WEB-CRYPTIK
Br1 USER'S GUIDE

A web-based application for CMVP

Abstract

The Web Cryptik Br1 User's Guide is intended to provide users of the CVMP Web Cryptik Br1 application with clear and comprehensive guidance for accessing and most effectively using Web Cryptik Br1 to generate and submit their module packages.

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

Table of Contents

1 Introduction

Web-Cryptik Br1 is a web-based application for the Labs to create and submit their CMVP submissions to NIST.

1.1 Getting Started

Web-Cryptik Br1 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 Br1

This section provides the instructions and steps to request access to the Web-Cryptik Br1 application.

The Web-Cryptik Br1 URL is https://cryptik.nist.gov:8444 (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:

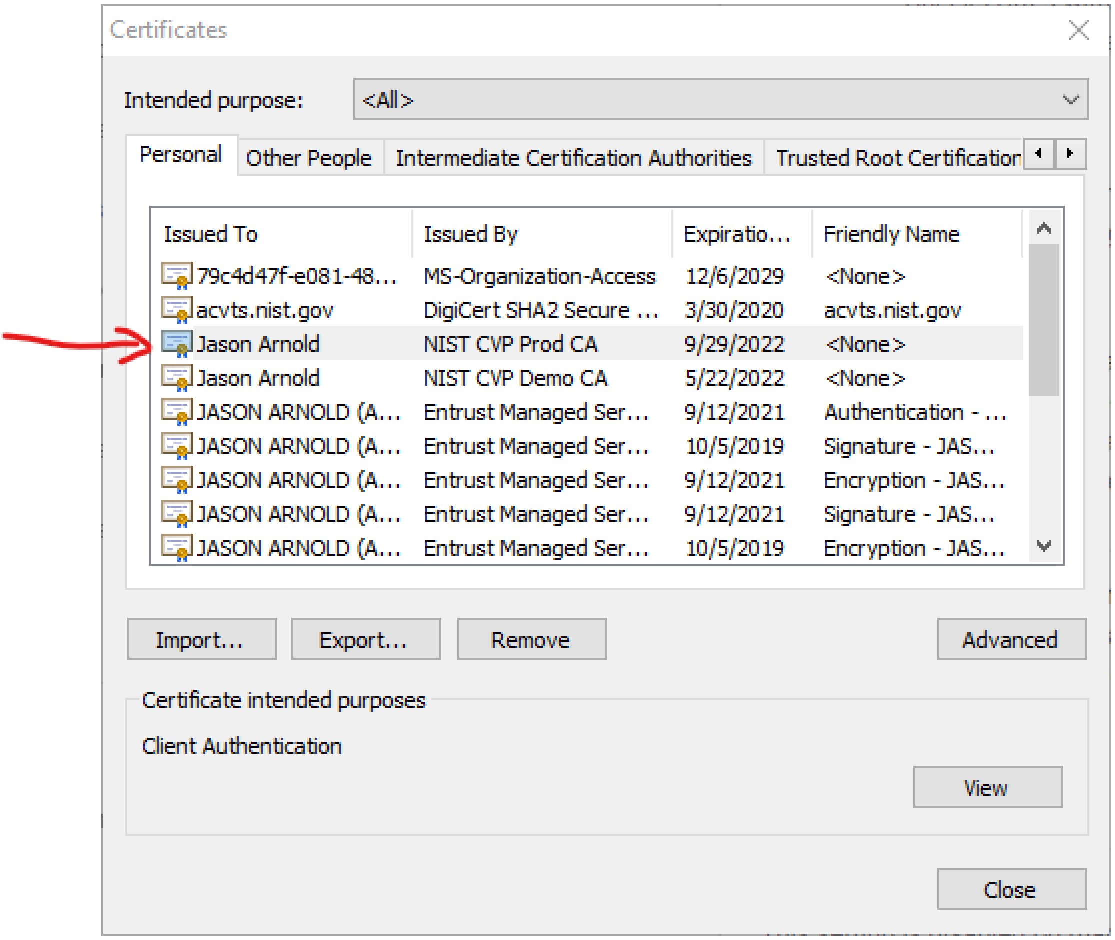
```
# receive back certificate from NIST

# 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.



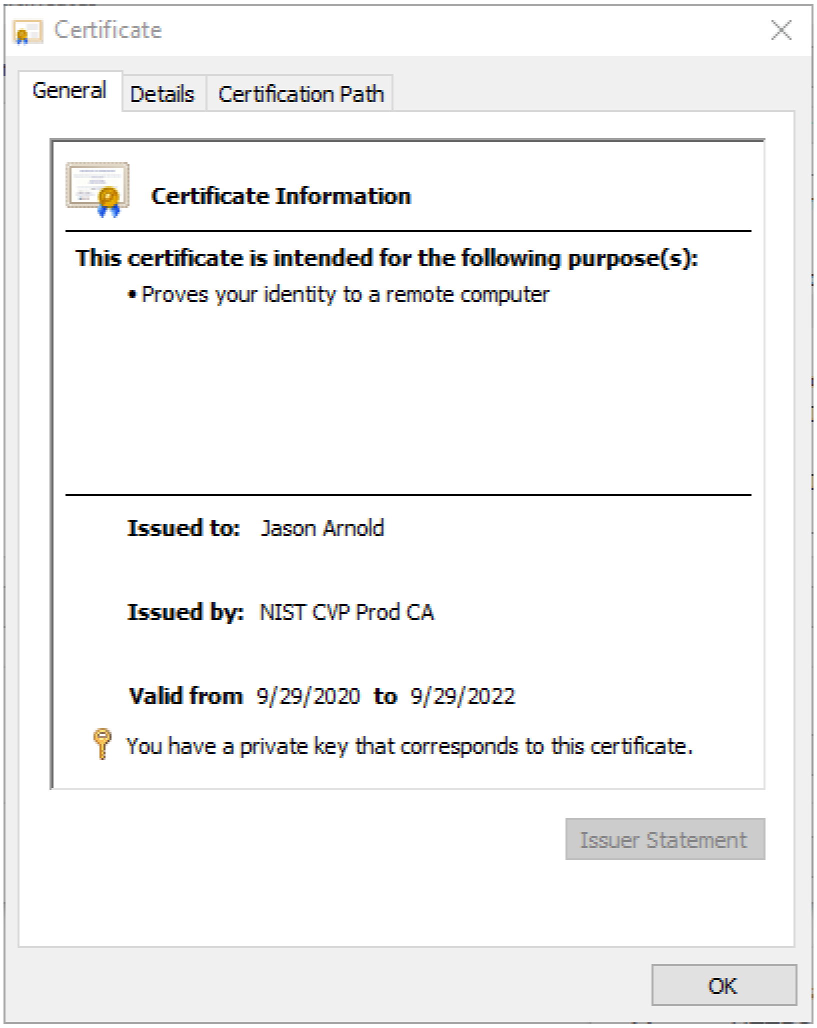
Intended purpose: <All>

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 Br1 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.



Certificate Information

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 Br1 certificates, so that should be what is shown in your pop-up window.

1.5 Creating a BOX Account for Web-Cryptik Br1

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 look at these folders by logging 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 Br1 Overview

Web-Cryptik Br1 is a file creation and submission system. All transactions through Web-Cryptik Br1 are into NIST. All transactions back to CSTL originate from Resolve via PGP email and are outside the scope of this documentation.

Web-Cryptik Br1 is intended to support the various submissions listed in Section 4.3 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual. Users are required to specify their Transaction Type, and if appropriate, the related Scenario information in the Module Information portion of the General Info screen. The remaining Web-Cryptik Br1 data entry fields are subsequently customized to fit the selected Transaction Type.

(Note: Detailed definitions and the rules associated with each Submission Scenario are contained in Section 7.1 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual. Users are encouraged to review this material to better understand the content and process flow distinctions between the different scenarios.)

Web-Cryptik Br1 provides Save and Import utilities to facilitate the creation and revision of submission packages. Once the user is satisfied with the completeness and correctness of their submission data, the Create Package and Send utilities are provided to generate the completed package and send it to NIST via the Box process.

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. LC – Lab Code [pre-filled by Laboratory Information page]
3. Lab internal ID
4. Signature 1 *
5. Title 1*
6. Signature 2
7. Title 2
8. Signature 3
9. Title 3
10. Tester 1*
11. CVP Number 1*
12. Tester 2
13. CVP Number 2
14. Tech Reviewer 1*
    - Should include the CVP (unless separate field is defined for this available).
15. Tech Reviewer 2

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 (POC1)*
12. Email 1*
    - Check formatting
13. Phone 1*

    - Check formatting

14. Fax 1
    - Check formatting
15. Contact 2 (POC2)
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 scenarios listed in Section 4.3 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual, as well as Implementation Under Test (IUT), Approve and Reject selections. The most common selection is Full Submission.

