Change Document

Version 1.0

March 15, 2024

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Lab Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NVLAP #: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vendor Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Module Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Submission Scenario: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tester 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CVP # \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tester 2: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CVP # \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tech Reviewer 1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CVP # \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contents

[1. Submission Scenarios 3](#_Toc161415363)

[1.1. Requirements for all revalidations 3](#_Toc161415364)

[1.2. FS 5](#_Toc161415365)

[1.3. VUP 6](#_Toc161415366)

[1.4. VAOE 7](#_Toc161415367)

[1.5. NSRL 8](#_Toc161415368)

[1.6. ALG 9](#_Toc161415369)

[1.7. OEUP 10](#_Toc161415370)

[1.8. RBND 11](#_Toc161415371)

[1.9. PTSC 13](#_Toc161415372)

[1.10. UPDT 15](#_Toc161415373)

[1.11. CVE 17](#_Toc161415374)

[1.12. TRNS 19](#_Toc161415375)

[1.13. PHYS 24](#_Toc161415376)

[2. Certificate Modification Tables 25](#_Toc161415377)

[3. Affected TEs and Security Policy Changes 26](#_Toc161415378)

[4. Predefined Regression Testing 27](#_Toc161415379)

CSTL **shall** fill in all applicable tables under “CSTL Compliance evidence / justification”.

# Submission Scenarios

Please review the below tables and requirements within the context of the FIPS 140-3 Management Manual Section 7.1 requirements.

* 1. Requirements for all revalidations

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The purpose of the revalidation (scenario, objective, etc.) with reference to applicable guidance (e.g., Section(s) within Management Manual Submission Scenarios 7.1). |  |
| The CSTL is responsible for an independent evaluation of the impacts throughout the module requirements for any change and performs any testing needed prior to submission. The CSTL **shall** address all affected TEs and the CSTL’s assessment. |  |
| Summary of the modifications (e.g., changes made to the module code, documentation, etc.). |  |
| Indicate whether the modified cryptographic module replaces the previously validated module or adds to it.  |  |
| If the individual section(s) is being lowered as part of the revalidation, this is considered security relevant and the module may be submitted as a UPDT with full testing on the individual section(s) that is being lowered.If the individual section(s) is being raised or if the physical embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and **shall** undergo full validation testing by a CSTL and submitted as an FS. |  |
| It is not possible to combine any revalidation scenarios outside of what is explicitly permitted by the submission scenario.For the revalidation scenarios that *can* be combined (see MM 7.1.15 #5), the main submission **shall** meet all applicable requirements of the added/secondary scenario, in addition to the main scenario requirements. For example, a RBND + NSRL must include proper regression testing and documenting the changes per NSRL specifications. |  |
| A revalidation submission cannot be performed on a submission that is in the queue. It **shall** be on a completed validation (e.g., UPDT on a *validated* FS). |  |

If a CSTL has been contracted to perform a revalidation for a validated module for which the CSTL did not perform the original testing on the base module:

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The vendor **shall** provide the CSTL with the design documentation and implementation (including source code, HDL, etc.) of the base validated module and of the module that has been updated. |  |
| The vendor **shall** provide the CSTL with the latest Security Policy as shown on the base module’s most recent certificate.  |  |
| The CSTL **shall** determine that the provided base documentation and implementation is identical to the base validated module. |  |
| The CSTL **shall** examine each modification and confirm that the change is appropriate for the submission type (e.g., non-security relevant for NSRL). |  |
| The CSTL **shall** determine that no other modifications, including unintentional, have been made apart from what is permitted by the revalidation scenario.  |  |
| The CSTL **shall** meet all requirements of the revalidation scenario(s) submitted. |  |
| The CSTL **shall** indicate which submission scenario is applicable and a summary of associated changes. |  |
| The CSTL **shall** use the format for listing the information for the certificate as required by each revalidation scenario. |  |
| The CSTL **shall** submit, at a minimum, what is required by the revalidation scenario. |  |

* 1. FS

This Change Document is N/A for an FS.

