

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.

Hawes, David J. (Fed)
david.hawes@nist.gov

Table of Contents

1	Introduction.....	4
1.1	Getting Started	4
1.2	Accessing Web Cryptik	4
1.3	Installing a Certificate in Chrome	5
1.4	Creating a BOX Account for Web Cryptik	6
2	Web Cryptik Br1 Overview	8
3	Graphical User Interface (GUI) Functionality	9
3.1	Home	9
3.2	Validation.....	9
3.2.1	New Validation & INTU	9
3.2.1.1	General Info.....	9
3.2.1.1.1	Laboratory Information	9
3.2.1.1.2	Vendor Information	9
3.2.1.1.3	Module Information	10
3.2.1.1.4	CAVP Certs	12
3.2.1.1.5	MIS Tables.....	13
3.2.1.1.6	Supplemental Information	13
3.2.1.2	Reports	13
3.2.1.3	References.....	14
3.2.2	Revalidation	14
3.2.2.1	Vendor Update (VUP).....	14
3.2.2.2	Vendor Affirmed Operation Environment (VAOE)	14
3.2.2.3	Rebrand (RBND)	15
3.2.2.4	Operating Environment Update (OEUP)	15
3.3	Help.....	16
3.4	Cancel Validation	16
3.5	Actions – New Validation & INTU	16
3.5.1	Save.....	16
3.5.2	Import	16
3.5.3	Import INTU	16
3.5.4	Create Package:	17
3.5.5	Create INTU Package:	17

3.5.6	Send Results.....	17
3.6	Actions – Revalidation	18
3.6.1	Save.....	18
3.6.2	Import	18
3.6.3	Create Package:	18
3.6.4	Send Results.....	18
4	File Naming Conventions.....	18
5	Submission File Content Requirements	19
Appendix A: Security Statement.....		22
Appendix B: Submission Scenario Mapping to 140-2 and CRADA.....		24
Appendix C: Document Change Log		25

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 Accessing Web Cryptik

Here are the instructions and steps to request access to the Web Cryptik Br1 application.

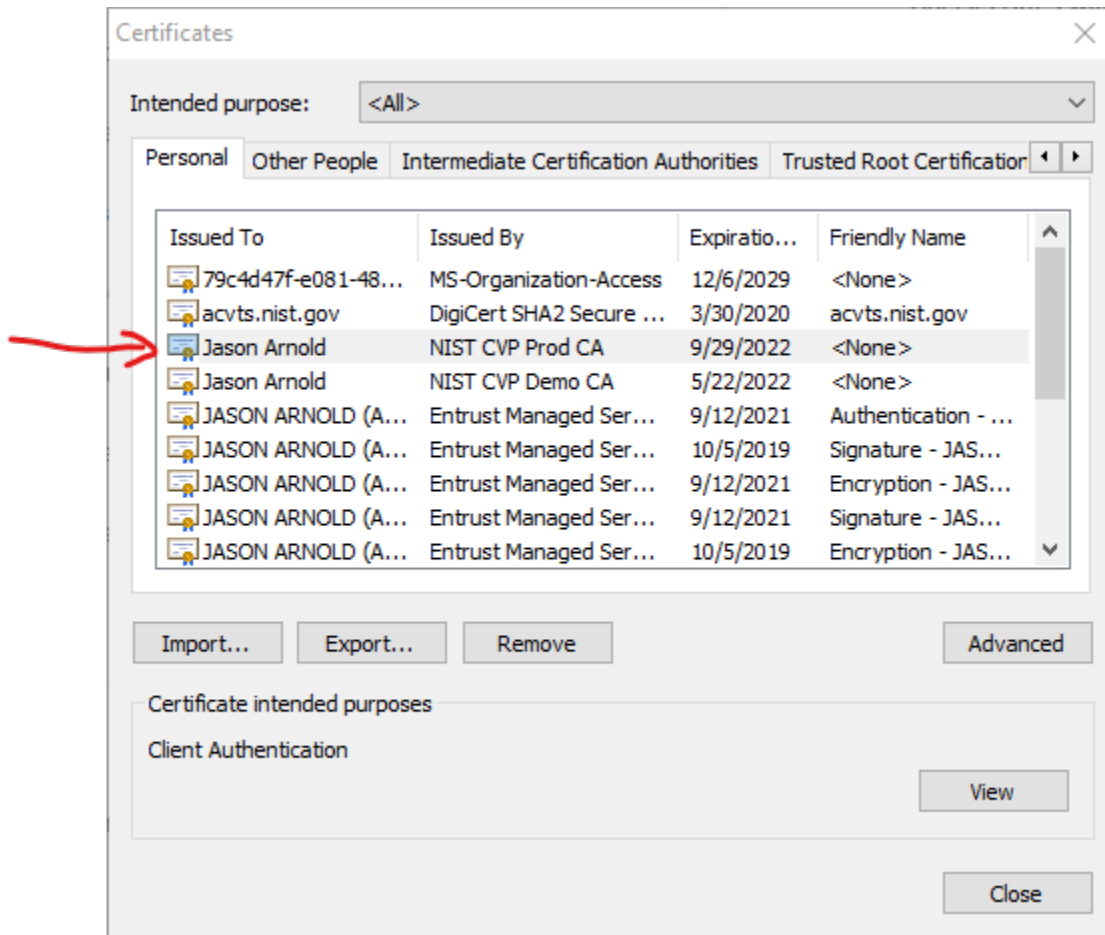
The Web Cryptik Br1 URL is <https://cryptik.nist.gov:8444> (mTLS is required to access).