The IUT options are:

- 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

The Approve and Reject options are used for Labs to approve or reject a Draft Certificate that has been sent to them.

- Transaction Code *

  Value is inherited from the Transaction Type selection and is only displayed if the initial Transaction Type selection is one of the Implementation Under Test (IUT).

- Scenario (s)

2. CSTL TID*
    - Check formatting

3. CCCS TID*
    - Defaults to grayed out 0000 for non-ITAR submissions and ITAR for ITAR submissions.

4. Module Name(s)*
    - 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.

5. FIPS Version* (Auto set to FIPS 140-3)

6. Module Count*
    - A number. See FIPS 140-3 – CMVP Management Manual Section 7.7 (Module count definition).

7. Module Description*

    Referenced by: [ref. TE02.03.01]

8. 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.

9. 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.]

10. Operational Environment Type*:
    - Modifiable
    - Limited
    - Non-Modifiable

11. 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 FIPS 140-3 – CMVP Management Manual Section 7.5 (Partial validations and non-applicable areas)

12. Administrative Flags
    - ITAR
    - Add Module to MIP List

13. Cert Caveat: the specific stipulations that make this certificate valid.
    - List of potential caveats.
    - This caveat may be modified or expanded by the CMVP during the validation process.

14. PIV Cert #
    - The cert number related to PIV validation.
    - 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 FIPS 140-3 – CMVP Management Manual Section 7.6 (CMVP requirements for PIV validations)

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

3.1.4 CAVP Certs

The CAVP Certs functionality provides a utility for locating and including relevant CAVP certification information within the submission package. The basic process flow for finding and including the desired algorithm certification information is listed below.

- Use the Search functionality to retrieve ACVP certifications for a given vendor.
- Add the desired algorithm certifications by selecting the + symbol in the Action column of the CAVP Results table for each desired algorithm.
- Repeat the previous two steps as needed to add algorithm certifications from different vendors.
- Select the Build OEs button beneath the Added CAVPs table to show the OEs associated with the added algorithm certifications.
- Use the checkboxes within the OEs table to select the desired OEs.
- Use the Algorithms Search functionality to retrieve the OE ID and Algorithm name for the selected CAVP Cert.
- Use the + symbol or Add all button to be able to edit the Capabilities associated with the algorithm. A secondary table containing the Implementation description for the algorithm will also be displayed.
- Repeat the previous two steps as necessary until all desired algorithms have been added.

If the ITAR option is selected within Module Information, a CAVP ITAR Algorithms table appears at the top of the CAVP Certs page, allowing users to manually enter their ITAR algorithms.

3.1.5 MIS Tables

The MIS Tables capture the data set forth in NIST SP 800-140-Br1. The tables are appropriately customized based on the Module Type specified on the Module Information screen. A detailed description of each table and guidance for correctly filling out the tables can be found in the MIS Table Descriptions document located on CSRC at https://csrc.nist.gov/projects/cmvp/sp800-140b.

3.1.6 Supplemental Information