## VUP

No unique table requirements for a VUP. The general table requirements for all revalidation scenarios still apply (e.g., Sections: 1.1, 2, and 3).

## VAOE

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| Management Manual 7.9 *Vendor or User Affirmation of Modules for the vendor affirmed OEs* |  |

## NSRL

Modifications are made to hardware, software or firmware components **that do not affect any FIPS 140-3 security relevant items**. Per [IG 2.4.A](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#2.4.A%20Definition%20and%20Use%20of%20a%20non-Approved%20Security%20Function), “the term *security* is not defined in the Terms and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6 Functional Security Objectives, and the specific Section 7 Security Requirements derived from those objectives. The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report, design documentation, source code, source code difference evidence, FSM, security policy differences, etc.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| CSTL **shall** review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario. |  |
| CSTL **shall** determine additional testing as necessary to confirm that FIPS 140-3 security relevant items have not been affected by the modification. |  |
| Identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to: * Review the COMPLETE list of assertions applicable to the module,
* Identify, from the previous validation report, the assertions that have been affected by the modification,
* Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
* Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the IG is still applicable.
 |  |
| What changes are being proposed? |  |
| What is the justification that each change is considered non-security relevant? |  |
| Are changes made to: approved / allowed security functions/algorithms, SSPs, approved security services, self-tests, security states within the FSM, or other areas that affects how the module meets the security objectives and requirements of FIPS 140-3? |  |

## ALG

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. The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report and applicable CMVP rulings, design documentation, source code, security policy differences, etc. Code or configuration changes are not permitted under this revalidation scenario. For example, if self-tests are required for approved algorithms, the module must already support these self-tests. In essence, this means that ALG can only be used when a previously vendor affirmed or allowed algorithm now has CAVP testing available and already meets the algorithm requirements (e.g., self-tests).

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario. |  |
| The CSTL **shall** identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to: * Review the COMPLETE list of assertions applicable to the module,
* Identify, from the previous validation report, the assertions that have been affected by the modification,
* Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
* Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the module still meets the IG as it existed at the time of the original validation, except for IGs related to the newly tested algorithm where the latest IGs **shall** be met.
 |  |

## OEUP

No changes to the module with an addition, modification, or deletion of tested operational environments (OEs). Purely deleting OEs can be done as an NSRL, but deleting can be combined in an OEUP if also adding and/or modifying OEs. This requires CAVP-testing the algorithm validations on the new/modified OEs.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| If an entropy source assessment is applicable per [IG 9.3.A](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#9.3.A%20Entropy%20Caveats), ESV(s) to cover all new/modified OEs and/or platforms **shall** be submitted and validated separately prior to submission. |  |
| The CSTL **shall** perform the full regression test suite shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources). |  |
| The only time code changes are allowed as part of an OEUP is if they are non-security relevant and necessary to correctly run the module on the new/modified OE (e.g., compilation flags or configuration options that need to be updated). No other changes are permitted (even to incorporate other non-security relevant changes such as bug fixes). In this case, the CSTL selects the “Limited NSRL” sub-option in Web Cryptik after choosing the OEUP submission scenario. |  |