Users should contact their lab manager to request the Lab's Production credential to access Web Cryptik Br1.

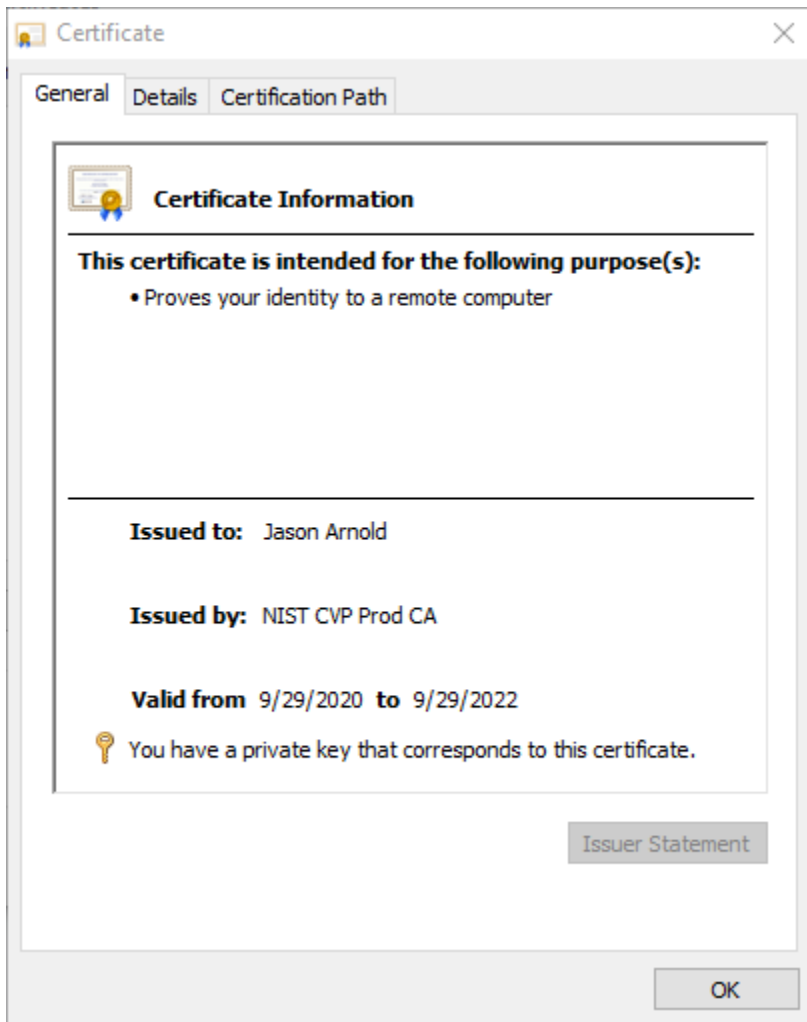
Users may email cryptik-support@nist.gov to request to be added to a "Cryptik Maintenance" notification list. Use of the list will be limited to sending out deployment, outage and maintenance notifications, so the frequency of emails is quite low. However, if users prefer not to receive such notifications, please notify NIST accordingly and the specified email address(es) will be removed.

