17 November 2016

Frequently Asked Questions for NIAP Policy #5

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

   This policy is being issued to streamline the NIAP evaluation process, help reduce cost, and eliminate 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. ***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 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 implementation of the validated cryptographic algorithm has not been modified upon integration into the TOE; and

   b. The operational environment under which the validated cryptographic algorithm

implementation was tested must be the same as the operational environment of the TOE that is being tested by the CCTL, with these two exceptions:

1. For all OE software, minor version variations that do not affect interfaces used by the TOE are considered equivalent. For instance, if System X were specified as the Operational Environment Software, and the TOE used no interfaces that were changed by System X Revision 1, then the TOE can claim System X Revision 1 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 AAR.
2. Processors in the OE that are implemented by the same manufacturer in the same family as hardware listed in the ST is also considered equivalent (for instance, Intel Core-series processors (i3, i5, i7), Snapdragon processors implemented with Krait-400 cores (800, 801)).

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

1. If the processor supports 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 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). 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) listing as described below.
    a. 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.”
    b. 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.”

5. 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 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 following cPP/PP requirements must be addressed by obtaining a CAVP certificate number:

FCS_CKM (except .4)
FCS_COP
FCS_RBG_EXT.1

6. ***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.

7. ***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.

8. ***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 Security Target.

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.

9. 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.