## RBND

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.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** include the OEM’s written approval for re-branding in the submission package and determine that the re-branded module is identical to the OEM module (n.b. this requirement applies equally to open source and non-open-source modules). Written approval **shall** note the terms of permission (e.g., subsequent addition of OEs, possible re-use of CAVP certificates, entropy, remediation of CVEs, non-security relevant changes, whether a rebrand of a rebrand is acceptable, etc.). If these terms do not explicitly allow a vendor to further rebrand the OEM module, then a rebrand of that rebranded module is not permitted unless written permission is granted by the OEM.  |  |
| Additionally, for modules containing any open-source licensed code, the CSTL **shall** ensure the open-source licensing requirements are met (e.g., any required notices are contained in the Security Policy). The submission **shall** include a letter requesting the validation of the re-branded module and indicate the applicable documentation changes (e.g., vendor name, address, POC information, versioning information, etc.). |  |
| A RBND **shall** include at least one OE from the original validation and cannot include OEs that are not listed in the original validation.  |  |
| CAVP testing **shall** cover all of the list OEs. |  |
| The only time it is allowed to combine a RBND with other scenarios is as follows:1. A RBND may be combined with a PHYS only if physical changes are necessary to correctly rebrand the module. For example, if the paint or coating on the hardware of the rebranded module is changed to reflect the new company's color schemes, and/or to change the vendor and product names on the enclosure. In this case, the CSTL selects the “PHYS” sub-option in Web Cryptik after choosing the RBND submission scenario.
2. The only time code changes are allowed as part of a RBND is if they are necessary to correctly rebrand the module (e.g., to display the new module name/version/logo, or to use the new vendor's color schemes/visual aesthetics). No other changes are permitted (even to incorporate other non-security relevant changes such as bug fixes). In this case, the CSTL selects the “Limited NSRL” sub-option in Web Cryptik after choosing the RBND submission scenario.
3. A vendor may reuse OEM’s CAVP certificates with proper permission. But if the OEM does not permit the vendor to reuse the CAVP certificates, then the vendor will need to perform CAVP testing on all listed OEs. If CAVP testing is redone, the CSTL selects the “CAVP Testing Redone” sub-option in Web Cryptik after choosing the RBND submission scenario.
4. A RBND is almost guaranteed to be combined with a VUP to address the vendor changes so this will not be separately selectable in Web Cryptik.
 |  |
| The CSTL **shall** provide an updated security policy which is technically identical to the originally validated security policy and describes the re-branded module. |  |

## PTSC

A sub-chip cryptographic subsystem that was previously validated in a single-chip (see [IG 2.3.B](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#2.3.B%20Sub-Chip%20Cryptographic%20Subsystems)) can be ported to other single-chip constructs as a PTSC submission to the CMVP.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** verify that there are no security relevant changes in the sub-chip cryptographic subsystem; |  |
| If an entropy source is contained within the sub-chip cryptographic subsystem, ESV(s) to cover all new single-chip environments **shall** be submitted and validated separately prior to submission;**Note 1**: An ESV may not be required, if the entropy is collected outside the sub-chip cryptographic subsystem, depending on changes to the entropy source or the subsystem housing it. Please refer to IG 9.3.A and IG D.J for details on applicable caveats and entropy estimates. **Note 2**: Single chip embodiments may implement an ESV or a DRBG linked to a dedicated entropy source inside the physical boundary. Such cases may be implemented (a) inside the sub-chip cryptographic subsystem or (b) in two or more sub-chip cryptographic subsystems. The case (b) represents multiple disjoint sub-chip cryptographic subsystems (see 3 of IG 2.3.B). |  |
| Approved security functions **shall** be retested and validated by the CAVP if implemented in a soft circuitry core recompiled in a different part configuration. **Note 3**: If the original algorithm testing was performed as stated in the [Management Manual](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual) Section 7.3 – *Testing using Emulators and Simulators* in a module simulator, and there is no change to the soft-core, no additional algorithm testing is required. |  |
| Full regression testing (see FIPS 140-3 [Resources page](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources)) **shall** be performed on the new sub-chip cryptographic subsystem after fabrication (transformation of the HDL to a gate or physical circuitry representation); |  |
| **ISO/IEC 19790:2012** Section 7.3 **shall** be addressed for the new single-chip module for all Security Levels within this Section. |  |
| **ISO/IEC 19790:2012** Section 7.7 **shall** be addressed for the new single-chip module at Security Level 1.  |  |
| **ISO/IEC 19790:2012** Sections 7.11.2 and 7.11.9 **shall** be addressed for the new single-chip module for all Security Levels within this Section. |  |
| A new Security Policy **shall** be provided for the new single-chip module.  |  |
| Versioning information on the new certificate **shall** be provided for:* the new physical single-chip,
* non-security relevant single-chip functional subsystem firmware if applicable,
* the sub-chip cryptographic subsystem soft and hard circuitry cores (which are unchanged from the original validation), and
* the associated firmware.
 |  |
| The only time code changes are allowed as part of an PTSC is if they are non-security relevant and necessary to correctly run the module on the new/modified single chip environment (e.g., compilation flags or configuration options that need to be updated). No other changes are permitted (even to incorporate other non-security relevant changes such as bug fixes). In this case, the CSTL selects the “Limited NSRL” sub-option in Web Cryptik after choosing the PTSC submission scenario. |  |

