**28 May 2021**

# Frequently Asked Questions for NIAP Policy #5

1. ***Why is this policy being issued?***

   This policy streamlines the NIAP evaluation process, helps reduce cost, and eliminates redundant activities. This policy does not provide an exemption from protection profile mandated documentation (e.g., Security Target, required entropy documentation, etc.), but does provide an alternative to the testing that is conducted by the CCTL. Evaluation activities that are performed during a cryptographic algorithm or module validation which results in a NIST CAVP/CMVP certificate may be used to demonstrate compliance to some PP/cPP assurance activities. Additional Common Criteria testing is unnecessary for these assurance activities.

2. ***How is this policy applicable for products evaluated against NIAP-approved PP/cPPs, but outside of NIAP?***

   All assurance activities described in the PP/cPP must be performed in order to successfully complete a Common Criteria evaluation. NIAP recognizes evaluation activities performed during a NIST cryptographic algorithm or module validation as evidence of meeting some PP/cPP assurance activities. However, the CCRA Compliant Certification Body conducting the evaluation determines if CAVP/CMVP certificates are acceptable to show compliance.

3. ***NIST has transitioned from the Cryptographic Algorithm Validation System (CAVS) tool to the new Automated Cryptographic Validation Testing (ACVT) tool for algorithm testing. Does NIAP accept NIST CAVP certificates that were validated by NIST using the CAVS tool?***

   Yes, NIAP recognizes Cryptographic and Security Testing (CST) Lab evaluation activities that are performed during a cryptographic algorithm or module validation which results in a NIST CAVP/CMVP certificate regardless of whether CAVS or ACVT was used.

4. ***When can a CAVP certificate be applied to a PP assurance activity?***

   CAVP certificates can be applied to a PP assurance activity when the cryptographic algorithm implementation validation (software, firmware, hardware, and any combination thereof) meets the requirements (standards, modes, states, key sizes, etc.) specified in the PP/cPP.

   The Cryptographic Algorithm Validation Program Management Manual and CAVP FAQ defines the OEs for software, firmware, and hardware cryptographic algorithm implementations differently. For software implementations the OE is the processor and operating system, for firmware implementations the OE is the processor, and for hardware implementations the OE is the part number. NIAP has refined this guidance for NIST validated cryptographic algorithm implementations used in Targets of Evaluations (TOEs) as follows.

   For firmware and hardware cryptographic implementations, for a validated cryptographic algorithm implementation to be applicable to a TOE, the OE must correspond exactly to the hardware platforms specified in the Security Target (ST).

For software cryptographic implementations, for a validated cryptographic algorithm implementation to be applicable to a TOE, the following requirements must be met:

a. The processor specified as the platform in the ST must be reported at the microarchitecture level and must be an identical match to the processor specified on the CAVP certificate (e.g., Intel Xeon E5-2620v1 (Sandy Bridge), Intel Atom C3308 (Goldmont), QUALCOMM SD710 (Cortex-A75).

b. The implementation of the validated cryptographic algorithm has not been modified upon integration into the TOE; and

c. The operating system specified as the platform in the ST under which the validated cryptographic algorithm implementation was tested must be an identical match to the operating system specified on the CAVP certificate, with this one exception:

    1. For all operating systems, minor version variations that do not affect interfaces used by the TOE are considered equivalent. For instance, if System X.1.3 were specified as the operating system, and the TOE used no interfaces that were changed by System X.1.4, then the TOE can claim System X.1.4 as equivalent. If the version numbering system used by the vendor is not obvious in terms of major vs. minor, the vendor must provide a clear description of their versioning system and it must be documented in the Assurance Activity Report (AAR)

***5.*** If claiming equivalency for a processor, the fully tested processor must be listed along with the processors where equivalency is claimed in the ETR. The equivalency argument will include:

- Fully tested processor(s)
- Equivalent processor(s) mapped to fully tested processor(s)
- Equivalency argument
- Both Hardware and Virtual Machines must have a fully tested product instance.

