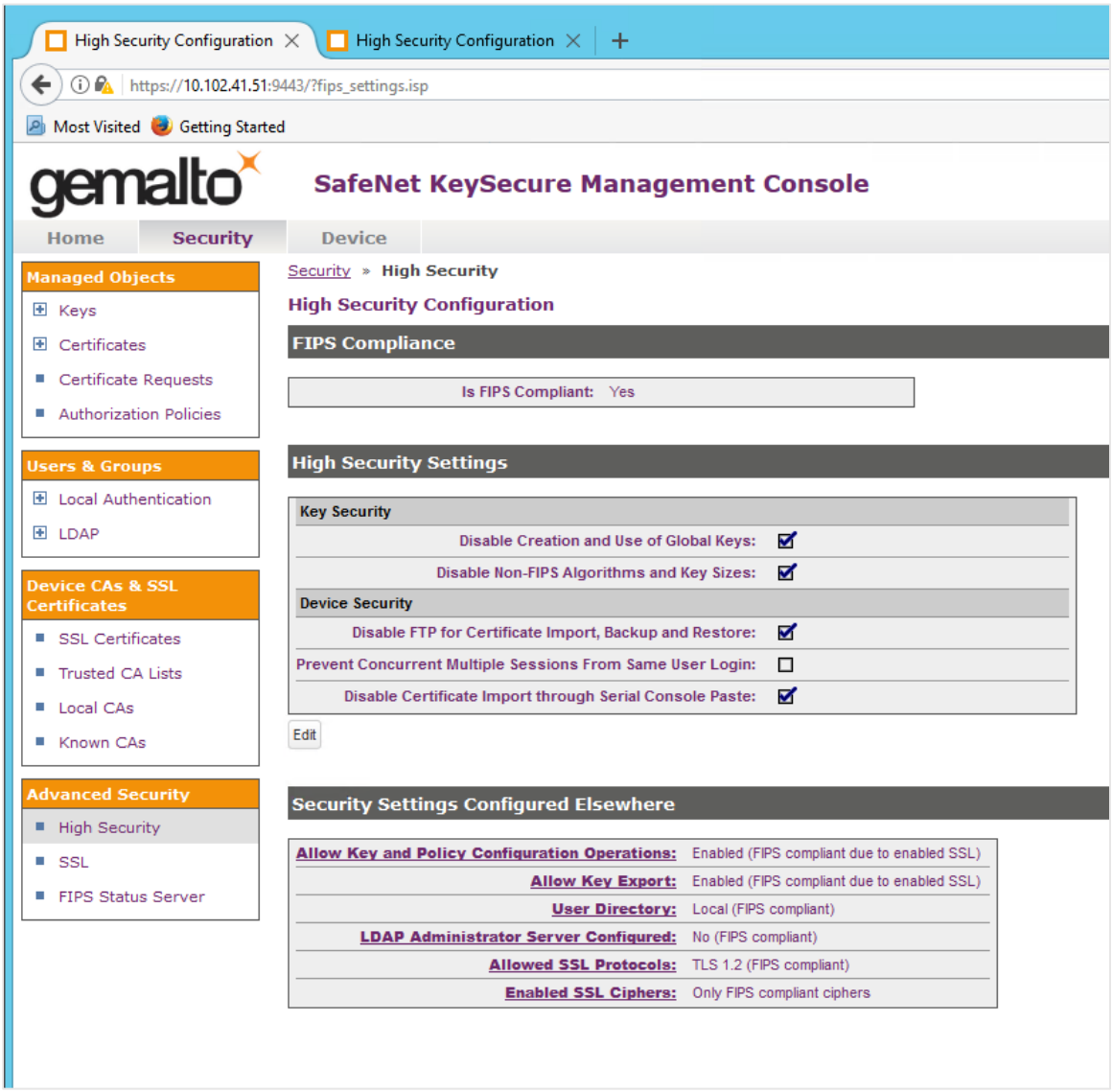
- SafeNet KeySecure 450 (R330)
- SafeNet KeySecure 450 (R320)
- SafeNet KeySecure 450 (R610)
- SafeNet KeySecure 150
- SafeNet KeySecure 250
- Virtual SafeNet KeySecure 150v
- Virtual SafeNet KeySecure 450v