## UPDT

Modifications are made to hardware, software or firmware components **that affect some of the FIPS 140-3 security relevant items**. Per [IG 2.4.A](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#2.4.A%20Definition%20and%20Use%20of%20a%20non-Approved%20Security%20Function), “the term *security* is not defined in the Terms and Definitions, but, within the scope of FIPS 140-3, is determined based on the Section 6 Functional Security Objectives, and the specific Section 7 Security Requirements derived from those objectives. An updated cryptographic module can be considered in this scenario if less than a 30% of security changes were made to the module.

The CSTL is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient, and the vendor is responsible for submitting the requested documentation to the CSTL. Documentation may include a previous validation report and applicable CMVP rulings, design documentation, source code, source code difference evidence, FSM etc.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** provide a summary of the changes and rationale of why this meets the <30% guideline. The CMVP upon review, may determine that the changes are >30% and **shall** be submitted as an FS.Security changes include impacts to: approved / allowed security functions/algorithms, SSPs, approved security services, self-tests, and security states within the FSM. None of these, assessed individually, can exceed 30% of changes. The individual ratios for each of these **shall** be provided to the CMVP within the Change Document (e.g., 2 approved security services out of 10 total results in 20% change).  |  |
| Review and independently verify the accuracy of the vendor-supplied documentation and identify any additional documentation necessary to confirm the applicability of this revalidation scenario. |  |
| Identify the assertions affected by the modification and **shall** perform the tests associated with those assertions. This will require the CSTL to: * Review the COMPLETE list of assertions applicable to the module,
* Identify, from the previous validation report, the assertions that have been affected by the modification,
* Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
* Review assertions where specific Implementation Guidance (IG) was provided to confirm that the module meets all current applicable IGs.
 |  |
| In addition to the tests performed against the affected assertions, the CSTL **shall** perform the regression test suite shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources). |  |
| The UPDT can also be used to for resetting the module’s sunset date when a module has not changed, provided the above requirements are met. |  |
| UPDT can be combined with any submission scenario(s) except VUP or VAOE. In this case, the CSTL selects the appropriate sub-option(s) in Web Cryptik after choosing the UPDT submission scenario. |  |

Original submission date of the revalidation certificate: [DATE]

|  |  |  |  |
| --- | --- | --- | --- |
| **IG(s) published or modified and date since original submission date** | **Summary of IG changes** | **Applicable to module?** | **How the module meets the requirements found to be applicable** |
| **See** [**Change Summary**](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#Change%20Summary) |
| NEW IGs |
| [example]03/17/23: 10.2.A Pre-operational Integrity Technique Self-test  |  [example] | [example]Yes | [example]Module already runs a pre-operational KAT on the HMAC KAT (SHA2-256) before the integrity test. AS10.20 – pre-operational KAT for HMAC SHA2-256  |
| … | … | … | … |
| MODIFIED IGs |
| [example]11/22/23: 2.4.C Approved Security Service Indicator | [example]Clarified the API example in the Resolution and added a related Additional Comment 5. | [example]Yes | [example]Module uses PAA = AES-NI from the IG list below and all algorithms have been tested with and without PAA:**Known PAAs:** ● Intel Processors – Xeon, Core i5, Core i7, Core M and Atom with Westmere, Sandy Bridge, Ivy Bridge, Haswell, Broadwell, Skylake, Kaby Lake, Coffee Lake, Goldmont Plus, Whiskey Lake, Amber Lake, Cascade Lake, Comet Lake, Sunny Cove, or Golden Cove micro-architectures: PAA = AES-NI |
| … | … | … | … |

## CVE

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 (Common Vulnerability and Exposure). For more information about CVEs please see <https://cve.mitre.org/>.

