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	6 August 2021
Version	2.7
Distribution	Public
Filename	NSI_08_Performing_Testing_v2.7.doc

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Purpose of this document

This instruction provides the rules an ITSEF has to follow for performing (penetration) testing. It also describes other aspects of testing such as how public domain vulnerabilities have to be handled in the test plan, the cut-off date for consideration of public domain vulnerabilities and how the attack potential rating of a TOE can be increased with its guidance.

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 certifier. The 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 Evaluation Work Plan and approved by the 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 ITSEF intends to repeat;
- the additional independent testing will be performed;
- the rationale for the sampling strategy;
- the penetration testing that the ITSEF 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 certifier and must be approved.

6 Validity of test results

As the date of approving the ETR or issuance of the certificate may have consequences for the re-usability in composition activities, there must be a limit defined for the validity of testing activities. Internationally it is agreed that the validity of ATE testing is indefinitely as long as the TOE does not change.

The validity of AVA vulnerability analysis and pen testing is limited to 6 months. This means that the maximum time frame between these activities and the approval of the ETR can be no longer than 6 months. If this time frame is exceeded, the evaluator will need to provide argumentation to the certifier why the results can still be used. This argumentation shall include a renewed analysis to confirm that the pen testing is still state of the art and no new vulnerabilities and attack methods have been identified.

The certifier reserves the right to request a renewal/verification of the related activities.

7 Re-use of test results

Results from evaluator testing activities performed on the same product under a different scheme (e.g. EMVCo) can only be re-used when described in the Evaluation Work Plan and approved by the certifier. The validity of the test results as described in section 6 also apply for this re-use.

The ITSEF is obliged to inform the scheme about their intention Evaluation Work Plan and provide information when the scheme can expect the test plan and/or test results from the earlier testing. At the second evaluation meeting the ITSEF has to present the test plan in which it is described which tests are planned to be re-used and which additional testing will be done. In the third evaluation meeting the ITSEF has to present the results of all testing done.

8 Handling of public domain vulnerabilities

In general it can be stated that the search for public domain vulnerabilities is not a one-time activity performed at a given point in the evaluation; it should be a continual activity during the conduct of the evaluation. Some Common Criteria schemes even state that vulnerabilities posted in the public domain up to the point of certification have to be considered in the evaluation. For software centric TOEs where security patches are frequently issued, this may result in a never finishing evaluation and certification process. Therefore under the NSCIB the following rules apply:

1. Within an evaluation, it is the intention that the evaluation results are effectively accepted at the successful conclusion of final (3rd) evaluation meeting. Evaluation activities are ongoing to until this meeting, and as part of those ongoing evaluation activities the public domain should be actively monitored for release of further potential vulnerabilities that are relevant to the TOE. Any relevant public domain vulnerabilities posted prior to the date of the final evaluation meeting should be considered by the evaluators.

2. The treatment of any vulnerabilities announced between the date of the final evaluation meeting and publication of the certification report will be considered on a case by case basis by the certifier. The consideration will be influenced by factors such as attack potential rating, prevalence of vulnerability in product type, possible workarounds, how easy it is to fix, etc.

9 Handling of potential vulnerabilities identified by the scheme or otherwise

There are cases where the scheme has identified potential vulnerabilities that are considered to be inconsistent with the assurance requirements.

In those cases the ITSEF should perform an assessment of all potential vulnerabilities specifically identified by the scheme for consideration within a given evaluation. This assessment may determine that the required attack potential for a potential vulnerability is beyond that of the AVA_VAN component specified in the ST. This analysis should be reported in the ATE/AVA presentation.

It can occur that applicability of those potential vulnerabilities will require access to lower levels of design representation (e.g. source code) than are available according to the EAL. For example the analysis of an Open Source crypto library requires access to the source code in order to identify the publicly reported issues. The evaluators need to consider whether any of the potential vulnerabilities are easily transferrable with a lower attack potential to other cryptographic libraries that have been developed based on the Open Source library.

Similarly the scheme can also require the evaluators to demonstrate particular functionality in the ST that may require the evaluators to have a greater understanding of the design than required by application of the ADV requirements. For example, if the ST includes the extended component FCS_RBG_EXT.1 (e.g. taken from NDPP) for random number generation, and the component includes statements like "...the RBG shall be seeded with a minimum of 256 bits of entropy…", then the evaluator has to test the statement. This may require the evaluator to have access to more information than would be required to satisfy the ADV components and would seem to be inconsistent with the assurance package. However, the ST should only include such a statement if the evaluator is able to verify it in the evaluation activities.

