WEB-CRYPTIK USER'S GUIDE

A web-based application for CMVP

Abstract

The Web Cryptik User's Guide is intended to provide users of the CVMP Web Cryptik application with clear and comprehensive guidance for accessing and most effectively using Web Cryptik to generate and submit their module packages.

O'Brien, Gavin W. (Fed)
go@nist.gov

Table of Contents

1 Introduction

Web-Cryptik is a web-based application for the Labs to create and submit their CMVP submissions to NIST.

1.1 Getting Started

Web-Cryptik requires a certificate to be installed in your browser and the CMVP needs to create a BOX account for sending and storing your files.

1.2 Creating a Certificate for Accessing Web-Cryptik

This section provides the instructions and steps to request access to the Web-Cryptik application.

The Web-Cryptik URL is https://cryptik.nist.gov:8443 (mTLS is required to access)

The request for a CSR (Certificate Signing Request) file needs to be sent to NIST via the NIST Secure File Transfer service found at https://nfiles.nist.gov. NIST security policies prohibit accepting a CSR via email or email attachment. It must be sent through the nfiles system. Please send a Web-Cryptik credential request email to Web-Cryptik support (cryptik-support@nist.gov) so that we may provide further instructions.

If users do not already have an existing nfiles account, or the nfiles account has gone dormant due to inactivity (per NIST policy), one can be requested through normal email using the above email address. A return email will then be sent via the nfiles service with instructions for establishing/re-activating your nfiles account.

Please send the CSR file in PEM format following these requirements:

- Use this naming convention for your CSR – please make sure this matches exactly as specified, otherwise the ingest process will not see it:
    - OrganizationName_FirstName_LastName_Demo.csr
- No spaces in the filename, please
- Do not zip the file, send it exactly as specified above please
- There should be no more than 3 underscore "_" characters in the filename
- Filename must have a .csr filename extension

- Use a minimum 2048-bit RSA key pair
- Sign using at least a SHA-256 hash
- Ensure to include the EMAILADDRESS attribute in the certificate subject
    - This can either be the user's email address OR a group alias email address (if applicable)
- Ensure to include the CN attribute in the certificate subject
    - This can either be the user's first and last name OR the name of the organization
    - No URLs in the CN attribute, please

- If you are submitting multiple CSRs using your organization's name and group email alias, the CN attribute *must* be unique for each submission

  - For example: CN=Orgname 1, CN=Orgname 2, CN=Orgname 3, etc.

- Ensure the C (country) attribute is only 2 letters

For example:

EMAILADDRESS=email.address@domain.com, CN=firstname lastname, OU=organization.unit, O=organization.name, L=city, ST=state, C=country.abbreviation.

Upon receipt of a user's CSR file, it will be validated against the above stated requirements. If there are any issues, NIST will let the user what needs to be corrected so that the file can be fixed and resubmitted.

Once the certificate is generated, it will be sent via a nfiles message. Users may begin using the credentials immediately upon receipt.

Users are expected to protect the key pair from unauthorized use and to notify NIST in the event the keypair becomes compromised. Also, since Web Cryptik does not have a formal login page, the following notice applies when accessing the site:

> ***WARNING***WARNING***WARNING
>
> You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicates your understanding of this warning.
>
> ***WARNING***WARNING***WARNING

The user's email address (and the email address included in the CSR, if different) will be added to a "Cryptik Maintenance" notification list. Use of the list will be limited to sending out outage and maintenance notifications, so the frequency of emails is quite low. However, if users prefer not to receive such notifications, please notify NIST accordingly and the appropriate addresses will be removed.

1.3 OpenSSL Detailed Instructions

Part 1:

# generate private key (minimum 2048)

```
openssl genrsa -out NIST_John_Doe_Cryptik.key 4096
```

# generate CSR (minimum sha256)

```
openssl req -out NIST_John_Doe_Cryptik.csr -key NIST_John_Doe_Cryptik.key -new -
sha256
```

# send CSR file to Jason

Part 2:

# receive back certificate from NIST

# create PFX/p12 bundle (contains priv key and pub cert)

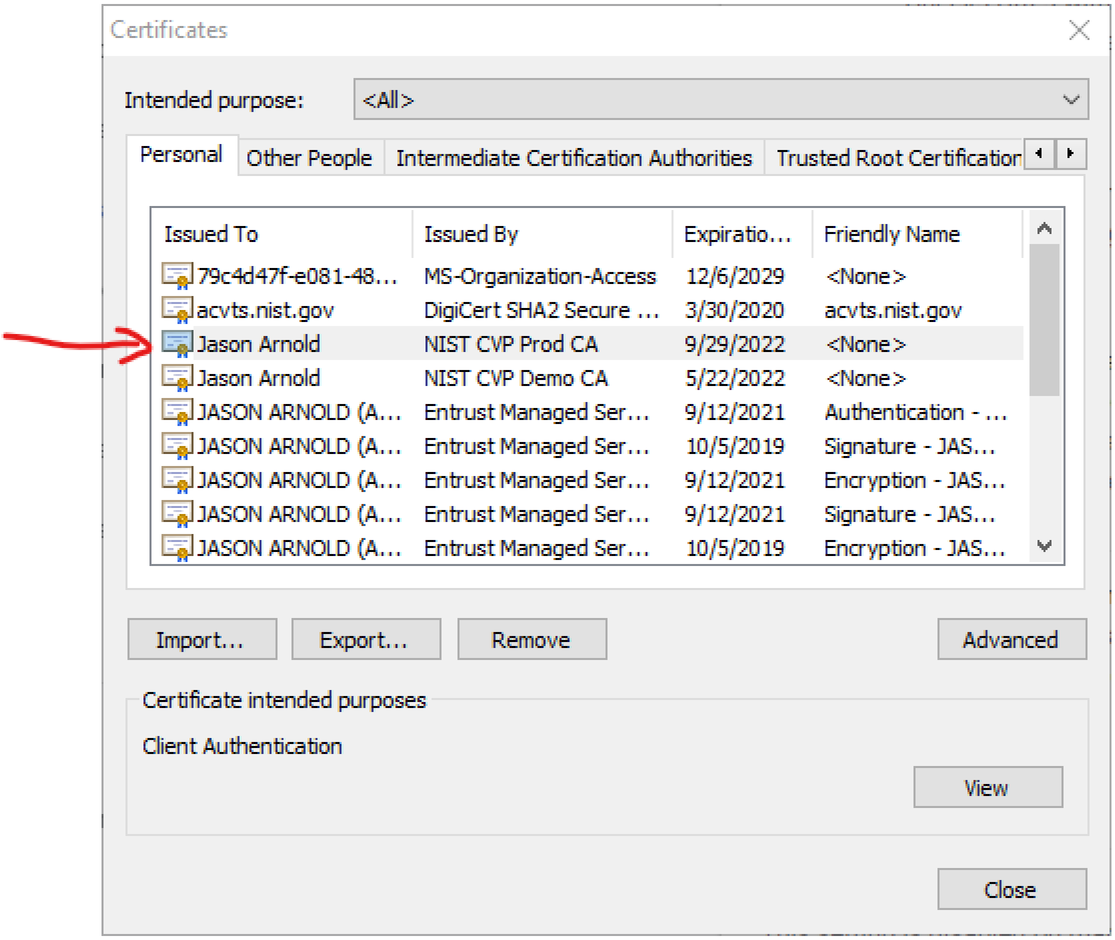
```
openssl pkcs12 -export -out NIST_John_Doe_Cryptik.pfx -inkey
./NIST_John_Doe_Cryptik.key -in ./NIST_JaJohn_Doe_Cryptik.cer
```

Part 3:

# import PFX into browser (follow your browser-dependent process)

1.4 Installing a Certificate in Chrome

In Chrome, access Settings – Privacy and security – Security – Manage device certificates. This gives you access to a Certificates pop-up window. The Personal tab should look similar to the screenshot below.