The purpose of this revalidation scenario is to provide the vendor a means to quickly fix, test and revalidate a module that is subject to a *security-relevant* *CVE1*, while at the same time providing assurance that the module still meets the FIPS 140-3 standard. If a CVE does not require security relevant changes to address it, then the vendor may pursue a NSRL revalidation.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** determine that security relevant changes to the module are only to correct the vulnerability disclosed in the CVE (non-security relevant changes, as defined in Scenario NSRL, are permissible) |  |
| The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3.  |  |
| The CSTL **shall** determine that no other modifications have been made.  |  |
| The CSTL **shall** identify the assertions affected by the security-relevant modification and **shall** perform the tests associated with those assertions. |  |
| The vendor is not required to address IGs that have been published since submission of the original module, besides following the continual guidance of IG 11.A (CVE Management).  |  |
| If the fix to address the CVE is in the scope of an algorithm implementation, then this algorithm **shall** be CAVP tested again to obtain a new CAVP certificate with the new module version. |  |
| Because the change to the module is to address a security-relevant CVE, the previous version of the module is no longer considered validated and **shall** be removed from the certificate |  |
| In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources), under CVE. |  |
| Because the change to the module is to address a security-relevant CVE, **the previous version of the module is no longer considered validated and shall be removed from the certificate**; exceptions may be made if the vendor shows how the CVE can be mitigated by policies included in the Security Policy, while still adhering to the FIPS 140-3 standard. |  |

## TRNS

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. For example, the 2024 non-SP 800-56Brev2 RSA-based key encapsulation/un-encapsulation transition explained in FIPS 140-3 [IG D.G](https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf#D.G%20Key%20Transport%20Methods). If the algorithm transition will NOT cause the module to move to the historical list (i.e., considered a “soft” transition), changes cannot be made as part of this submission.

Note: a single Scenario TRNS submission may combine multiple algorithm transitions. However, this may increase review time.

The purpose of the TRNS revalidation is to provide the vendor a means to quickly address algorithm transition requirements, test and revalidate a module in order to meet a CMVP transition, while at the same time providing assurance that the module still meets the FIPS 140-3 standard.

Module code is *changed*:

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL **shall** determine that security relevant changes to the module are only to address a specific CMVP transition. Other changes are permitted if only directly impacted by the TRNS change (e.g., addressing the TRNS may require changing the version number, and that requires the show version service be updated). In this case, the CSTL selects the “Limited NSRL” sub-option in Web Cryptik after choosing the TRNS submission scenario. |  |
| The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3. |  |
| The CSTL **shall** determine that no other modifications have been made. The vendor is not required to address IGs or guidance that have been published since submission of the original module, unless directly applicable to the transitioning algorithm (e.g., CAVP testing or self-test requirements). |  |
| The CSTL **shall** identify the assertions affected by the security-relevant modification and **shall** perform the tests associated with those assertions. |  |
| If the means to meet the transition are in the scope of an algorithm implementation, and the path chosen to meet the requirements necessitates testing, then this algorithm **shall** be CAVP tested to obtain a new CAVP certificate with the new module version. In this case, the CSTL selects the “CAVP Testing Redone” sub-option in Web Cryptik after choosing the TRNS submission scenario. |  |
| In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources) under TRNS on all versions listed on the module’s certificate and on at least one of the listed OEs for hybrid or software/firmware modules (if the module binary image is identical across all OEs; if not, testing on at least every binary image is required). |  |
| The CSTL **shall** provide justification on why regression testing is not necessary for the untested OEs. With proper justification, these may remain on the module’s certificate.  |  |
| If regression testing is not performed on some versions, then those **shall** be removed from the module’s certificate. OEs without proper justification or regression testing **shall** be removed from the module’s certificate. |  |

