March 3, 2015

Dear CST Laboratories,

Thank you for your feedback concerning the addition of cryptographic algorithm testing information to the CAVS tool's vendor/implementation information page. This additional cryptographic algorithm testing information addresses how and by whom the algorithm testing was performed.

I have taken your feedback into consideration for finalizing the addition of the algorithm testing information. This information has been added to the Cryptographic Algorithm Validation System (CAVS) 17.5 tool to be released March 4, 2015.

Below you will find the feedback that I received, along with my responses.

Sincerely,

Sharon Keller
CAVP Director
NIST

1. … since the vendor's signature is required with the CAVS submission, does this mean it will no longer be required for the CMVP CRYPTIK submission?

The CAVS and the CMVP processes are two separate processes that are testing two different entities. Therefore the signatures required for each program are independent. For the CAVP, the vendor's signature is only required if the testing is performed by the vendor. If a tester at the CSTL performs the testing, we ask for their signature. We are asking for this to gain a stronger credibility for who performed the testing.

2. Currently, if an implementation has several algorithms, and each algorithm is separately version controlled, then we are required to have a separate CAVS file (*.inf) for each. If a group of algorithms for the same implementation are submitted at the same time, but each generates its own "Algorithm Validation Testing Details" sheet, are we required to have the vendor provide a signature for each algorithm? Could we concatenate the information into one coversheet with only one vendor signature?

We do ask for a signature for each different CAVS folder because each different IUT may be tested by a different tester. Note that the vendor's signature is only required if the testing is performed by the vendor. If the testing is performed by the CSTL tester, we ask for their signature.

3. XTS-AES has a vendor assurance of the length of data units for any instance of an implementation of XTS-AES SHALL not exceed 2^20 blocks. We are currently asking vendor to sign a vendor affirmation letter for that. Do you want to include this vendor assurance?

The information we are addressing in this instance pertains to who and where the testing of an IUT was performed. Therefore, this XTS-AES assurance is outside the scope of this information.

The assurances that are required for individual cryptographic algorithms are mentioned on the individual algorithm tabs. (The XTS_AES assurance listed in this question is included on the XTS_AES screen.) It is the responsibility of the CSTL to assure these assurances are met. The way you are handling it (having a vendor affirmation letter for the implementer to sign) is an acceptable way to get this assurance.

4. Is it possible to just have the Approved Signatory sign the letter rather than the CSTL individual who performed the testing?

No. The purpose of gathering this information is to gain a stronger credibility of the actual tester who performs the validation testing. That's why we want the actual tester to sign the letter.

The approved signatory will sign the complete submission letter like always.

5. Can the customer provide a digital signature? Or is a physical signature required?

A physical signature is required at this time.

6. Where it asks for "location", is this intended to be an address? It isn't clear how much location identification is needed.

The CAVP has decided to remove the "location" field. We will only have check boxes to confirm if the CAVS test vectors are applied to the IUT:

by the CSTL at the CSTL

by the CSTL at an offsite location

by the CSTL at the vendor facility

by the vendor at the vendor site and directly observed by the CSTL

by the vendor at the vendor site and unobserved by the CSTL

Depending on which scenario applies to the IUT, the cover letter will require the appropriate signatures: if the testing is performed by a tester at the CSTL, the tester's signature will be required; if the testing is performed by a vendor's tester, then the vendor's tester's signature will be required; if the vendor performs the testing and an observer from the CSTL observes the testing, both the vendor's tester and the CSTL's observer's signatures will be required.

7. Can you elaborate on the expectation of the lab reviewing a test harness developed by a vendor/other? You provide both "yes" and "no" options. Or is this an internal metric for CAVP note only?

Handbook 150 and 150-17 gives detailed information on the records that shall be kept by a laboratory on the testing of algorithms and modules. So if a test harness developed by a vendor/other was used in the testing of an IUT, the details of this should be included in those records. The lab would want to assure that the test harness is actually testing the IUT – that no man in the middle attack is possible – that the results are generated by the IUT.

8. How does this impact certificates that are only tested as algorithm projects? We have some customers who want a CAVP certificate, but do not intend to pursue a FIPS validation certificate. Will it still apply to them?

The CAVP test cryptographic algorithm implementations. What these implementations are used for or what they are included in is outside the scope of the CAVP. The information we are asking for here will apply to every algorithm validation.

9. Is it possible to have the customer fill out this information in a Word or Excel document that could be directly imported into the CAVS tool? Data entry is the most common error in our process and it would be greatly improved if we could import directly.

This information is supplied by the tester. The tester may be at the CSTL or at the vendor site. This information needs to be filled out by the tester. Currently the CSTL will need to ask the tester for this information prior to the form being developed by the CAVS tool that requires the tester's signature. One of our tasks for the future is to provide a means for the customer to fill out as much as the information as possible. It's not possible at this time.