1.3 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.



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.



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

1.4 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 in 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 set up 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, or 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 review 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 covered in Section 7.1 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual. In version 2.0.0 and subsequent releases of Web Cryptik Br1, users first need to select whether they're generating a New Validation or Revalidation. (Note: The New Validation option is also used for Interim Update (INTU) requests.)

Selecting the New Validation option and clicking on the Start Validation button will re-direct the user to the General Info screen where they can begin entering the required data for their submission. 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.

Starting a Revalidation will present the user with a Revalidation Scenario selection box. Making a scenario selection prompts the user for a Transaction Type and subsequently a Revalidation Certificate number. Searching on the selected certificate retrieves the current data associated with that certificate and populates the data entry tables needed for the selected scenario.

(Note: Section 7.1 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual contains detailed definitions and rules associated with each of the supported Submission scenarios. 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 Results 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 Home

The Home page clarifies when to use the Br1 tool versus the non-Br1 tool. The page also contains links to related information.

3.2 Validation

The Validation screen is used to select and start either a New Validation or a Revalidation. Interim Updates (INTUs) are processed via the New Validation workflow.

3.2.1 New Validation & INTU

Starting a New Validation & INTU re-directs the user to the General Info screen where they can begin entering the data required for their submission.

3.2.1.1 General Info

Required info is marked with a double asterisk **.

3.2.1.1.1 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

3.2.1.1.2 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/Province
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

3.2.1.1.3 Module Information

1. Transaction Type **

Defines the type of submission and controls the files generated during the Create Package process. The most common selection is Full Submission. Other currently supported selections are various Implementation Under Test (IUT) requests and several Processing Support items.

The remaining scenarios covered in Section 7.1 (Submission Scenarios) of the FIPS 140-3 – CMVP Management Manual are currently under development for inclusion within Web Cryptik Br1. In the interim, these scenarios are requested and processed manually without the use of the Cryptik application.

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 Processing Support items are:

- sCMn - CMVP Comments or Returned CSTL Addressed Comments

- Drop Submission - CSTL Request to Drop Report
- ECR Accept: Extended Cost Recovery
- ECR Reject
- STAT - Query Report Status
- OTHR - Other
- Draft Certificate Approve
- Draft Certificate Reject

A required Transaction Code field is also displayed if the user selects one of the IUT items. The Transaction Code value is inherited from the Transaction Type selection. A Scenario (s) field also appears for the IUTA and IUTB selections. The Scenario (s) field is an optional freeform text box

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 Standalone

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.

3.2.1.1.4 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 Certificates table to show the OEs associated with the added algorithm certifications.
- Use the checkboxes within the OEs table to select the desired OEs.
- A Tested Algorithms table is built containing the CAVP Cert Name, OE ID and Algorithm for the selected OEs.
- Use the + symbol or Add all button within the Tested Algorithms table generate an Implemented Algorithms by OE table. This table can be used to be able to edit the Capabilities associated with the algorithm or to delete unwanted entries.
- A secondary table, Implemented Algorithms by CAVP Cert, containing the Implementation description for the algorithm will also be displayed.
- Repeat the previous editing steps as necessary until all desired algorithms have been added.
- Click on the Save Algorithms button to save your algorithm selections.
- Use the Update MIS Tables button in incorporate your algorithm selections into the appropriate portions of the MIS Tables.