Supplemental Information provides a series of Yes/No questions about the module being submitted for review. The questions are organized into sections corresponding to the different Module Requirement reports (e.g., General, Cryptographic Module Specification, Cryptographic Module Interfaces).

3.2 Reports

The Reports section is organized into the 12 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

All Report subsections 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 evaluation item.
- Reset All to Open → Used to clear all Test Status selections and reset them to Open.

3.3 References

The Reference tab is used to create reference documents that can be referred to when filing out individual evaluation items within the Reports section. References are created by entering the Title of the desired reference and then using the + icon within the Actions column to add the reference. Added references can be subsequently edited or deleted as needed.

3.4 Help

The Help page provides links to web pages and documents related to the CMVP submission process. A replica of the Help page and the associated links are provided below.

Help:

- Contact us for help at web-cryptik@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 Management Manual: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual

Documents:

- User's Guide: https://csrc.nist.gov/projects/cmvp/sp800-140b

Release Notes:

- Release Notes: https://cryptik.test.nist.gov:8444/release-notes

3.5 Save

The Save button allows Users to select Module and Report Section files and save them to their local disk. All files are saved in JSON format. The files are saved with the correct file naming conventions (see Section 3.8.1 – File Naming Requirements). The TID-xx- … -V1_module.json file contains the content provided in all sub-sections of General Info. The TID-xx- … -V1_report_section#.json files contain all information entered for that report section. If you are looking for the definition of the schema, simply save these files and they will contain the JSON schema.

3.6 Import

The Import button allows Users to import previously generated and saved Module and Report Section files into the current Web-Cryptik Br1 session. All imported files need to be JSON format.

3.7 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. Module File
   - <ZIP FILE NAME>_module.json
3. Reports:

   - <ZIP FILE NAME>_report_sectionx.json (14 files)
   - <ZIP FILE NAME>_report.txt
4. Change Letter:
   - <ZIP FILE NAME>_change_letter.pdf
5. Signature
   - <ZIP FILE NAME>_signature.pdf
6. Physical Report (mandatory at Physical Security Levels 2, 3 and 4)
   - <ZIP FILE NAME>_physicalreport.pdf
7. Comments:
   - <ZIP FILE NAME>_comments.doc
8. Security Policy:
   - <ZIP FILE NAME>_securitypolicy.doc
9. Signed Letter of Affirmation (ITAR)
   - <ZIP FILE NAME>_???

The Assessment Reports, Module File, Reports, and Draft Certificate file types are auto generated by Web Cryptik Br1. 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 Br1.

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).

3.7.1 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.

3.7.2 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									

3.8 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 its 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 and CRADA

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

This 22 January 2024 instance of the Web Cryptik Br1 User's Guide is the baseline version corresponding to the initial full public release of Web Cryptik Br1. 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.

- Br1 Version 1.0.0 (29 January 2024)
  - Baseline version