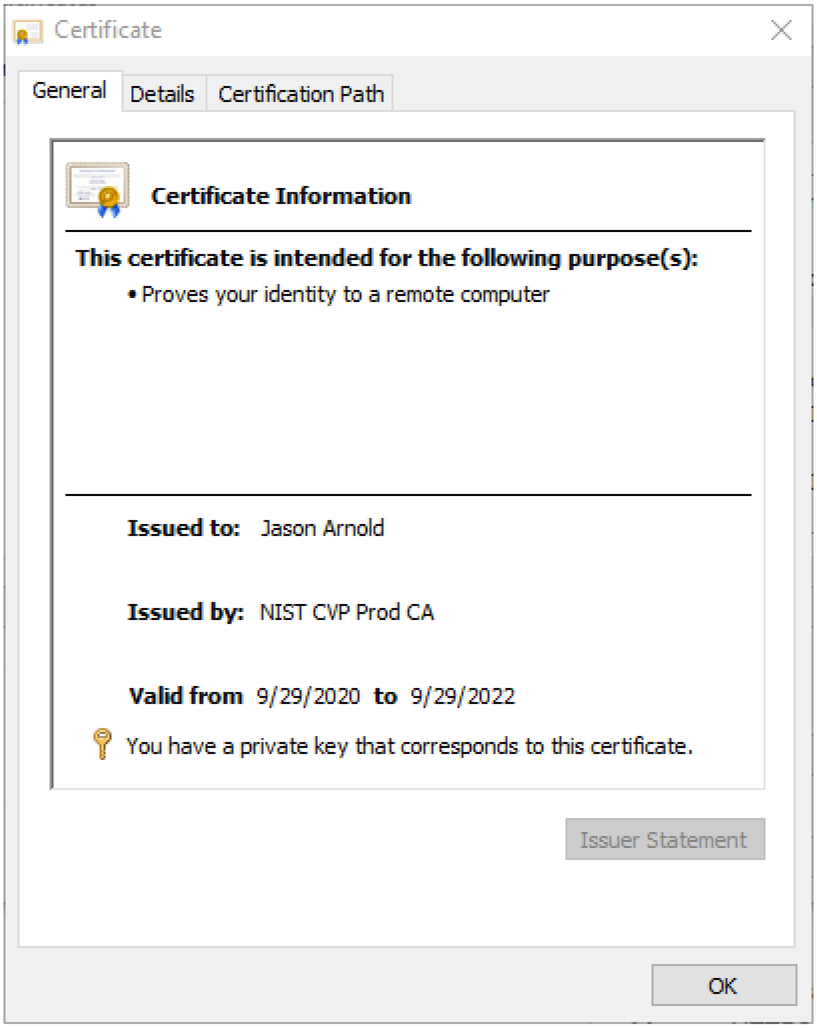
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
79c4d47f-e081-48...	MS-Organization-Access	12/6/2029	<None>
acvts.nist.gov	DigiCert SHA2 Secure ...	3/30/2020	acvts.nist.gov
Jason Arnold	NIST CVP Prod CA	9/29/2022	<None>
Jason Arnold	NIST CVP Demo CA	5/22/2022	<None>
JASON ARNOLD (A...	Entrust Managed Ser...	9/12/2021	Authentication - ...
JASON ARNOLD (A...	Entrust Managed Ser...	10/5/2019	Signature - JAS...
JASON ARNOLD (A...	Entrust Managed Ser...	9/12/2021	Encryption - JAS...
JASON ARNOLD (A...	Entrust Managed Ser...	9/12/2021	Signature - JAS...
JASON ARNOLD (A...	Entrust Managed Ser...	10/5/2019	Encryption - JAS...

Certificate intended purposes

Client Authentication

Use the Import button to install your Web-Cryptik certificate. After completing the install process, you can click on the “View” button to confirm that you have a corresponding private key installed. You should see a pop-up window like the screenshot below.



This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer

Issued to: Jason Arnold

Issued by: NIST CVP Prod CA

Valid from 9/29/2020 to 9/29/2022

You have a private key that corresponds to this certificate.

Note that the “NIST CVP Prod CA” issues the Web-Cryptik certificates, so that should be what is shown in your pop-up window.

1.5 Creating a BOX Account for Web-Cryptik

Users will have to create a BOX account using their personal email.

For users who do not own a NIST email address, which is the likely case for the labs, the link for creating a BOX account is:

https://account.box.com/signup/n/personal.

The link for users who own a NIST email address is:

https://psd.oism.nist.gov/box.

After filling the requested information, users will have to verify their email address to access the BOX instance. An email address verification request will be sent to their email. Simply click on the Verify Email button within the verification request to complete the process.

Users will then be redirected to the BOX interface, where they can see and manage their files. Files will only be seen after receiving and accepting an invitation from NIST to collaborate within a folder. Accepting the invitation can be done either through the email invitation, or through the BOX interface upon logging in.

Users will have to then setup their phone number for the 2-step verification process being used for BOX access. When logging in to collaborate on a specific folder, users will be prompted to enter the verification code that will be sent to their phone number during the login process. From there, users can access their folders and upload/view the files within.

Each lab will have access to 2 different folders:

- Submission folder: This is the folder where labs will be uploading their files to us. Within this folder, labs can upload, view, and pretty much manage their files as they wish
- Processed files folder: This folder will contain all the processed submissions from the first folder. When processing a submission, processed files will be moved from the first folder to this one, labs can't upload, delete, edit files within this folder but will be allowed to review the processed files to keep track of the current state of processing.
- You can at any time take a look at these folders by login into BOX or using the embedded version in the cryptic website by clicking "SEND RESULTS"
    - Link: https://cryptik. nist.gov:8443/send-results

2 Web-Cryptik Workflow

Web-Cryptik is a file creation and submission system. All transactions through Web-Cryptik are into NIST. All transactions back to CSTL originate from Resolve via PGP email and are outside the scope of this documentation.

2.1 Basic Transaction Types

2.1.1 Implementation Under Test (IUT) Submissions

- IUTA = IUT – Add ➔ Add report to IUT list
- IUTB = IUT – Billing ➔ Request an invoice from NIST for Cost Recovery before report submission
- IUTC = IUT – Cancel Billing ➔ Cancel a request for an invoice from NIST for Cost Recovery - Only available if the invoice has not been paid
- IUTR = IUT – Remove ➔ Remove report from the IUT list
- IUTM = IUT – Modify ➔ Modify an existing IUT entry

IUT Submissions: IUTA submissions are partial submissions notifying the CMVP that the lab is working on an implementation. IUTB allow for the lab to pay for the submission ahead of time. IUTC, IUTR, and IUTM allow for the lab to modify the IUT in the appropriate manner. IUTB and IUTC access the CMVP billing system. All IUTs have impact on the IUT list.

IUTs only require General Info to be completed.

2.1.2 Reviewed Submissions

- FS = Full Submission ➔ The first time a new software, firmware, hardware, or hybrid module is submitted for validation. See the FIPS 140-3 Management Manual (MM) Section 7.1.2 *Full Submission (FS)*.
- UPDT = Update ➔ Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-3 security relevant items. See the FIPS 140-3 MM Section 7.1.10 *Update (UPDT)*.
- Reviewed Submission Follow-ups:
  - sCMn ➔ CMVP comments or returned CSTL addressed comments
  - FCLC ➔ CSTL Approve or Reject response to Draft Certificate

Reviewed Submissions: Once submitted and it moves to the top of the queue, the CMVP reviews the submission and sends a response to the lab. The module is now in "Coordination". At this point, a series of communications happen via the sCMn or comments submissions until all issues have been resolved. Once the reviewers agree there are no issues the draft cert is sent to the lab and the lab responds with an FCLC submission. If the lab OKs the FCLC then the certificate is posted to the CSRC. If the lab does not accept the draft certificate it goes through another round of submissions until an FCLC OK is submitted. This completes the validation process.

2.1.3 Maintenance Submissions

- VUP = Vendor Update ➔ Administrative updates (e.g., updating vendor contact information, grammatical Security Policy corrections). See the FIPS 140-3 MM Section 7.1.3 *Vendor Update (VUP)*.
- VAOE = Vendor Affirmed Operating Environment ➔ Security policy change of vendor affirmed OEs. See the FIPS 140-3 MM Section 7.1.4 *Vendor Affirmed Operating Environment (VAOE)*.