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.

3.2.1.1.5 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>.

3.2.1.1.6 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).

3.2.1.2 Reports

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

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.

3.2.1.3 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.

3.2.2 Revalidation

Starting a Revalidation presents the user with a Revalidation Scenario selection box. Making a scenario selection yields the necessary data entry fields needed for the selected scenario. The currently supported Br1 revalidation scenarios are listed below. The remaining scenarios will be added in subsequent Br1 release updates.

- Vendor Update (VUP)
- Vendor Affirmed Operating Environment (VAOE)
- Rebrand (RBND)
- Operating Environment Update (OEUP)

3.2.2.1 Vendor Update (VUP)

Upon selecting the VUP scenario, the user is prompted to select a Transaction Type and subsequently enter their desired Revalidation Certificate number. The only supported Transaction Type for a VUP is Initial Submission (IS). Clicking the Search button will retrieve the current information for the specified certificate and populate the Vendor and Module data fields eligible for updating. A blank Laboratory Information section is also provided in case the user wishes to provide updated laboratory information. Note that the CSTL TID and Lab Name fields require an entry.

Once the desired updates are completed, the Save action can be used to save work in progress, or the Create Package action can be used to download a Transaction zip file that can be subsequently submitted to NIST via a Send Results action. The zip file contains a properly formatted Json file customized for the given scenario.

3.2.2.2 Vendor Affirmed Operation Environment (VAOE)

Upon selecting the VAOE scenario, the user will be prompted to select a Transaction Type and subsequently enter their desired Revalidation Certificate number. The only supported Transaction Type for a VAOE is Initial

Submission (IS). Clicking the Search button will retrieve the current information for the specified certificate and populate the Module and MIS Tables data fields eligible for updating. A blank Laboratory Information section is also provided in case the user wishes to provide updated laboratory information. Note that the CSTL TID and Lab Name fields require an entry.

Once the desired updates are completed, the Save action can be used to save work in progress, or the Create Package action can be used to download a Transaction zip file that can be subsequently submitted to NIST via a Send Results action. The zip file contains a properly formatted Json file customized for the given scenario.

3.2.2.3 Rebrand (RBND)

Upon selecting the RBND scenario, the user will be prompted to select a Transaction Type and subsequently enter their desired Revalidation Certificate number. Transaction Type options for a RBND are:

- Initial Submission (IS),
- Lab Resubmission (RSUB),
- Lab Comment Response (LCOM),
- Drop Submission (DRPT),
- Approve Final (APRV), and
- Reject Final (RJCT)

Clicking the Search button will retrieve the current information for the specified certificate and populate the Vendor, Module, and MIS Tables data fields eligible for updating. A blank Laboratory Information section is also provided in case the user wishes to provide updated laboratory information. Note that the CSTL TID and Lab Name fields require an entry.

Once the desired updates are completed, the Save action can be used to save work in progress, or the Create Package action can be used to download a Transaction zip file that can be subsequently submitted to NIST via a Send Results action. The zip file contains a properly formatted Json file customized for the given scenario.

3.2.2.4 Operating Environment Update (OEUP)

Upon selecting the OEUP scenario, the user will be prompted to select a Transaction Type and subsequently enter their desired Revalidation Certificate number. Transaction Type options for a OEUP are:

- Initial Submission (IS),
- Lab Resubmission (RSUB),
- Lab Comment Response (LCOM),
- Drop Submission (DRPT),
- Approve Final (APRV), and
- Reject Final (RJCT)

Clicking the Search button will retrieve the current information for the specified certificate and populate the Vendor, Module, and MIS Tables data fields eligible for updating. A blank Laboratory Information section is also provided in case the user wishes to provide updated laboratory information. Note that the CSTL TID and Lab Name fields require an entry.

Once the desired updates are completed, the Save action can be used to save work in progress, or the Create Package action can be used to download a Transaction zip file that can be subsequently submitted to NIST via a Send Results action. The zip file contains a properly formatted Json file customized for the given scenario.

