

Netherlands Scheme for Certification in the Area of IT Security (NSCIB)



Nederlands Schema
voor Certificatie op het
gebied van IT-Beveiliging
(NSCIB)

NSCIB Scheme Instruction 08

Performing Testing

Approved.....
Technical Manager NSCIB

Instruction	08
Report title	Performing Testing
Date of issue	1 October 2017
Version	2.3
Distribution	Public
Filename	NSI_08_Performing_Testing_v2.3.docx

1 Purpose of this document

According to the NSCIB documentation rules supervision of the (penetration) testing is generally agreed upon during the preparation phase of the certification process. NSCIB (commercial) certifiers endeavour to attend (penetration) testing based on the evaluator's chosen test approach and initial vulnerability analysis. This instruction provides the rules an ITSEF has to follow for performing (penetration) testing.

2 Preparation

The ITSEF must submit a test plan to the (commercial) certifier for review. The test plan is required to cover ATE_IND.x.2E/3E and AVA_VAN.x.4E activities as appropriate for the claimed EAL.

Before undertaking any test activities related to ATE and AVA work units the test plan must be approved by the (commercial) certifier. Results from evaluator testing activities performed on the same product under a different scheme (e.g. EMVCo) can only be re-used when agreed by the (commercial) certifier during the kick-off meeting and as described in the work plan. The (commercial) certifier reserves the right to witness functional testing and penetration testing and to involve additional experts particularly in evaluation areas related to RNG evaluation, cryptographic aspects and side channel assessments.

3 Location

In general it is required for the evaluator to perform (penetration) testing activities at the ITSEF location. It is accepted there might be situations where this is undesirable or not possible. These situations could be:

1. Testing to be performed during manufacturing/production

For some products (e.g. smartcards) certain tests can only be performed during the manufacturing phase, as certain interfaces that are needed to test low level functionality are not available in the finalized product.

2. Physical size limitations

Some products are physically too large to be housed at the ITSEF or require special environmental conditions that are not available at the ITSEF facility.

3. Test equipment not available at ITSEF

Some (bespoke) test equipment could be too expensive for an ITSEF to acquire. For these tools it is allowed for the ITSEF to use equipment at a third party facility.

All deviations from the general rule must be identified in the work plan and approved by the (commercial) certifier.

In all cases the ITSEF remains responsible for the testing done. The evaluator must be present and must instruct the operating personnel to perform the testing in accordance with the test plan. In some cases it is more efficient to ask the developer to support the creation of test scripts etc. that implement additional independent tests as defined by the evaluator. Then the evaluator is expected to be able to verify that the script, created by the developer on behalf of the evaluator, accurately implements the purpose of the test.

Another special category are networking products. These products might be tested remotely by the evaluator from the ITSEF facility while the actual TOE remains at a different location. In these cases the evaluator remains responsible for installing and configuring the TOE within the test environment in person at the remote site. As such the evaluator can verify that the procedures described in the guidance for AGD_PRE.1 are correct (see also ATE_IND.x-1, ATE_IND.x-2 and equivalent AVA_VAN work units).

4 Test plan

The test plan must build upon the developer test activities and at a minimum, cover the following aspects:

- the developer functional testing the lab intends to repeat;
- the additional independent testing will be performed;
- the rationale for the sampling strategy;
- the penetration testing that the lab intends to perform.

It is mandatory as part of the additional independent testing to define alternative tests to those defined by the developer.

5 Execution

The testing shall be executed according to the test plan. Any deviations will be communicated to the (commercial) certifier and must be approved.