- NSRL = Non-Security Relevant ➔ Modifications are made to hardware, software or firmware components that do not affect any FIPS 140-3 security relevant items. See the FIPS 140-3 MM Section 7.1.5 *Non-Security Relevant (NSRL)*.
- ALG = Algorithm Update ➔ Post validation, approved security relevant functions or services for which CAVP testing was not available (or vendor affirming was still permitted per the CMVP/CAVP transition schedule) at the time of submission to the CMVP for validation are now CAVP-tested and are being submitted for inclusion as an approved function or service. See the FIPS 140-3 MM Section 7.1.6 *Algorithm Update (ALG)*.
- OEUP = Operating Environment Update ➔No changes to the module with an addition of a tested OE that does not affect any security relevant items other than CAVP-testing the algorithm validations on the new OE. See the FIPS 140-3 MM Section 7.1.7 *Operating Environment Update (OEUP)*.
- RBND = Rebrand ➔This scenario applies if there are no modifications to a module and the new module is a re-branding of an already validated Original Equipment Manufacturer (OEM) module. See the FIPS 140-3 MM Section 7.1.8 *Rebrand (RBND)*.
- PTSC = Port Sub Chip ➔A sub-chip cryptographic subsystem that was previously validated in a single-chip (see IG 2.3.B) can be ported to other single-chip constructs as a PTSC submission to the CMVP. See the FIPS 140-3 MM Section 7.1.9 *Port Sub Chip (PTSC)*.
- CVE = Common Vulnerabilities and Exposures ➔ A CSTL has been contracted to perform a revalidation for a module on which the vendor has made FIPS 140 security-relevant changes in response to one or more CVEs. See the FIPS 140-3 MM Section 7.1.11 *Common Vulnerabilities and Exposures (CVE)*.
- TRNS = Algorithm Transition ➔A CSTL has been contracted to perform a revalidation for a module on which the vendor has made FIPS 140-3 security relevant changes solely in response to a published CMVP algorithm transition that will cause some previously validated modules to be placed on the Historical list. See the FIPS 140-3 MM Section *7.1.12 Algorithm Transition (TRNS)*.
- PHYS = Physical Enclosure ➔ Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module. See the FIPS 140-3 MM Section 7.1.13 *Physical Enclosure (PHYS)*.

Maintenance Submissions: These submissions are small updates that should only require a relatively light review. These submissions may follow a similar process described above in **Reviewed Submissions**.

2.1.4 Status Submissions

- STAT ➔ Query report status
- RQFG ➔ CSTL Request For Guidance
- DRPT ➔CSTL request to DROP report
- OTHR ➔ Other request
- sHLD ➔ Place report on HOLD

Status Submissions: These submissions are information requests or notifications for an existing submission.

2.2 Submission Workflow

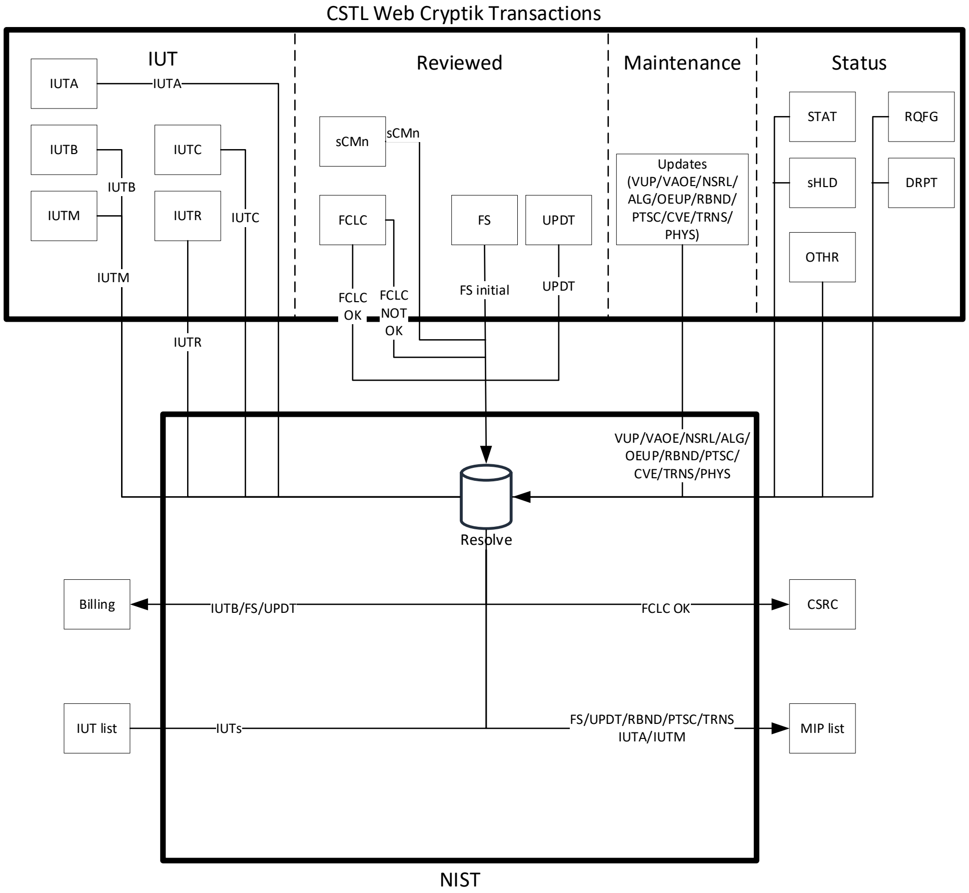


Figure 1: Web Cryptik File Submission Workflow

3 Graphical User Interface (GUI) Functionality

3.1 General Info

Required info is marked with an asterisk *.

3.1.1 Laboratory Information

1. Lab Name *
   - Lab names are obtained from NVLAP
   - Address Info is not needed it is obtained from NVLAP
2. Signature 1 *
3. Title 1*
4. Signature 2
5. Title 2
6. Signature 3
7. Title 3

3.1.2 Vendor Information

1. Vendor Name*
   - The name of the vendor (including Corp., Inc., Ltd., etc.) that developed the cryptographic module. Please include any registration marks or special characters.
2. Address 1*
3. Address 2
4. Address 3
5. City*
6. State/Provence
7. Postal Code*
8. Country*
9. Vendor Web site*
   - Format checking "https://"
10. Product Link*
    - a URL that may be specific to the module or products which utilize the module. Do not include the prefix https:// or duplicate the Vendor Web site URL.
11. Contact 1*
12. Email 1*
    - Check formatting
13. Phone 1*
    - Check formatting
14. Fax 1*
    - Check formatting
15. Contact 2

16. Email 2
    - Check formatting
17. Phone 2
    - Check formatting
18. Fax 2
    - Check formatting

3.1.3 Module Information

1. Transaction Type *

Defines the type of submission and controls the files generated during the Create Package process. Options include all the Transaction Types listed in Section 2.1 - Basic Transaction Types as well as Approve and Reject selections. The Approve and Reject options are used for Labs to approve or reject a Draft Certificate that has been sent to them.

   a. Submission Type *

   Required if the initial Transaction Type selection does not match one of the twelve valid 140-3 Submission Types (i.e., Full Submission (FS), Vendor Update (VUP), Vendor Affirmed Operating Environment (VAOE), Non-Security Relevant (NSRL), Algorithm Update (ALG), Operating Environment Update (OEUP), Rebrand (RBND), Port Sub Chip (PTSC), Update (UPDT), Common Vulnerabilities and Exposures (CVE), Algorithm Transition (TRNS), and Physical Enclosure (PHYS)).