3.3 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>
- CMVP FIPS 140-3 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.nist.gov:8444/release-notes>

3.4 Cancel Validation

The Cancel Validation button can be used to clear the content in either the New Validation or Revalidation screens and reload the site. Upon selecting Cancel Validation, the user will be prompted to confirm or cancel the reload site request. Reloading the site will return the user to the Notice & Consent pop-up and subsequently the Validation screen.

3.5 Actions – New Validation & INTU

When working on a New Validation & INTU, the Actions button provides a dropdown selector for the available Save, Import, Import INTU, Create Package, Create INTU Package, and Send Results utilities.

3.5.1 Save

The Save utility allows Users to select Module and Report Section files and save them to their local disk. All files are saved in JSON format with the correct file naming conventions.

3.5.2 Import

The Import utility allows Users to import previously generated and saved Module and Report Section files into the current Web Cryptik Br1 session. Module and Report Section files need to be JSON format. Zip files containing properly formatted JSON files can also be selected for import.

3.5.3 Import INTU

The Import INTU utility allows Users to import previously generated and saved Transaction and Report Section files into the current Web Cryptik Br1 session. Transaction and Report Section files need to be JSON format. Zip

files containing properly formatted JSON files can also be selected for import.

3.5.4 Create Package:

The Create Package utility provides an interface for building a submission package zip file containing the following required and optional files. Required files are noted with an *.

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 Document:
 - <ZIP FILE NAME>_change_document.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. Entropy Report:
 - <ZIP FILE NAME>_entropyreport.pdf
8. Comments:
 - <ZIP FILE NAME>_comments.doc
9. Security Policy Template*:
 - <ZIP FILE NAME>_sptemplate.doc

The Assessment Reports, Module File, and Reports are auto generated by Web Cryptik Br1. The remaining files can be added to the package via the provided Add file utilities. Change Document and Signature document templates can be found on the 140B webpage (<https://csrc.nist.gov/projects/cmvp/sp800-140b>).

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

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

3.5.5 Create INTU Package:

The Create INTU Package utility provides an interface for building an INTU submission package zip file. The required and optional file contents for the INTU package are the same as listed in the previous section, with one exception. The INTU package contains a Transaction file instead of a Module file.

3.5.6 Send Results

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

3.6 Actions – Revalidation

When working on a Revalidation, the Actions button provides a dropdown selector for the available Save, Import, Create Package, and Send Results utilities.

3.6.1 Save

The Save utility allows Users to save a properly named and formatted zip file of their Revalidation content.

3.6.2 Import

The Import utility allows Users to import a saved zip file containing the contents of an in-progress or previously worked Revalidation.

3.6.3 Create Package:

The Create Package utility provides an interface for building a Revalidation package zip file. Required and optional package content vary based on Revalidation Scenario and Transaction Type, as do the applied file naming conventions.

3.6.4 Send Results

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

4 File Naming Conventions

The file naming conventions used vary slightly between a New Validation, an INTU, and a Revalidation.

A format example and corresponding definition for a New Validation are shown below. **Format Example:** TID-16-0001-0000-**FS**-ACME-100921-V1

Format Definition: TID-[Lab Code]-[CSTL 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>

CSTL TID #: is the NIST assigned TID

CCCS TID #: is the CCCS assigned TID

or 0000 for IUT submission types

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.

A format example and corresponding definition for an INTU are as follows.

Format Example: TID-16-0001-INTU-IS-ACME-2603271002

Format Definition: TID-[Lab Code]-[CSTL TID #]-[INTU]-[Transaction Type]-[Vendor Name]-[DateTime]

The field descriptions are the same as previously described for a New Validation, except the DateTime field, which uses a YYMMDDHHMM format.

A format example and corresponding definition for a Revalidation are as follows.

Format Example: TID-15-0327-RBND-IS-2603271002

Format Definition: TID-[Lab Code]-[CSTL TID #]-[Reval Scenario]-[Transaction Type]-[DateTime]

The field descriptions are the same as an INTU, except the INTU field is replaced with a Revalidation Scenario value and the Vendor Name field is removed.