***6. What additional level of specificity is required in the OE description for software cryptographic implementations applicable to a TOE?***

1. If the processor supports instruction-set extensions used by the cryptographic implementation (e.g., AES-NI, PCLMULQDQ), then the use or non-use of those extensions must match what is listed in the ST. For example, if the operational environment of the CAVP certificate specifies that a processor supporting AES-NI was used, and that the AES-NI instructions were used, then the processors listed in the ST are acceptable only if they support AES-NI.
2. Any virtual machine (VM) used during testing shall be listed in the OS field of the Operating Environment (OE) on the CAVP certificate and must exactly match the VM specified in the ST. If the VM was running between the software implementation and the OS, as in the case of a Java VM, it should be listed along with the OS using the same vendor and family/version number requirements.
3. Any hypervisor shall be specified in the operating environment (OE) of the CAVP certificate listing and must match the hypervisor specified in the ST as described below.

- For a Type 1 (or native) hypervisor, where the hypervisor runs directly on the hardware, the OE listing shall include the processor, guest OS and hypervisor using the following format: “Processor w/ Guest OS on hypervisor.”
- For a Type 2 (or hosted) hypervisor, where the hypervisor runs on a host operating system (OS), the OE listing shall include the processor, guest OS, hypervisor and host OS using the following format: “Processor w/ Guest OS on hypervisor on Host OS.”

7. ***What is the level of specificity required for processors in the evaluation documentation (e.g. Security Targets, AARs, ETRs, EAs, EARs, etc.).***

   The evaluation documentation must describe all tested configurations down to processor manufacturer, model number, and microarchitecture version (e.g. Intel Xeon E5-2620v1, Sandy Bridge). This must be an identical match to the processor specified on the CAVP certificate.

8. ***Some PP/cPPs include guidance that allows for equivalency across product models, product versions, hardware platforms, software platforms, and their operational environments. What effect do those guidelines have on the CAVP/CMVP certificates?***

   For all products evaluated in the US Scheme, at least one product instance must be fully tested on at least one platform with cryptography mapped to a CAVP certificate. This includes products that rely solely on the platform to provide the cryptography.

9. ***How is a CAVP certificate applied to a PP assurance activity?***

   When the CCTL addresses an assurance activity where the vendor has indicated in the ST that there is a relevant CAVP validation, the CCTL shall consult the appropriate NIST Algorithm Validation List. If the CCTL finds that the associated tests, implementation, operational environment and modes, states and key sizes cover the elements of the assurance activity, then the CCTL does not need to test those elements. The CCTL must provide clear evidence in the Evaluation Technical Report in accordance with the NIAP Certificate Reporting Template. The CCTL shall also indicate in the Assurance Activity Report that those elements were tested as part of the CAVP validation.

   NIAP has developed a CAVP mapping document which specifies which CAVP Algorithm Validation List is applicable to each cryptographic requirement. Vendors and CCTLs must be familiar with this document to ensure their implementations meet cPP/PP requirements.

   For products evaluated in the US Scheme, the NIAP CAVP mapping document specifies which requirements must be met with a CAVP certificate.

10. ***In cases where the cryptography is platform-provided, how would the evaluator verify the platform satisfies the cryptographic requirements?***

    There are two ways to ensure the platform-provided cryptography satisfies the cryptographic requirements:

    1. If the platform has been evaluated and is on the NIAP Product Compliant List (PCL), the evaluator may rely on the Security Target of the evaluated platform to verify the functionality

was evaluated.

- Verifying cryptographic requirements for platform provided cryptography
  - ST may be claimed from a current validated/certified platform
  - The new evaluations ST must reference the validated/certified platform to include the full name of the validated/certified platform, VID number (if applicable), and certification date.
  - The previously certified evaluation's ST must be provided in the ETR claiming the platform provide cryptography
  - Screen shot evidence of the previously evaluated ST showing how the new evaluations cryptographic requirements are met in the ETR.
  -

2. If the platform has not been evaluated or is no longer on the NIAP PCL, the vendor must obtain CAVP certificates for the specified platform and document in the ETR their applicability to the TOE. The CAVP certificates must show that all FIPS-approved and NIST-recommended cryptographic algorithms and their individual components that are used in the evaluated configuration (e.g. for configured cipher suites, the random number generator, etc.) are within the scope of the algorithm validation.