2. LC – Lab Code [pre-filled by Module Information page]

3. CSTL TID*
    - Check formatting

4. CSEC TID*
    - Check formatting

5. Lab internal ID

6. Test Date
    - (UI) Calendar pick list

7. Tester 1*

8. CVP Number 1

9. Tester 2

10. CVP Number 2

11. Tech Reviewer 1*
    - Should include the CVP (unless separate field is defined for this available).

12. Tech Reviewer 2

13. Module Name(s)*
    - Referenced by: [Security Policy, Draft Certificate]
    - The complete name of the cryptographic module. Do not include the version number with the name unless by vendor choice. The name of the cryptographic module must be consistent with ISO/IEC 24759:2017 AS02.11 and the name found in the Security Policy and test report. Please include any registration marks or special characters.
14. FIPS Version (Change) add FIPS 140-3*
    - Referenced by: [Security Policy, Draft Certificate]
15. Entropy
    - Select only for legacy purposes when ENT (P) and/or ENT (NP) is claimed.
    - Will *not* trigger an ENT review, since ESV certification is required as of Jan 1, 2023.

16. Entropy Technology
    - Select only for legacy purposes when ENT (P) and/or ENT (NP) is claimed.
    - Entropy Technology field selection maps to the following entries on the module certificate:
        - [Ring Oscillators, RDSEED/RDRAND, Quantum Source, Other Hardware Source] → ENT (P);
        - [CPU Jitter, Linux RNG, Other Software Source] → ENT (NP);
        - IG 9.3.A Scenario 2 → no entry.
    - If both an ENT (P) and ENT (NP) are claimed, select ENT (P) and the CMVP will update the CSRC webpage to also include the ENT (NP) once validation is completed.
17. Module Count:
    - A number. See FIPS 140-3 MM Section 7.7 *Module count definition*.

18. Module Hardware Version

    Referenced by: [Security Policy / Draft Certificate TE.02.03.02, TE02.12.01]

19. Module Software Version

    Referenced by: SP/DC TE.02.03.02, TE02.12.01

20. Module Firmware Version

    Referenced by: [SP/DC TE.02.03.02, TE02.12.01]

    - Rule: Must select at least one of (Hardware, Software, Firmware)*

For **Hardware, Software and Firmware versioning**, the specific versioning information representative of each of the crypto module's elements. This number **shall** be of sufficient level such that updates/upgrades/changes **shall** be reflected in a new version (see **AS04.32**). For example, version 4 may not be sufficient if the releases are numbered 4.0, 4.1, 4.2, etc. The version number may also include letters, for example, 4.0a, 4.0b, 4.0c, etc. This **shall** include the version numbers for each element; hardware, software, and firmware, if applicable. Each elements version number (e.g. hardware, firmware, software) **shall** be separated by a semi-colon. If a module does not include an element, leave the field blank; do not enter "NA". The version numbers **shall** be the same as the ones found in the Security Policy. For example, hardware version: 4.2; software version: 4.0a.

If possible, a hardware version of a module **shall** represent all the components of the module, included (**AS02.15**) or excluded (**AS02.14**). If there are any additional components, included (**AS02.15**) or excluded (**AS02.14**), that are inside the module boundary but are not within the scope of the hardware version then the module certificate **shall** list these additional components separately in the hardware version field. Brackets **shall** be used to group hardware versions with their corresponding components. If the module is a collection of different hardware components, included (**AS02.15**) or excluded (**AS02.14**), and does not contain a hardware version, then the module certificate **shall** list all of the components of the module in the hardware version field without referencing any hardware version.

If there are multiple modules listed on the certificate, or if there are multiple part numbers with different versions of firmware for example, brackets **shall** be used to clearly indicate the pairings between the versioning information and/or the module names.

Examples:

- **Hardware Versions: 5.2 and 5.3, Build 3; Firmware Version: 2.45**
  Two different hardware modules, each with the same embedded firmware. All of the components in these hardware modules must be considered: included (**AS02.15**) or excluded (**AS02.14**).
- **Hardware Versions: 5.2 [1] and 5.3 [2], Build 3; Firmware Versions: 2.45 [1] and 2.50 [2]**
  Two different hardware modules each with the specified version of embedded firmware.
- **Hardware Version: 88X8868; Software Version: 1.0**
  Software hybrid module referencing the hardware and disjoint software components.
- **Hardware Version: BN45; Firmware version 1.0; Software Version 2.0**
  Software hybrid module referencing the hardware and disjoint software versions. The hardware component also has firmware embedded within it.
- **Hardware Version: 88X8686; Firmware Version 1.4;**
  Firmware hybrid module referencing both the hardware and disjoint firmware versions.
- **Hardware Version: [XYZ1, XYZ2, and XYZ3 with components 1234, 1235, 1236] and [ZYX1, ZYX2 and ZYX3 with components 1234, 5123, 6123]; Firmware Version: 1.0**
- Hardware module contains multiple hardware versions that have additional corresponding components that are included (**AS02.15**) or excluded (**AS02.14**). Note the use of brackets and commas.
- **Hardware Version: P/N 5432, 7654, and 4321; Firmware Version: 1.0**
  Hardware module that is a collection of hardware components that are included (**AS02.15**) or excluded (**AS02.14**) rather than a versioned hardware module.

21. Module Description*

    Referenced by: [ref. TE02.03.01]

22. Module Embodiment*
    - Single chip
    - Multi chip embedded
    - Multi-chip stand alone

    Rules: [Affects the files that need to be submitted.]

    Referenced by: [TE.07.04.01, SP/DC TE.07.09.01]

    See ISO/IEC 19790:2012 Section 7.7.1 for examples of each.

23. Type*:
    - Software
    - Hardware
    - Firmware
    - Software-hybrid
    - Firmware-hybrid

    Referenced by: [Display in TE.02.03.01] TE.02.03.01-type (should have two boxes)

    Rules: [Affects the files that need to be submitted.]

24. Section Levels:

- The total level is computed as the floor of all the levels. Levels for A and B are also set as the floor of the levels 1-12.
- If Module Type is "Software": Section 7 is N/A otherwise Section 7 cannot be N/A
- If Module Type is "Software": Section 6 cannot be Level 3 or Level 4
- See 140-3 MM Section 7.5 *Partial validations and non-applicable areas*

25. Flags
    - Maintenance
    - By Pass
    - Identity Auth.

      Other references: [TE 03.20.01]

26. Administrative Flags
    - ITAR
    - Add Module to MIP list

27. Cert Caveat: the specific stipulations that make this certificate valid.
    - List of applicable caveats. See CMVP webpage on Caveats.
    - This caveat may be modified or expanded by the CMVP during the validation process.
28. Operating Environment
    - This is the specific operational environment(s) or configuration(s) that was employed during testing by the CST laboratory. It applies to software, firmware, hybrid, or sub-chip modules. The

operational environment includes the operating system(s), the tested platform(s), and the processor(s).

- For multiple operating environment entries, separate each with a semi-colon; do not use "and".

Examples:

- **BlackBerry OS® Versions 3.8, 4.0 and 4.1 on a BlackBerry® 7230 with Qualcomm Snapdragon S4 Plus;**
- **Debian GNU/Linux 4.0 (Linux kernel 2.6.17.13) running on a 4402-A ViPr Desktop Terminal with an Intel i7-8550U;**
- **HP-UX 11.23 running on an IBM RISC 6000RB2 with an Intel Xeon E3-1230;**
- **Microsoft Windows XP with SP2 running on a Dell Optiplex Model 4567 with an Intel i7-8550U;**
- **Microsoft Windows XP with SP2 running on an HP Pavilon 4.5 with an AMD A8-3850;**
- **SEPOS running on Apple TV 4K with an Apple A10X Fusion;**
- **Sun Solaris Version 2.6SE running on a Sun Ultra SPARC-1 workstation with an Intel Xeon X5670;**
- **Tintri OS 4.5 running on a EC6030 with an Intel Xeon E5-2609;**
- **Wind River Linux 6.0 running on a Xerox Explorer 60 with an Intel Atom E3800;**

If the *firmware* module's physical security meets ISO/IEC 19790:2012 Section 7.7 levels 2, 3 or 4, the hardware platform **shall** include applicable specific versioning information.

- **Little OS® Version 3.7b running on a Crypto Unit (Hardware Version: 1.0) with AMD Duron 800**

The operating system may also represent virtual environments. Virtual environments are run by computer software, firmware or hardware called a hypervisor. Native hypervisors run directly on the host computer. Hosted hypervisors run on a conventional operating system.