5 Submission File Content Requirements

A Submission package 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).

In general, the Create Package utility for the various Scenario/Transaction Type combinations has been customized to display the required and optional files allowed for each Scenario/Transaction Type submission. The following table summarizes the content requirements for the different Scenario/Transaction Type submissions.

Table 1: Content Requirements by Scenario/Transaction Type

Note: Documents tagged with [O] are optional. Documents tagged with [C] are to be included only if there are changes from the previous submission. Other listed documents are required.

	IS	RSUB	LCOM	DRPT	APRV	RJCT
VUP	Trns SPTemp					
VAOE	Trns SPTemp					
RBND	Trns SPTemp VenApr Change	Trns SPTemp VenApr Change	Trns SPTemp Com	Trns	Trns	Trns Com
OEUP	Trns SPTemp Change RTL [O]	Trns SPTemp Change RTL [O]	Trns SPTemp Com	Trns	Trns	Trns Com
INTU	TR Trns TRData Change [O] Sig [O] PTR [O] EnRpt [O] Com [O] SPTemp	TBD	TR Trns TRData Com [O] SPTemp	Trns MIS TRData – SecB SPTemp	TR Trns TRData Change [O] Sig [O] EnRpt [O] Com [O] SPTemp	TR Trns TRData Change [O] Sig [O] EnRpt [O] Com [O] SPTemp
FS	TR MIS TRData Change [O] Sig [O] PTR [O] EnRpt [O] Com [O] SPTemp	TBD	TR MIS TRData Com [O] SPTemp	MIS TRData – SecB SPTemp	TR MIS TRData Change [O] Sig [O] EnRpt [O] Com [O] SPTemp	TR MIS TRData Change [O] Sig [O] EnRpt [O] Com [O] SPTemp

The legend for the package contents is provided below.

Name	Code	Filename Info
Transaction	Trns	****_transaction.json
Security Policy Template	SPTemp	****_sptemplate.docx
Remote Testing Letter	RTL	****_remotetesting.pdf
Vendor Approval Letter	VenApr	****_vendorletter.pdf
Change Letter	Change	****_changedocument.pdf
Signature Document	Sig	****_signature.pdf
Comments Document	Com	****_ModuleComments.docx
Physical Test Report	PTR	****_physicalreport.pdf
Entropy Report	EnRpt	****_entropyReport.pdf
Test Report	TR	****_report.pdf
Module Data	MIS	****_module.json
Test Report Data	TRData	****_report_sectionX.json

Appendix A: Security Statement

This Go-Live Security Assessment Report (SAR) covers the scope of the Web Cryptik Br1 website (<https://cryptik.nist.gov:8444>) 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. Their 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>). There are approximately 20 such 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	Operational 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 29 January 2024 instance of the Web Cryptik Br1 User's Guide was the baseline version corresponding to the initial full public release of Web Cryptik Br1. Subsequent changes to the document are summarized below to provide a change log history of the guide. Changes are listed in date-descending order.

- Br1 Version 1.4 (8 July 2026)
 - Removed the Lab Resubmission (RSUB) Transaction Type option from the Vendor Update (VUP) and Vendor Affirmed Operating Environment (VAOE) Revalidation scenarios.
- Br1 Version 1.3 (28 May 2026)
 - Updated the document to reflect the Revalidation scenarios added and other enhancements made with the Br1 v2.0.1 through v2.0.4 release updates.
- Br1 Version 1.2 (6 May 2025)
 - Updated the document to reflect the GUI changes made in Web Cryptik Br1 v2.0.0 to implement Revalidation scenario processing.
- Br1 Version 1.1 (31 January 2025)
 - Updated the certificate creation information to reflect the use of Secure File Collaboration (SFC) instead of nFiles.
 - Minor content changes to account for the Cryptik Br1 release updates and program changes that during 2024.
- Br1 Version 1.0 (29 January 2024)
 - Baseline version