***11.* What if the CAVP for platform-provided cryptography does not include the OE details required?**

The CCTL must provide NIAP with a detailed analysis of the differences and submit to NIAP at check-in. This includes:

- providing evidence highlighting the differences between what is specified in the OE vs what is required per Policy 5,
- an explanation for why the application vendor is not able to perform the algorithm testing, and
- a rational for why the OE on the certificates should be acceptable to NIAP.

***12. When new algorithm implementations are validated by NIST and added to the Algorithm Validation List, will CAVP certificates be required for evaluations conducted in NIAP when the PP does not include a specific testing assurance activity?***

There are three types of assurance activities within a PP (TSS, Guidance & Testing). If any of these assurance activities requires the verification of the correct implementation of a function for which NIST provides validation testing the vendor may use the appropriate CAVP certificate to demonstrate compliance to the PP/cPP assurance activities.

***13. What is a Component Validation? Will NIAP accept a Component Validation in lieu of a complete Algorithm Validation?***

Situations exist where an algorithm is implemented across multiple cryptographic boundaries. In these cases, it is not possible to obtain algorithm validation because testing requires the complete algorithm to be within the same cryptographic boundary. Therefore, component testing was introduced. Component testing allows assurance of the individual components of an algorithm. For example:

– Module includes ECDSA Signature Generation but the implementation is not contained within one algorithm boundary

- The vendor would need 2 algorithm validations:
  - SHA validation
  - Component validation (CVL) for ECDSA Signature Generation Component

NIAP does accept CVL Certificates in lieu of a full algorithm validation certificate if it meets the requirements within the PP/cPP. The NIAP CAVP mapping document specifies which requirements may be met with a CVL certificate.

### *14. How is a CMVP certificate applied to a PP assurance activity?*

If a vendor wants to use the results from a FIPS 140-2 cryptographic module validation in which a CMVP certificate number was awarded, then the vendor must provide the CMVP certificate number in the ST and provide the relevant assertions, AS, from the draft NIST Derived Test Requirements (DTR) for FIPS PUB 140-2, dated January 4, 2011, in the description of how the appropriate TOE SFR is met in the AAR.

When the CCTL addresses an assurance activity where the vendor has indicated that there is a relevant NIST DTR assertion, the CCTL will verify the claim using the Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules List. If the CCTL finds that the associated module covers the elements of the assurance activity, then the CCTL does not need to test those elements. The CCTL shall indicate in the Assurance Activity Report that the PP assurance activities were conducted as part of the FIPS 140-2 validation. In addition, cryptographic algorithm validation is a prerequisite of a cryptographic module validation and therefore the module's applicable CAVP validations must also be listed in the ST and must match the CAVP validations cited on the Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules List.

### *15. How do CAVP/CMVP certificates relate to the protocol SFRs? Are they required?*

Applicable CVL's for SP800-135 KDFs (such as IKEv1, IKEv2, TLS, SSH, SRTP, SNMP) are encouraged, but not required, for the protocol SFRs included in PP/cPPs. These will be required as AAs are developed and incorporated into PP/cPPs.

### *16.* **What information is required to claim multiple processors from different microarchitectures?**

To meet the policy 5 requirements one processor must be fully tested and display exactly across the ST, ETR, AAR, AGD. As an Example, if a processor that is fully tested is Intel Xeon E5-2620v1 (Sandy Bridge), then this processor must be displayed exactly on the NIST certificate as well as the ST, ETR, AAR, AGD, EAR.

If there are multiple processors with the same microarchitecture an equivalency argument may be proposed. Other processors may be claimed from different processor microarchitectures however, at least one processor must be displayed using the same microarchitecture on the NIST certificate.

- At least one fully tested processor
- Multiple processor families may be claimed however at least one processor of each family displayed down to the family/series level on the NIST certificate. If the processor claimed is

not exactly what is displayed on the NIST certificate an equivalency argument can be made provided both processors are the same microarchitecture.

- Equivalency arguments can be made for processors in the same family to the fully displayed processor in that family.