For a Type 1 (or native) hypervisor, the OE listing **shall** include the guest OS, hypervisor, platform, and processor using the following format:

- ***<Guest OS>*** on ***<hypervisor>*** running on ***<platform>*** with <***processor***>
  Example: Windows 10 on VMWare ESX 5 running on a Dell Optiplex 5460 with an Intel Core i5

For a Type 2 (or hosted) hypervisor, the OE listing **shall** include the guest OS, hypervisor, host OS, platform, and processor using the following format:

- **Operational Environment**: ***<Guest OS>*** on ***<hypervisor>*** on ***<Host OS>*** running on ***<platform>*** with <***processor***>
  An example is: Windows 10 on Oracle VM VirtualBox on Oracle Solaris 11 running on a HP Model 20 with Intel Xeon E5-2670v3

29. PIV Cert #

- the cert number related to PIV validation. (format) a number less than
- Check format 4-digit number.
- When a module implements a validated PIV application, the application validation certificate type and number shall be included. Additional information relating to PIV versioning can be found in the MM Section 7.6 *CMVP requirements for PIV validations References*.

30. Revalidation Cert Number: It is a cert number assigned to an existing submission that is undergoing revalidation (i.e., anything besides FS)

31. Special Instructions

- E.g., which module submissions should be grouped, what are the dependencies, etc.

3.1.4 Appendix B Tables

Appendix B captures data set forth in the SP 800-140B.

3.1.4.1 Section 1: General

- Introduction: an introduction for the Security Policy
- Security levels: the security levels are input on the Module information Page.

Table 1: Security Levels

Section	**FIPS 140-3 Section Title**	**Security Level**
1	General	[Level 1-4]
2	Cryptographic module specification	[Level 1-4]
3	Cryptographic module interfaces	[Level 1-4]
4	Roles, services, and authentication	[Level 1-4]
5	Software/Firmware security	[Level NA, 1-4]
6	Operational environment	[Level NA, 1-2]
7	Physical security	[Level NA, 1-4]
8	Non-invasive security	[Level NA, 1-4]
9	Sensitive security parameter management	[Level 1-4]
10	Self-tests	[Level 1-4]
11	Life-cycle assurance	[Level 1-4]
12	Mitigation of other attacks	[Level NA, 1-4]
	Overall Level	Overall Level

Referenced by: TE.06.03.01, 07.09.02

3.1.4.2 Section 2: Cryptographic Module Specification

Table 2: Software, Firmware, Hybrid Tested Operational Environments

#	**Operating System**	**Hardware Platform**	**Processor**	**PAA/Acceleration**	**Actions**

1					[DELETE] [EDIT]
2	[Text box]	[Text box]	[Text box]	[Text box]	[ADD]

Referenced by: TE.06.03.01

Table 3: Software, Hardware, Hybrid Vendor Affirmed Operational Environment

#	Operating System	Hardware Platform	Actions
1			[DELETE] [EDIT]
2	[Text box]	[Text box]	[ADD]

Referenced by: TE.06.03.01

Table 4: Hardware Tested Configuration

#	Model	Hardware [Part Number & Version]	Firmware Version	Distinguishing Features [1]	Actions
1	RS9113	6.0	RS9113.N00.WC.FIPS.OSI.1.8.2	Bootloader v 1.8	[DELETE] [EDIT]
2	[Text box]	[Text box]	[Text box]	[Text box]	[ADD]

Referenced by: TE.06.03.01

Table 5: Approved Algorithms

#	Vendor Name	CAVP Cert	Algorithm and Standard	Mode / Method	Description/Key Size/Key Strength	Use/Function	Actions
1	VendorA	A9999	<AES-CBC, AES-ECB, AES-CCM, AES-CFB1, etc.>	<AES-CBC, AES-ECB, AES-CCM, AES-CFB1, etc.>	128, 192, 256-bit keys with 128, 192, 256-bit key strength	Symmetric encryption; Symmetric decryption	[DELETE] [EDIT]
…	[SEARCH]	[Pull down]	[Pull down]	[Text box]	[Text box]	[Text box]	[ADD]

[1] Examples may be ports and interfaces, memory storage devices and sizes, field replaceable and stationary accessories (power supplies, fans), etc.

Enter a vendor name and then the CAVP Cert pull down will be populated. Once the user selects a CAVP cert the Algorithm and Standard Pull down will be populated.

These are the approved algorithms included in the cryptographic module and utilized by the module's callable services or internal functions.

If a module contains within it or is bound to an already validated cryptographic module, all approved security functions that are used by the module's callable services and internal functions **shall** be included in this table (e.g., both those within the embedded/bound module and in addition to the embedding/binding module). Algorithms that are never called **shall not** be include. An algorithm that can only be called by a service that performs the self-tests also **shall not** be included; however, the module's Security Policy **shall** have an entry for the corresponding self-test and explain that this algorithm can only be executed when running a self-test.

The algorithm **shall** meet all three (3) conditions to be listed as approved:

1. an approved security function as specified in one of the **SP 800-140** documents and validated by the CAVP (see the CAVP supported algorithms);
2. meet all requirements of FIPS 140-3 (self-tests, etc.); and
3. used in at least one approved cryptographic function or service for that cryptographic algorithm in an approved mode of operation.

Referenced by: TE02.20.01

Table 6: Vendor Affirmed Approved Algorithms

#	Algorithm	Caveat	Use / Function	Actions
1	CKG (SP 800-133Rev2)	Vendor Affirmed	Cryptographic Key Generation; SP 800-133 and IG D.I.	[DELETE][EDIT]
2	[Text box]	[Text box]	[Text box]	[ADD]

Referenced by: TE02.20.03, TE02.20.04

Table 7: Non-Approved Algorithms Allowed in the Approved Mode of Operation

#	Algorithm	Caveat[2]	Use / Function	Actions
1	AES	Cert. A9999, key unwrapping[3]. Per IG D.G.	Symmetric key unwrapping	[DELETE][EDIT]
2	EC <Diffie-Hellman or MQV> with non-	Provides N or M bits of encryption	Shared secret computation using non-NIST curves	[DELETE][EDIT]

[2] Encryption strength caveat applies when the security strength of the SSP establishment scheme can be less than that of the agreed or transported key. Encryption strengths are based on algorithm key sizes in bits only. The calculation of the encryption strength based on key size is performed per IG D.B. The effective encryption strength may be less depending upon the amount of available entropy. See IG 9.3.A, IG D.J and this guidance for additional guidance and applicable caveats.

[3] This is an allowed but non-SP-800-38F-compliant key unwrapping (IG D.G), where the key used in key transport is of equal or greater strength than the unwrapped key and therefore the strength caveat is not required.

	NIST recommended curves	strength)[4]. Per IGs D.F and C.A.	[curveX, curveY, with strengths N and M]	
3	ECDSA with non-NIST recommended curves	Provides N or M bits of encryption strength)[5]. Per IG C.A.	Key pair generation, digital signature generation, digital signature verification using non-NIST curves [curveX, curveY, with strengths N and M]	[DELETE][EDIT]
4	RSA[6]		Asymmetric key un-encapsulation	[DELETE][EDIT]
5	RSA[7]	Provides N bits of encryption strength. Per IG D.G.	Asymmetric key encapsulation and un-encapsulation	[DELETE][EDIT]
6	RSA[8]	RSA component Cert. A9999. Provides N bits of encryption strength. Per IG D.G.	Asymmetric key encapsulation and un-encapsulation	[DELETE][EDIT]
…	[Text box]	[Text box]	[Text box]	[ADD]

These are cryptographic algorithms that are not approved but are allowed to be used in an approved mode of operation. Allowed algorithms **shall** be listed in alphabetical order.

For the non-approved establishment schemes, refer to IG D.F and IG D.G.