It should be noted that the Protection Profiles where this sort of extended component is taken includes assurance activities to specifically address the testing of such as requirement. Therefore any ST that includes this extended component should likewise include the necessary assurance components (e.g. higher EAL) or the explicit assurance activities to test the requirement.

Otherwise, without such assurance activities it would indicate there is an inconsistency in the ST between the SFRs and SARs. This would require modification or removal of the functional requirement or revision of the assurance package claim to ensure the functional and assurance requirements in the ST are consistent.

10 Use of guidance to increase attack potential rating

10.1 Principles for increase of rating using guidance

In order to achieve the necessary attack potential rating and meet the AVA_VAN claim, the TOE sometimes relies on the operational environment (physical and/or logical) to provide additional protections. Any protection provided by the operational environment must be clearly specified in the operational guidance document (as assessed in AGD_OPE.1). These protections are taken into account when calculating attack potential, often as part of the *Window of Opportunity* rating. They may also be taken into account when considering a full attack path that requires multiple partial attacks, some of which are countered by the TOE and some that are countered by the operational environment (such as an operating system that will later be composed with the current TOE as part of a composite evaluation).

However, it is view of NSCIB that over-reliance on the environment can degrade the meaning of a TOE certificate. As such guidance should typically only be used to raise the attack potential rating of a TOE by **a single level**, although it is recognised that in isolated cases, it may be acceptable to rely on guidance to raise the rating by two levels. The principles are outlined as follows:

1. It is typically possible to use guidance to raise a single level (e.g. from Basic to Enhanced-basic), as long as the guidance is reasonable (the guidance presents realistic measures that are possible to implement and do not compromise the expected use of the TOE).
2. In rare instances it is permitted to raise the rating by 2 levels (e.g. from Enhanced-basic to high). This is only permissible if the ITSEF can provide a rationale that the measures/mechanisms described in the guidance are in line with industry standard practice (e.g. for a composite product where the platform TOE is susceptible to perturbation attacks and relies on the operating system that it will be composed with to provide program flow checking mechanisms). The evaluator rationale must demonstrate that the implementation of the described measures will not compromise the effectiveness of the composed TOE (i.e. the measures do not incur prohibitive slowdown or increased power consumption requirements, etc).
3. Lifting the attack potential by 3 levels is not permissible in the NSCIB scheme.

10.2 Testing by ITSEF

The ITSEF must *test* the effectiveness of the combination of the TOE plus the complementary measures described in guidance. This *testing* may be achieved through use of test software with the TOE (e.g. sample software installed on a hardware platform TOE) or through analysis. This testing must demonstrate an existence proof. If there is a proven code example of the guidance, then it needs to be documented. If analysis is performed it must include a rationale to demonstrate that the guidance is reasonable and practicable.

10.3 Composition

In composite evaluations, the evaluator has **no** justification for not testing, so the implementation of the guidance has to be tested on the platform during the composite evaluation.

10.4 Reporting

The penetration testing effort must be described in terms of at least the total amount of weeks of testing and the percentage of that time spent per attack category. The evaluator should use the following format (including only the relevant categories of penetration testing):

> "The total test effort expended by the evaluators was < nn > weeks. During that test campaign, <…%> of the total time was spent on physical attacks, <…%> overcoming sensors and filters, <…%> perturbation attacks, <…%> retrieving keys with FA, <…%> side-channel attacks, <…%> exploitation of test features, <…%> attacks on RNG, <…%> ill-formed Java Card application, <…%> software attacks, and <…%> application isolation penetration tests."

Where guidance has been used to increase the rating of the TOE's attack potential, this will be reported in the Certification Report.

If the rating is increased by a single level, the CR will draw attention to any particularly unusual guidance provided, but will otherwise just retain the usual CR statement of:

> *"Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE."*

If the guidance has been used to increase the rating of the TOE's attack potential by two levels, the evaluator needs identify the sections in the guidance that address this, and the statement in the CR will be revised to read:

> *"This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in <ref to sections>. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained."*