

Swedish Certification Body for IT Security
Scheme Note 25 - Use of CAVP-tests in CC evaluations

Scheme Note

| | | |
|---|--|----------------------|
| Decision Date 2017-11-30 | Matter ID CR-2458 | |
| Decision by (Name/Title) Mats Engquist, delegated by Dag Ströman, Head of CSEC | Scheme Note Number 25 | Dnr 17FMV9859-4:1 |
| Presentation by Jerry Johansson | Present at the Meeting CCB 2017-11-30 | |

Schematolkningens innebörd/Scheme Note Statement

Description and References

Background

It is common that products under evaluation also have undergone CAVP testing. Under certain conditions, these tests may be used as evidence of testing in the CC evaluation.

Use of CAVP testing as complementary developer testing

At EAL2 and above, developer testing is required. CAVP testing may be used as part of this testing if:

- The CAVP testing was performed on the same version of the TOE as the one under CC evaluation, or
- the CAVP tested components and the relevant environment (e.g. processor, operating system) are identical to those of the TOE under CC evaluation.

The tests may only be used for (module) testing of FCS class SFRs, i.e. key generation/management and cryptographic operation SFRs.

Note that the CAVP tests use internal interfaces and does not necessarily test the TOE as delivered to the end user. Therefore, cryptographic primitives (described in FCS_COP.1 requirements) also must be verified within the scope of the CC evaluation, preferably by testing TOE in its finalized form through external interfaces.

The developer must be prepared to provide more information about the CAVP testing if the CAVP certificate text does not provide sufficient detail about the versions of the tested products.

Use of CAVP testing as complementary evaluator testing

In evaluations where no developer testing occurs, such as certain NIAP PPs and cPPs, CAVP testing may be used as evidence of evaluator testing, provided the following conditions are being met:

- The CAVP testing was performed on the same version of the TOE as the one under CC evaluation, or
- the CAVP tested components and the relevant environment (e.g. processor, operating system) are identical to those of the TOE under CC evaluation.

The tests may only be used for testing of FCS class SFRs, i.e. key generation/management and cryptographic operation SFRs.

Note that the CAVP tests use internal interfaces and does not test the TOE as delivered to the customer. Therefore, externally visible functionality (such as FCS_COP.1) also must be covered within the CC evaluation by testing through external interfaces of the complete TOE in its finalized form.

The CAVP testing must be performed under the authority of the evaluation facility performing the CC evaluation, i.e. by staff reporting to and that are accountable to the ITSEF performing the CC evaluation. Thus, the evaluation facility will be able to provide clarifications regarding the testing if necessary.

Swedish Certification Body for IT Security
Scheme Note 25 - Use of CAVP-tests in CC evaluations

It must be explicitly shown that the tests required by the ST (and PP) actually are covered by the CAVP testing. When there are detailed test instructions (in the PP or a supporting document), mapping from the test instructions to suitable CAVP documentation shall be made with comments explaining the degree of similarity covering each test case covered by CAVP testing.

Appended Documents