Referenced by: TE02.20.02

Table 8: Non-Approved Allowed in the Approved Mode of Operation with No Security Claimed

#	Algorithm	Caveat	Use / Function	Actions
1	MD5	Only allowed as the PRF in TLSv1.0 and v1.1 per IG 2.4.A	Message digest used in TLSv1.0 / v1.1 KDF only	[DELETE][EDIT]

[4] Compliant to IG D.F Scenario 3 (and IG C.A) with no claim of compliance with SP 800-56A Rev3. This entry must be accompanied with an approved SP 800-56A Rev3 method using at least one NIST-recommended curve as required by IG D.F Scenario 3 (c).

[5] Compliant to IG C.A. This entry must be accompanied with an approved ECDSA entry using at least one NIST-recommended curve as required by IG C.A.

[6] The module does not support RSA key encapsulation but does employ RSA key un-encapsulation that uses a PKCS#1-v1.5 padding scheme with no claim of compliance with any testable component of SP 800-56B Rev2.

[7] Uses an RSA-based PKCS#1-v1.5 padding scheme with no claim of compliance with any testable component of SP 800-56B Rev2.

[8] The RSADP component of an RSA-based PKCS#1-v1.5 padding scheme is tested by CAVP for its compliance with SP 800-56B Rev2. The module supports both the encapsulation and the un-encapsulation of the cryptographic keys using RSA. The listed RSADP Component certificate applies only to the key un-encapsulation portion.

…	[Text box]	[Text box]	[Text box]	[ADD]

See IG 2.4.A.

Referenced by: TE02.21.01, TE02.21.02

Table 9: Security function implementation (SFI)

#	Name	Type	Description	SF Properties	Algorithms/CAVP Cert	Actions
1	[Text box]	[Pull down]	[Text box]	[Text box]	[checkbox]	[DELETE][EDIT]
2	KAS-1	KAS	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2).	P-224 curve providing 112 bits of encryption strength	* KAS ECC SSC Sp800-56Ar3/A999 * KDF IKEv2/A999 * KAS KC Sp800-56 (Component)/A999 [PRE-REQUISITES[1]]	[ADD]
3	KAS-2	KAS	SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2).	2048-bit key providing 112 bits of encryption strength	* KAS FFC Sp800-56Ar3/A999 [PRE-REQUISITES[1]]	
4	KAS-3	KAS	SP 800-56Brev2. KAS-IFC per IG D.F Scenario 1 path (2).	3072-bit modulus providing 128 bits of encryption strength	* KAS IFC/A999 [PRE-REQUISITES[1]]	
5	KTS-1	KTS	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128, 192, and 256-bit keys providing 128, 192, or 256 bits of encryption strength	* AES GCM/A999 [PRE-REQUISITES[1]]	
6	KTS-2	KTS	SP 800-56Brev2. KTS-IFC (key encapsulation and un-encapsulation) per IG D.G.	2048-bit modulus providing 112 bits of encryption strength	* KTS IFC KTS-OAEP-basic/A999 [PRE-REQUISITES[1]]	
…						

[1] As applicable.

This table will incorporate the module's approved KTS and/or KAS implementations both that are end-to-end CAVP tested or the combination of separate CAVP tests (see IGs D.F and D.G). Each unique KTS and/or KAS implementation is listed as a separate row.

Table 9 Columns:

- Name – a unique name that relates to the Security Function. E.g., it can be KTS1, KAS1, or KTS xxx.
- Type – Select either KAS (Key Agreement Scheme) or KTS (Key Transport Scheme).
- Description – details and usage. This should include a reference to a specific Publication Section, IG, etc.
- SF Properties – If there are specific properties or characteristics associated with this SF implementation. This includes the curve/key/modulus sizes and corresponding bit strength caveats for KAS and KTS, if the

security strength of the scheme can be less than that of the agreed or transported key. The strength caveat looks like: “providing [N and/or M] bits of encryption strength”.

- Algorithms/CAVP Cert – what Algorithms from the Approved Algorithm list are part of the implementation. Include prerequisites.

Table 10: Entropy Certificates

#	Algorithm	Caveat	Actions
1	[SEARCH]	[Pull down]	[DELETE][EDIT]
2			[ADD]

Search of available ESV certificates used by the module.

Referenced by:

Table 11: Non-Approved Algorithms Not Allowed In the approved Mode of Operation

#	Algorithm/Function	Use/Function	Actions
1	RC4	Symmetric encryption; Symmetric decryption	[DELETE][EDIT]
	[Text box]	[Text box]	[ADD]

Referenced by: TE02.20.02

File Upload 1: Illustrative Diagram, schematic or photograph of module.

- Insert a new and location of file to be uploaded.
- This could contain multiple files

Referenced by: TE02.15.09 need to contain a reference to an Illustrative Diagram:

File Upload 2: Block Diagram.

Block Diagram Description: text box to describe you block diagrams

3.1.4.3 Section 3: Cryptographic Module Interfaces

Table 12: Ports and Interfaces

#	Physical port	Logical interface	Data that passes over port/interface	Actions
1				[DELETE][EDIT]

2				[ADD]

Hardware and Hybrid modules are expected to have at least one "Physical port" defined since any of their logical interfaces must ultimately map to a physical port. N/A is an acceptable entry for Software-only and Firmware-only modules.

Referenced by: TE03.01.01

3.1.4.4 Section 4: Roles, Services, and Authentication

Table 13: Roles, Services, Input, and Output

#	Roles	Service	Input	Output	Actions
					[DELETE][EDIT]
					[ADD]

Referenced by: TE04.03.01

Table 14: Roles and Authentication

#	Role	Authentication Method	Authentication Strength	Actions
				[DELETE][EDIT]
				[ADD]

Referenced by: TE04.03.01

Table 15: Approved Services

#	Service	Description	Approved Security functions	Keys/SSPs	Roles	Access rights to Keys/SSPs	Indicator	Actions
								[DELETE][EDIT]
								[ADD]

Referenced by: TE04.11.02

3.1.4.5 Section 5: Software/Firmware Security

3.1.4.6 Section 6: Operational Environment

3.1.4.7 Section 7: Physical Security

Table 16: Non-Approved Services

#	Services	Description	Algorithms Accessed	Role	Indicator	Actions
						[DELETE][EDIT]
						[ADD]

Table 17: Physical Security Inspection Guidelines

#	Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details	Actions
				[DELETE][EDIT]
				[ADD]

Referenced by: TE07.01.01

Table 18: EFP/EFT

	Temperature or Voltage Measurement	EFP/EFT?	Specify if this condition results in a shutdown or zeroization
Low Temperature			
High Temperature			
Low Voltage			
High Voltage			

Referenced by: TE07.03.01

Table 19 –Hardness testing temperature ranges

	Hardness tested temperature measurement
Low Temperature	
High Temperature	

3.1.4.8 Non-invasive security

3.1.4.9 Sensitive security parameter management

Table 20 SSPs

#	Key/SSP/ Name/Type	Strength	Security Function Cert Number	Generation	Import /Export	Establishment	Storage	Zeroization	Use & related keys	Actions
										[EDIT][DELETE]
										[ADD]

Table 21 Non-Deterministic Random Number Generation Specification

#	Entropy Sources	Minimum number of bits of entropy	Details	Actions
				[EDIT][DELETE]
				[ADD]

3.1.4.10 Self-tests

3.1.4.11 Life-cycle assurance

3.1.4.12 Mitigation of other attacks

3.2 Reports

All subsections of the Reports section contain the following utilities to facilitate updating and reviewing the entered data.

- Check Status ➔ Used to confirm whether Section is Open or Closed
- Filter By Status ➔ Used to filter items based on Test Status
- Jump to ➔ Used to quickly relocate to a specific Section item
- Reset All to Open ➔ Used to clear all Test Status selections and reset them to Open

The Reports section is organized into the 14 subsections listed below. Each subsection contains the Assertion, Vendor, and Test evaluation items required for that subsection at the chosen Security Level.

- 1. General
- 2. Cryptographic module specification
- 3. Cryptographic module interfaces
- 4. Roles, services, and authentication
- 5. Software/Firmware security
- 6. Operational environment
- 7. Physical security
- 8. Non-invasive security

- 9. Sensitive security parameter management
- 10. Self-tests
- 11. Life-cycle assurance
- 12. Mitigation of other attacks
- Appendix A
- Appendix B

3.3 References

The Reference tab is used to create references within the Report section of the interface.