6. To demonstrate the KeySecure k150v is FIPS 140-2 validated, provide your auditor the following artifacts:

   A) FIPS 140-2 Certificate #2049
   B) The relevant Security Policy pdf file for certificate #2049
   C) The relevant sections of the application Administrator Guide
   D) Evidence that the k150v is deployed

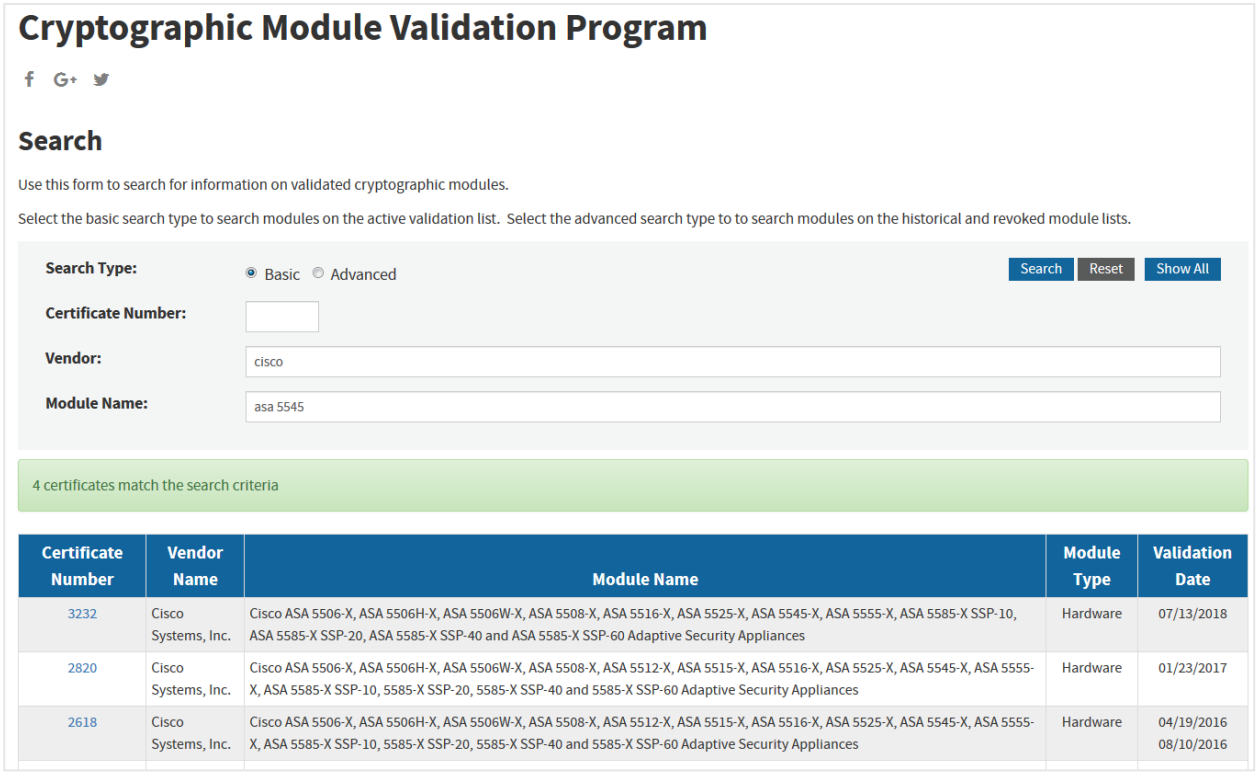


E) Evidence of the appliance's "High Security" settings, demonstrating that the appliance has been configured in accordance with the Administrator Guide to use the FIPS validated module.



Example 3: Cisco ASA 9.6

1. Visit the NIST CMVP website to search for Cisco ASA modules. Review the search results and details for the various Cisco Adaptive Security Appliance (ASA) modules running on hardware model 5545 to determine which module applies to the ASA 9.6. Select Certificate #2820.



Cryptographic Module Validation Program

Search

Use this form to search for information on validated cryptographic modules.

Select the basic search type to search modules on the active validation list. Select the advanced search type to to search modules on the historical and revoked module lists.