If the module code is *unchanged* to address an algorithm transition and the change is purely to documentation, one or more of the following options apply:

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| **Option 1** |
| Services or functionality were not moved to or from the approved mode to remain compliant (e.g., previously non-compliant services remain in the approved mode but are updated to demonstrate compliance rather than moved into non-approved mode), then the vendor may pursue a Scenario ALG revalidation. | [Submitted as a Scenario ALG] |
|  |  |
| **Option 2:**The vendor moves all non-compliant functionality into the non-approved mode of operation from the approved mode of operation.**Option 3:** The vendor recategorizes the non-compliant functionality as claiming no security per [IG 2.4.A](#_1.23_Definition_and), and this functionality remains in the approved mode of operation. |
| The CSTL **shall** state that the change to address the transition is purely documentational and which option applies. |  |
| The CSTL **shall** determine that security relevant changes to the module are only to address a specific CMVP transition. |  |
| The CSTL **shall** examine each modification and confirm that the change does not conflict with the requirements of FIPS 140-3. |  |
| The CSTL **shall** determine that no other modifications have been made. The vendor is not required to address IGs or guidance that have been published since submission of the original module, unless directly applicable to the transitioning algorithm (e.g., CAVP testing or self-test requirements). |   |
| The CSTL **shall** identify the assertions affected by the security-relevant documentation modification and **shall** perform the tests associated with those assertions. |  |
| The CSTL **shall** demonstrate how the module still meets IG 2.4.C after the reclassification of non-compliant functionality into the non-approved mode of operation. |  |
| In addition to the tests performed against the affected assertions, the CSTL **shall** also perform the predefined regression tests shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources) under TRNS on all versions listed on the module’s certificate and on at least one of the listed OEs for hybrid or software/firmware modules (if the module binary image is identical across all OEs; if not, testing on at least every binary image is required). The only exception to this requirement is if the algorithm being transitioned is part of a standalone service and is not used by any other module service (e.g., cryptographic library where the module only provides the algorithm as an API service to a calling application as a stand-alone service). In this case, the CSTL **shall** provide justification on why regression testing is not necessary at all. |  |
| The CSTL **shall** provide justification on why regression testing is not necessary for the untested OEs. With proper justification, these may remain on the module’s certificate.  |  |
| If regression testing is not performed on some versions, then those **shall** be removed from the module’s certificate. OEs without proper justification or regression testing **shall** be removed from the module’s certificate. |  |
| The CSTL **shall** provide assurance that the non-compliant functionality is not used to meet any FIPS 140-3 requirements (key/CSP establishment, generation, storage, etc.). |  |
| In order to accommodate vendors who are updating their validation to prepare for an algorithm transition, fully compliant TRNS or ALG revalidations that have addressed the transition and are submitted to the CMVP before the date the transition is to take effect, will remain on the active list through the completion of the revalidation, even if it is not completed until after the transition date, unless the algorithm transition is to address a security concern that is deemed unacceptable by the CMVP. For newly submitted ALG submissions that address the transition, the CSTL **shall** include in the Special Instructions field the text “algorithm\_transition” (with or without the underscore) in order for the CMVP not to move this submission to the historical list come the algorithm transition date. |  |
|  |
| **Option 2** |
| The CSTL **shall** provide assurance, upon module examination, that no service, algorithm or CSP that relied on or used the non-compliant functionality, parameters, keys, etc. remain in the approved mode.  The approved mode **shall** only contain approved services. |  |
| Documentation **shall** be updated to indicate the module does not utilize non-compliant functionality in the approved mode of operation. |  |
|  |
| **Option 3** |
| The CSTL **shall** provide justification on how the requirements of [IG 2.4.A](#_1.23_Definition_and) are met. This scenario is intended to be rarely used/accepted and depends on the purpose or use of the service that utilizes the non-approved algorithms. For example, a software library implementing three-key Triple-DES Encryption as one of its approved services cannot simply state this algorithm does not claim any security (per [IG 2.4.A](#_1.23_Definition_and)) and be used in the approved mode, as this does not meet 3) or 4) in [IG 2.4.A](#_1.23_Definition_and) Additional Comment #2.  |  |
|  |  |
| **Option 4** A combination of any of three options above (CAVP testing, moving non-compliant functionality into the non-approved mode, and/or recategorized per [IG 2.4.A](#_1.23_Definition_and)), in which case, requirements of each option apply. |
| Each option **shall** be listed/indicated in the Change Document under Option 4 (e.g. under Option 4, the following are claimed: Options 1 and 2) and note how each of the applicable ‘shall’ statements for each option are met). |  |