3.4 Draft Certificate

FIPS 140-3
Validation Certificate

Certificate No

The National Institute of Standards and Technology, as the United States FIPS 140-3 Cryptographic Module Validation Authority; and the Canadian Centre for Cyber Security, as the Canadian FIPS 140-3 Cryptographic Module Validation Authority; hereby validate the FIPS 140-3 testing results of the Cryptographic Module identified as:

in accordance with the Derived Test Requirements for FIPS 140-3, Security Requirements for Cryptographic Modules. FIPS 140-3 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-3 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

<Company Name>

Hardware Version: <hardware version>

Firmware Version: <firmware version>
Embodiment: <embodiment>
Tested by the Cryptographic Module Testing accredited lab: *<Lab name>, NVLAP Lab Code <Lab code>*
CRYPTIK version: <WebCryptik Version>
Tested Configuration(s): <Operational Environments>
The testing levels are as follows:

Cryptographic Module Specification:	Level N	*Cryptographic Module Ports and Interfaces:*	Level N
Roles, Services, and Authentication:	Level N	*Finite State Model:*	Level N
Physical Security	Level N	*Cryptographic Key Management:*	Level N
(Multi-Chip Embedded) EMI/EMC:	Level N	*Self-Tests:*	Level N
Design Assurance:	Level N	*Mitigation of Other Attacks:*	Level N
Operational Environment:	Level N		

Overall Level Achieved <overall level>

The following Approved Algorithms are used:

3.4.1.1 Approved Algorithms

CAVP Cert	**Algorithm and Standard**	**Mode/Method**
No Algorithms Available		

3.4.1.2 Vendor affirmed approved algorithms

Algorithm	**Caveat**	**Use/Function**
No Algorithms Available		

3.4.1.3 Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	**Caveat**
No Algorithms Available	

3.4.1.4 Non-Approved Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	**Caveat**	**Use/Function**
No Algorithms Available		

3.4.1.5 Security function implementation (SFI)

Name	**Type**	**Description**	**SF Properties [O]**	**Algorithms/CAVP Cert**
No Security function implementations Available				

3.4.1.6 Entropy Certificates

Vendor Name	Certificate Number
No Entropy Certificates Available	

3.4.1.7 Non-Approved Algorithms Not Allowed In the approved Mode of Operation

Algorithm/Function	Use/Function
No Non-Approved Algorithms Not Allowed In the approved Mode of Operation Available	

Overall Level Achieved: 1

Signed on behalf of the Government of the United Signed on behalf of the
Government of Canada

Signature:_______________________________________
Signature:_______________________________________
Dated:___________________________________
Dated:___________________________________

Chief, Computer Security Division Director, Industry Program
Group
National Institute of Standards and Technology Communications Security
Establishment

3.5 Security Policy

This section is under construction and will change with the update of Security Functions.

1) Security Policy Page

We need a link that says generates security policy. In the “Security Policy” page is a table like this with Security Levels generated form the Security Levels on the Vendor.txt page.

a. Title Page

[Company Name]

[Product name]

FIPS 140-2 Non-Proprietary Security Policy

Mapping to the report

b. TE.02.03.01 should contain a pulldown for type**.**

i. Software

ii. Hardware
iii. Firmware
iv. Hybrid Software
v. Hybrid firmware

c. **TE.06.03.01** shall contain a table from the levels as described below ():

d. **TE.02.03.02** Also a table needs to be created as part of the input for [For Software/Firmware/Hybrid Module]

B.2.2 Cryptographic module specification

● Hardware, Software, Firmware, or Hybrid designation:

o For software, firmware, and hybrid cryptographic modules, list the operating system(s) the module was tested on and the operating system(s) that the vendor affirms can be used by the module.

Depending on what the Type in the vendor.txt page

e. **TE.02.20.01** add a data entry of all security functions with specific key strengths employed for approved services, as well as the implemented modes of operation (e.g. CBC, CCM), if appropriate.

TE.02.20.02 add data entry table for Non-Approved algorithms in the Approved Mode of Operations

a. Crypto Module Interfaces

B.2.3 Cryptographic module interfaces

● Table listing of all ports and interfaces (physical and logical).

● Define the information passing over the five logical interfaces.

● Specify physical ports and data that pass over them.

Related TEs **TE.02.20.02**

a. add data entry table for Non-Approved algorithms in the Approved Mode of Operations with no Security Claimed.

3.6 Help

The Help page provides useful links and other helpful information related to the CMVP submission process.

Contact us for help at CMVP@nist.gov

Useful links:

- CMVP Program: https://csrc.nist.gov/projects/cryptographic-module-validation-program
- Accredited labs: https://csrc.nist.gov/Projects/testing-laboratories
- Information about the CMVP process: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-management-manual-and-faqs
- Section 4 of the CMVP MM: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual

Documents:

- User's guide (Classic/Non-Br1): https://csrc.nist.gov/projects/cryptographic-module-validation-program/sp-800-140-series-supplemental-information/sp800-140b
- FIPS 140-3 IG: https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips 140-3/FIPS 140-3 IG.pdf

Templates:

- Change letter
- Signature

Release notes:

- Version X.X (Month/Day/Year)

3.7 Save

The Save button allows Users to select Vendor and Report Section files and save them to their local disk. Files are saved with the correct file naming conventions (see Section 3.9.1 – File Naming Requirements). TID-xx- … -V1_vendor.json contains all general information. TID-xx- … -V1_report_section#.json contains all the information from each section of the report. If you are looking for the definition of the schema simply save these files and they will contain the .JSON schema.

3.8 Import

The Import button allows Users to import previously generated and saved Vendor and Report Section files into the current Web Cryptik session. Vendor files can be either JSON or TXT format. Report Section files need to be JSON format.

3.9 Create Package:

The Create Package button provides an interface for building a submission package zip file containing the following files.

1. Assessment Reports
   - <ZIP FILE NAME>_report.pdf
2. Vendor File
   - <ZIP FILE NAME>_vendor.json
3. Reports:
   - <ZIP FILE NAME>_report_sectionx.json (14 files)
   - <ZIP FILE NAME>_report.txt
4. Security Policy
   - ZIP FILE NAME>_140sp.pdf
5. Draft Certificate:
   - ZIP FILE NAME>_140crt.pdf
6. Change Document:
   - <ZIP FILE NAME>_change_document.pdf
7. Signature
   - <ZIP FILE NAME>_signature.pdf
8. Physical Report (mandatory at Physical Security Levels 2, 3 and 4)
   - <ZIP FILE NAME>_physicalReport.pdf
9. Comments:
   - <ZIP FILE NAME>_comments.doc
10. Signed Letter of Affirmation (ITAR)
    - <ZIP FILE NAME>_???

The Assessment Reports, Vendor File, Reports, and Draft Certificate file types are auto generated by Web Cryptik. The remaining files can be added to the package via the provided Add file utilities. The Signature and Change Document templates are located on the Help page of Web Cryptik.

NOTE: .doc documents can be substituted with .docx or .rtf if desired.

NOTE: it is the labs responsibility to ensure that a typical submission package is within the limits allowed (i.e., total combined file sizes cannot exceed 25MB).

3.9.1 File Naming Requirements

Zip files shall be named in accordance with the format provided below.

Format Example: TID-16-0001-0000-**VI**-ACME-100921-V1

Format Definition: TID-[Lab Code]-[NIST TID #]-[CCCS TID #]-[Transaction Type]-[Vendor Name]-[Date]-[Version]

Lab Code: The 2-digit LC designations can be found at https://www-s.nist.gov/niws/index.cfm?event=directory.search#no-back

NIST TID #: is the NIST assigned TID

CCCS TID #: is the CCCS assigned TID or 0000 for IUT submission types

or [ITAR (for ITAR reports not reviewed by CCCS)]

Transaction Type: See FIPS 140-3 Transaction Types and their definitions provided in Section 2.1 – Basic Transaction Types.

Vendor Name: The first 9 characters of the Vendor Name filling white space with underscore.