Search Type: Basic Advanced — Search | Reset | Show All

Certificate Number:

Vendor: cisco

Module Name: asa 5545

4 certificates match the search criteria

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date
3232	Cisco Systems, Inc.	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, ASA 5585-X SSP-20, ASA 5585-X SSP-40 and ASA 5585-X SSP-60 Adaptive Security Appliances	Hardware	07/13/2018
2820	Cisco Systems, Inc.	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Adaptive Security Appliances	Hardware	01/23/2017
2618	Cisco Systems, Inc.	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Adaptive Security Appliances	Hardware	04/19/2016 08/10/2016

2. Review the details for Certificate #2820 and confirm the module is applicable for the ASA 9.6 running on 5545 hardware.

Cryptographic Module Validation Program

Certificate #2820

Details

Module Name	Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Adaptive Security Appliances
Standard	FIPS 140-2
Status	Active
Sunset Date	1/22/2022
Validation Dates	1/23/2017
Overall Level	2
Caveat	When operated in FIPS mode and with the tamper evident seals and security devices installed as indicated in the Security Policy
Security Level Exceptions	• Roles, Services, and Authentication: Level 3 • Mitigation of Other Attacks: N/A
Module Type	Hardware
Embodiment	Multi-Chip Stand Alone
Description	The market-leading Cisco ASA Security Appliance Series deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. The ASA 5500 Series Adaptive Security Appliances provide comprehensive security, performance, and reliability for network environments of all sizes.
Tested Configuration(s)	• N/A
FIPS Algorithms	AES: Certs. #2050, #2444, #2472, #3301 and #4249 CVL: Cert. #1002 DRBG: Certs. #332, #336, #819 and #1328 ECDSA: Cert. #989 HMAC: Certs. #1247, #1514, #2095 and #2787 RSA: Cert. #2298 SHS: Certs. #1794, #2091, #2737 and #3486 Triple-DES: Certs. #1321, #1513, #1881 and #2304
Other Algorithms	Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength); HMAC MD5; MD5; NDRNG; RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength); DES; RC4
Hardware Versions	ASA 5506-X[1], ASA 5506H-X[1], ASA 5506W-X[1], ASA 5508-X[2][3], ASA 5512-X[2], ASA 5515-X[5], ASA 5516-X[2][4], ASA 5525-X[5], ASA 5545-X[5], ASA 5555-X[5], ASA 5585-X SSP-10[6], 5585-X SSP-20[6], 5585-X SSP-40[6], and 5585-X SSP-60[6] with [ASA5506-FIPS-KIT=][1], [ASA5500X-FIPS-KIT=][2], [ASA5508-FIPS-KIT=][3], [ASA5516-FIPS-KIT=][4], [CISCO-FIPS-KIT=][5] or [ASA5585-X-FIPS-KIT][6]
Firmware Versions	9.6

Also notice that the “Caveat” indicates that the device must be operated in FIPS mode, and the “Other Algorithms” provides guidance that Diffie-Hellman needs to provide at least 112 bits of encryption strength.

3. In addition, open the Security Policy.

Firmware Versions 9.6

Vendor

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Global Certification Team
certteam@cisco.com

Related Files

Security Policy
Consolidated Certificate

Lab

GOSSAMER SECURITY SOLUTIONS INC
NVLAP Code: 200997-0

4. Review the Security Policy and note that Section 1 confirms the validated module applies to the Cisco ASA 9.6 on 5545 hardware when running in the FIPS 140-2 mode of operation.

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40 and 5585-X SSP-60 Adaptive Security Appliances (ASA) running Firmware 9.6; referred to in this document as appliances. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

Note that Section 3.1 indicates that "fips enable" must be configured to enable the FIPS-compliant mode of operation.

3.1 Crypto Officer Guidance - System Initialization

The Cisco ASA 5500-X series security appliances were validated with adaptive security appliance firmware version 9.6 (File name: asa962-1-lfbff-k8.SPA and asa962-1-smp-k8.bin). The ASA 5506-X, 5508-X, and 5516-X run the asa962-1-lfbff-k8.SPA firmware image. The ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X, and 5585-X run the asa962-1-smp-k8.bin. These are the only allowable images for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

Step 1: Disable the console output of system crash information, using the following command:

```
(config)#crashinfo console disable
```

Step 2: Install Triple-DES/AES licenses to require the security appliances to use Triple-DES and AES (for data traffic and SSH).