10. Will this only apply to upcoming tests? Or will CAVP require this information for past testing? What will the transition period be for implementing this new information gathering? It would be difficult, if not impossible; to gather this information for previously validated algorithms.

This will only apply to upcoming algorithm testing. The CAVP will not require this information for past testing.

11. It seems to be assumed that the vendor representative who signs this letter shall be the one who has performed the CAVS test. We think the accountability shall be associated to the organization instead of the individuals. As long as the vendor representative is accountable, s/he does not have to be the developer who actually performs the test. We have been asking the vendor to sign an assertion letter with us for how the CAVS is conducted. What we often see is that the project manager signs the letter while a team member does the actually testing. This should be allowed.

The CAVP disagrees with this statement. The CAVP is collecting this information to gain a stronger statement of assurance that the IUT testing has been performed correctly. We want the actual tester to sign this form to gain a stronger credibility for who performed the testing. (This refers to the team member that does the actual testing in the above statement). If the testing is performed by a tester at the CSTL, the tester's signature will be required; if the testing is performed by a vendor's tester, then the vendor's tester's signature will be required; if the vendor performs the testing and an observer from the CSTL observes the testing, both the vendor's tester and the CSTL's observer's signatures will be required.

12. There is a typo in “CSE Laboratory”. It should be “CST Laboratory”. Also, a CST lab manager should be allowed to sign off the letter on behalf of the lab tester who actually performs or observes the CAVS test.

Thank you for pointing this out – CSE has been changed to CST.

The CAVP disagrees with the rest of this statement. We want the actual tester to sign this form to gain a stronger credibility for who performed the testing. The CST Laboratory Manager will still be required to sign the Algorithm Submission Letter like always.

13. Please delete “2A.” and “:” from “2A. Test harness constructed by: CST Lab”. The letter should be readable out of the context of the CAVS Tool, which the vendor does not have.

The CAVP agrees and this has been modified to be readable out of the context of the CAVS Tool.

14. In a normal case, the algorithm testing is performed using module API. In some rare cases, it’s not true. Therefore, we suggest not to ask for API services used for algorithm testing because the list of API services can be very long and they are listed on the Security Policy. Instead, we suggest to ask for interface used for algorithm testing when the module API is NOT used for algorithm testing.

The CAVP has decided to eliminate the question concerning the module API. Also the question “The cryptographic module was modified to perform the algorithm validation testing” has been removed. These questions are out of scope of the algorithm testing.

15. There is no need to ask “Who parsed the IUT outputs for CAVS input”. The validation system documents (e.g. AESAVS, XTSVS, DSA2VS, ECDSA2VS, RSA2VS, etc.) have provided the well defined format of the response files that are expected as the IUT outputs. A CST lab shall take the response files provided by the vendor and feed them as input files directly to the CAVS Tool. Any post-processing to manipulate the IUT outputs by lab shall not be allowed.

The purpose for asking this question was really to determine who puts the output in the format required by the response file. This may be the vendor, the CSTL tester, or someone else. It also may coincide with who creates the test harness.

16. If you could add the CAVP Metrics question “Has the implementation FAILED on the first test” and eliminate the use of a separate METRIX tool for this information that would be a great relief for labs. We found it’s time-consuming and redundant to maintain the standalone METRIX Tool. We believe that the information gathered through METRIX Tool could be gathered through the CAVS Tool and Cryptik Tool for CAVS Metrics and CMVP Metrics respectively.

The CAVP can add this information to this screen. For now it will not eliminate the METRIX Tool but maybe this will be considered in the future.

17. Suggested additions to this information:

a. Description of tests harness, and version number(s)

b. Configuration management system(s) used for version control of the implementation under test and test harness (as applicable)

Handbook 150 and 150-17 gives detailed information on the records that shall be kept by a laboratory on the testing of algorithms and modules. This detail of information should be in those records at the CSTL. Because this information is maintained at the CSTL, the CAVP will not collect this information.

18. What signatures are required under the possible scenarios?

There are 5 different scenarios for performing the algorithm validation. They are:

If the CAVS test vectors are applied to the IUT:

1. by the CSTL at the CSTL
2. by the CSTL at an offsite location
3. by the CSTL at the vendor facility
4. by the vendor at the vendor site and directly observed by the CSTL
5. by the vendor at the vendor site and unobserved by the CSTL

Depending on which scenario applies to the IUT, the cover letter will require the appropriate signatures: if the testing is performed by a tester at the CSTL, the tester's signature will be required; if the vendor performs the testing and an observer from the CSTL observes the testing, both the vendor's tester and the CSTL's observer's signatures will be required; if the testing is performed by a vendor's tester unobserved by the CSTL, then the vendor's tester's signature will be required.