Date: YYMMDD

Version: The number of versions sent for each day … generally it is V1 because it is rare to submit more than once a day.

3.9.2 Submission File Content Requirements

The submission shall contain only one attachment (i.e., a single zip file containing one or more supporting documents). The name of the zip file and all the individual files shall have the exact same <ZIP FILE NAME>.

The contents of the zip file will be checked to verify that it contains all the files required for the designated Submission Type and the files are named correctly. These must be individual files and not appended to other files (e.g., physical security cannot be provided within the report.pdf). The documents required with each Submission Type are provided in the following table.

Table 1: Submission Package Files by Transaction Type

Transaction Type	Short Description	Documents								
		1	2	3	4	5	6	7	8	9

		Vendor.txt/.json	Report.pdf/.json	Security Policy	Certificate	Change Document	Signature	Physical Report	Comments (response submission)	Signed Letter of Affirmation (ITAR)
	IUT submissions									
IUTA	Implementation Under Test - Add	R								
IUTB	Implementation Under Test - Billing	R								
IUTC	Implementation Under Test - Cancel	R								
IUTR	Implementation Under Test - Remove	R								
IUTM	Implementation Under Test - Modify	R								
	Reviewed Submission									
FS	Full Submission	R	R	R	R		R	R	R	
UPDT	Update	R	R	R	R	R	R	R	R-	
	Reviewed Submission Follow Up									
FCLC	Draft Cert Approve /Reject								R?	
sCMn	Comments	R	D	D	D	D	R		R+	
	Maintenance Submissions									
VUP	Vendor Update	R	O	-R	O	R	R			
VAOE	Vendor Affirmed Operating Environment	R	O	R	O	R	R		R+	
NSRL	Non-Security Relevant	R	R	R	R	R	R			
ALG	Algorithm Update	R	R	R	R	R	R			
OEUP	Operating Environment Update	R	R	R	R	R	R		R+	
RBND	Rebrand	R	O	R	R	R	R			
PTSC	Port Sub Chip	R	R	R	R	R	R	-R		
CVE	Common Vulnerabilities and Exposures	R	R	R	R	R	R			
TRNS	Algorithm Transition	R	R	R	R	R	R			
PHYS	Physical Enclosure	R	R	R	R	R	R	-R		
	Status submissions									
DRPT	Drop report	R								
RQFG	Request for guidance	R								
STAT	Query report status	R								
OTHR	Other	R								
Notes:	R = Required R+ = Required After Initial Submission -R = Required for Physical Security Level 2+ O = Optional D = Depending on Initial Submission Requirements									

3.10 Send Results

The Send Results button provides a Secure Log In window where a user will be able to login to their BOX account to complete the submission process.

Appendix A Security Statement

This Go-Live Security Assessment Report (SAR) covers the scope of a new website (https://cryptic.nist.gov:8443) within the Computer Security Division (CSD), as well as, the websites integration with the Box service within the website. This website was approved for a pilot between NIST and an external lab on a temporary basis, using non-production Low research data only. The pilot began in September 2020, is ongoing, and awaiting approval for full deployment to use Moderate data in production. No significant security issues were identified during the pilot.

The website has been developed to support retrieval of FIPS 140-3 submissions at NIST. This process is occurring within CSD (for FIPS 140-2), however; currently a laboratory sends a PGP encrypted file to CSD. This website will leverage Box integration for secure transmission of files through the Cryptik website replacing the need to send the files through email. These files are retrieved from the Box service every 24-hours, deleted from the Box server, and then processed internally on a CSD protected network. The internal processing of this data is an ongoing process with an existing ATO and is not included within the scope of this go-live deployment.

The hosting server is an existing Windows Server that resides within AWS that was assessed and approved for the Automated Cryptographic Validation Protocol (ACVP). The server was deployed using OISM-supplied Windows Server 2012 R2 AMI. Cryptik runs on a dedicated EC2 instance on the server.

The Platform Services Division (PSD) will manage the Box security configurations for this project. CSD staff will manage the individual folder access permissions created for external lab submission of data. There are 3 staff in CSD with access to read/write/modify lab data submissions. NIST staff signing into Box will use Single Sign On (SSO) for authentication. External lab accounts connecting to Box must follow the account creation setup process consisting of exchanging certificates with CSD to access the Cryptik website.

The overall security categorization for this deployment is Moderate, with CIA impact levels of M/M/L (Moderate confidentiality for company proprietary information, Moderate integrity to ensure accurate validation is performed on the submissions, and Low for availability as the validations can take months to complete).

General Box authorization information:

- Box has a FedRAMP Moderate authorization for Government use and is in the process of undergoing a High FedRAMP assessment for use within the defense industry.
- Box has been approved for a Moderate use-case within NIST Engineering Laboratory (EL), however; it has not been approved enterprise wide for Moderate use. This go-live assessment and approval is specific to the Cryptik use-case only.

Key security enhancements identified and implemented during the pilot security assessment include:

- No sensitive data will be stored on the Cryptik website. All sensitive data is stored on Box. In the event of a website compromise, the attacker would not have access to the proprietary information, however; this would lead to embarrassment and potential loss of reputation for NIST and the FIPS 140-3 program.
- CSD has generated a script to retrieve and delete files submitted to Box every 24-hours. This minimizes the impact of any compromise of the Box server limiting to files only submitted within the last 24-

hours. Additionally, all files stored on the Box server itself are encrypted with FIPS validated encryption at rest and all communication with Box requires TLS 1.2 or higher level of encryption.

- External access to the website requires a NIST generated certificate implementing the use of mTLS. Without this certificate, external access is denied.
- Only 3 staff within CSD will have access to sensitive data stored on the Box service. There access will be reviewed at least annually or on an as needed basis.
- All users of the website will be laboratories with existing NIST relationships that have undergone National Voluntary Laboratory Accreditation Process (NVLAP: https://www.nist.gov/NVLAP). This is ~20 external laboratories so the userbase of the website is small and limits exposure to the general public.
- All Box account security configurations have been modified by OISM to enforce NIST password policy requirements and configured to require the use of two-factor authentication.
- The website has been scanned multiple times with Webinspect and vulnerabilities have been remediated and/or validated to be false positives.
- The hosting server has been scanned multiple times with Tenable and vulnerabilities have been remediated and/or validated to be false positives.
- All files submitted to Box are stored on Box servers using FIPS validated encryption.

Appendix B Submission Scenario Mapping to 140-2

The following is a mapping of the FIPS 140-3 submission scenarios compared to the FIPS 140-2 and original FIPS 140-3 submission types.

Submission Types			
NEW 140-3	**140-3 Long Name**	**140-2**	**140-3 (original)**
VUP	Vendor Update	1 (Option 1)	VU
VAOE	Vendor Affirmed Operating Environment	~~N/A~~	VU
NSRL	Non-Security Relevant	1 (Option 2)	UP
ALG	Algorithm Update	1 (Option 3)	OE
OEUP	Operating Environment Update	1 (Option 4)	OE
RBND	Rebrand	1A (Option 1)	UP-OEM (OEM)
PTSC	Port Sub Chip	1A (Option 2)	OE
REMOVED		~~1B~~	~~N/A~~
REMOVED		~~2~~	~~QU~~
UPDT	Update	3	UP
CVE	Common Vulnerabilities and Exposures	3A	QU
TRNS	Algorithm Transition	3B	QU
PHYS	Physical Enclosure	4	QU
FS	Full Submission	5	FS

Appendix C Document Change Log

After an initial series of reviews and document updates, the 08 March 2023 instance of the Web Cryptik User's Guide has been established as Version 1.0. Future changes to the document will be summarized in the following list to provide a change log history of the guide. Changes will be listed in date-ascending order.

- Version 1.0 (08 March 2023)
  - Baseline version
- Version 1.1 (2 August 2023)
  - Added examples to the SFI Table and modified surrounding text.
- Version 1.2 (16 January 2024)
  - Updated Introduction sub-sections to clarify and correct guidance related to certificates and Box account usage.
- Version 1.3 (29 March 2024)
  - Removed caveats from the document and pointed to the CMVP webpage.
  - Other minor clean up.