Step 3: Enable "FIPS Mode" to allow the security appliances to internally enforce FIPS-compliant behavior, such as run power-on self-tests and bypass test, using the following command:

```
(config)# fips enable
```

Additionally, note that Section 3.3 describes how to confirm the module is running in the approved move of operation.

3.3 Identifying Router Operation in an Approved Mode

The following activities are required to verify that the module is operating in an Approved mode of operation.

1. Verify that the tamper evidence labels and FIPS opacity shields have been properly placed on the module based on the instructions specified in the "Physical Security" and "Secure Operation" sections of this document.
2. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the "Secure Operation" section of this document.
3. Issue the following commands: 'show crypto IPSec sa' and 'show crypto isakmp policy' to verify that only FIPS approved algorithms are used.

5. To demonstrate the Cisco ASA is FIPS 140-2 validated, provide your auditor the following artifacts:

   A) FIPS 140-2 Certificate #2820
   B) The associated Security Policy PDF file for certificate #2820
   C) Evidence that the firewall is Cisco ASA 9.6 running on hardware model 5545

```
: Serial Number: [redacted]02G
: Hardware:   ASA5545, 12288 MB RAM, CPU Lynnf
!
ASA Version 9.6(3)1
!
```

   D) Evidence that the firewall has “FIPS Mode” enabled (in accordance with the Certificate’s “Caveat” section and the Security Policy’s “System Initialization” guidance)

```
hostname [redacted]
domain-name [redacted]com
enable password [redacted] encrypted
fips enable
```

   E) Evidence that only FIPS approved algorithms are used for both the IPSec SA and the ISAKMP policy. This can be provided with the “show” commands identified in section 3.3 of the Security Policy or the related commands from the configuration. The goal is to show that the “Other algorithms” from the Certificate are properly configured. In the case below, that means ensuring that the Diffie-Hellman group is sufficiently strong (e.g., GT 112 bits), which is equivalent to DH group of at least 14. (See IETF RFC 3526 and 5114).

```
crypto ipsec ikev2 ipsec-proposal FIPS256
 protocol esp encryption aes-256
 protocol esp integrity sha-384
crypto ipsec security-association pmtu-aging infinite
crypto map Outside_map 1 match address Outside_cryptomap
crypto map Outside_map 1 set pfs group14
crypto map Outside_map 1 set peer [redacted]
crypto map Outside_map 1 set ikev2 ipsec-proposal FIPS256
crypto map Outside_map 1 set security-association lifetime kilobytes unlimited
crypto map Outside_map 1 set nat-t-disable
crypto map Outside_map interface outside
```

IKE phase 1/ISAKMP

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha384
 group 14
 prf sha384
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 14
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 14
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside client-services port 443
```

Summary

Demonstrating compliance with FIPS 140-2 validated encryption is essential to achieving FedRAMP authorization. The FedRAMP “Digital Identity Requirements” document states, “FedRAMP continues to interpret ‘approved cryptographic techniques’ as FIPS 140-2 Validated cryptographic modules, which aligns with prior FedRAMP guidance.” Successful preparation for a FedRAMP assessment must address FIPS 140-2 validation.

The previous examples outline three methods for confirming FIPS 140-2 validation and demonstrating compliance with FedRAMP requirements for cryptographic modules. FIPS 140-2 validation is not a one-time effort, but rather an ongoing activity for first, achieving, and then maintaining FedRAMP authorization. Gathering evidence and documenting compliance can be challenging for some CSPs.

SecureIT has extensive compliance and audit experience to help you achieve FedRAMP authorization. Our security experts provide guidance and training that supports cost-effective compliance efforts that help CSPs expand their Federal business. Whether you need an advisor to guide compliance efforts or a 3PAO to conduct an assessment, SecureIT provides FedRAMP compliance expertise targeted to the specific needs of small and mid-sized businesses.

About SecureIT

SecureIT provides compliance, IT audit and cybersecurity services to enterprises, government entities, and cloud service providers. Our certified professionals assess cyber risk, conduct FedRAMP 3PAO assessments, and advise companies seeking compliance with regulatory requirements. Every day, we partner with our clients to deliver solutions critical to protecting and growing business.

12110 Sunset Hills Road
Suite 600
Reston, VA USA 20190
703.464.7010
www.secureit.com

Design by Marketlocity