## PHYS

Modifications are made only **to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module**.

|  |  |
| --- | --- |
| **Requirement** | **CSTL Compliance evidence / justification** |
| The CSTL is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. |  |
| The CSTL **shall** fully test the physical security features of the new enclosure to ensure its compliance to the applicable requirements of the standard. |  |
| Describe the change (pictures may be required)  |  |
| State that it is a security relevant change |  |
| Provide sufficient information supporting that the physical only change has no operational impact |  |
| Describe the tests performed by the CSTL that confirm that the modified enclosure still provides the same physical protection attributes as the previously validated module. For physical security levels 2, 3 and 4, the CSTL **shall** submit an updated Physical Security Test Report. |  |

# Certificate Modification Tables

For all revalidation scenarios the CSTL **shall** use the following format to cover all updated fields (e.g., vendor, CSTL, and module changes). Deletions **shall** be marked using strikethrough and additions **shall** be highlighted in yellow.

For example:

|  |  |  |
| --- | --- | --- |
| **Field(s)** | **Current Cert. #999** | **Change Requested Cert. [#999 or new Cert]** |
| Hardware Version | 3.1 | 3.1, 3.2 |
| Firmware Version | ~~a.1, b.1~~ | c.1 |
| Product Link | [www.product~~A~~.com](http://www.productA.com) | [www.productB.com](http://www.productB.com) |
| Vendor Name | Vendor ~~ABC~~ | Vendor DEF |

# Affected TEs and Security Policy Changes

The CSTL **shall** list the affected TEs, and a summary of the changes performed in their associated CSTL assessment.

For example:

|  |  |
| --- | --- |
| **TR/SP Section** | **Affected TE/SP and Assessment** |
| 1. General
 | The module’s name has been changed from ModuleA to ModuleBUpdated to reflect the updated firmware version, c.1.SP Cover Page: Updated to include new name and new firmware version. |
| 1. Cryptographic module specification
 | 02.11.01, 02.11.02: Updated and retested for new module name.02.12.01: Updated and retested for new firmware version.SP Section 2: Updated to include new name and new firmware version. |
| 1. Cryptographic module interfaces
 | No change |
| 1. Roles, services, and authentication
 | 04.13.01, 04.13.02, 04.13.03: Updated and retested for new version. |
| 1. Software/Firmware security
 | … |
| 1. Operational environment
 | … |
| 1. Physical security
 | … |
| 1. Non-invasive security
 | … |
| 1. Sensitive security parameter management
 | … |
| 1. Self-tests
 | … |
| 1. Life-cycle assurance
 | … |
| 1. Mitigation of other attacks
 | … |
| Appendix B |  |

# Predefined Regression Testing

The minimum predefined regression tests are shown on the [CMVP website](https://csrc.nist.gov/Projects/cryptographic-module-validation-program/140-3-resources) for the OEUP, PTSC, UPDT, CVE, TRNS (code changes), and TRNS (no code changes).