Licensing of evaluation laboratories for the Dutch scheme for Baseline Security Product Assessment (BSPA)

Date May 3, 2017

Colophon

Our reference number : 8c01bddc-or1-1.3

NLD DISS ref. number : 0

: T +31 (0)79 320 50 50

: F +31 (0)70 320 07 33

: P.O. Box 20010
2500 EA The Hague
The Netherlands

Author(s) : NLNCSA

Number of enclosures : 0

Table of contents

Introduction

The Dutch *Scheme for Baseline Security Product Assessment* (BSPA) evaluates the security features of hardware and software security products for use in the "sensitive but unclassified" domain that is covered by the Dutch *Baseline Informatiebeveiliging Rijksdienst* (Government security baseline, in short: BIR). The process is designed to work within a bounded scope and modest cost, in time and money. The process is also designed to work without non-disclosure agreements and without the cooperation of the product developer.

This document describes the licensing process for the evaluation laboratories that want to work within this scheme:

- Determining the evaluation lab's ability to perform assessments according to the BSPA criteria and methodology, and
- Determining the evaluation lab's technical expertise for the types of products that are within their licensing scope, and
- Ensuring the evaluation lab's impartiality and independence of the developer, and
- The compatibility of the evaluation lab's legal structure and organisation with these goals.

1 Licensing procedure

1.1 Application by candidate evaluation lab

A candidate evaluation lab must apply for licensing by sending the *BSPA licensing application form* to the Overseer (the NLNCSA). In doing so, the candidate evaluation lab agrees to follow the requirements set out in *Appendix A: Licensing requirements*, *Appendix B: Scope of licensing* and *Appendix C: Evaluation lab obligations.* In case of a successful outcome the evaluation lab will be placed on a public list of licensed evaluation labs, together with the applicable licensing domains.

The following information and documentation must be provided together with the licensing application form:

- A formal copy of the registration of the company in the Dutch Chamber of Commerce (KvK);
- Specification of the product categories and technical domains for which licensing is sought, as defined in *Appendix B: Scope of licensing*;
- A technical dossier demonstrating the professional capability of the candidate evaluation lab, including:
  - A general presentation of the company, including the various departments, teams, managers, responsibilities and roles. If the candidate lab is part of a larger organisation, organisational charts and description of the interaction with the larger organisation are required;
  - An overview of relevant professional experience and recent national and international references. The candidate evaluation lab must provide proof of expertise, experience, tooling and equipment in the intended product categories and technical domains;
  - The list of technical experts to be part of the licensing, and their resumes, demonstrating the required technical expertise.

The following information and documentation may be provided together with the licensing application form:[1]

- Any relevant accreditations the candidate lab has received for their quality system (like ISO9000), their evaluation activities (like Common Criteria), their technical facilities, their technical expertise etc.;
- Any accreditations the candidate lab has received to perform classified work and to handle classified information;
- A proposed pilot evaluation project;
- Any other relevant information about the candidate evaluation lab.

1.2 Confirmation of receipt of the application

The Overseer confirms receipt of the application. A staff-member of the Overseer is assigned to lead the licensing process of the candidate evaluation lab. Most notably this includes arranging the audit of the candidate lab.

1 This might make the licensing process easier and quicker.

1.3 Preliminary licensing audit

A preliminary audit is conducted at the location of the candidate evaluation lab to assess its ability to meet the licensing criteria listed in *Appendix A: Licensing requirements*. The Overseer documents the results in an audit report.
If the results are satisfactory, the candidate evaluation lab receives approval for the pilot evaluation.

1.4 Pilot evaluation

The candidate evaluation lab must perform a pilot evaluation to enable the Overseer to assess the candidate’s capabilities to carry out an evaluation under the BSPA scheme.

It is the candidate lab's own responsibility to negotiate and obtain a pilot evaluation project from some Sponsor. The Sponsor must be informed of the licensing status of the candidate lab, and the corresponding risks for the evaluation. In particular, the statement of conformance for the product will only be issued after successful licensing of the lab.

The pilot evaluation must be performed according to all BSPA procedures. It is subject to enhanced oversight from the Overseer.

The candidate evaluation lab has one year, starting from the approval for the pilot evaluation, to acquire a BSPA evaluation assignment and to complete the pilot evaluation. If this period is exceeded, the licensing process has to start anew.

1.5 Licensing audit

At the end of the pilot evaluation, the Overseer performs a new audit of the evaluation lab if necessary. The Overseer will verify that any non-compliancies identified during the pilot evaluation process have been addressed.

If the audit is successful, the Overseer issues a final licensing audit approval, which indicates that the candidate evaluation lab meets all licensing criteria listed in *Appendix A: Licensing requirements.*

Also the licensing audit approval indicates the scope of the license within which the evaluation lab may carry out assessments. The different product categories and technical domains are described in *Appendix B: Scope of licensing*.

1.6 Licensing decision

The Overseer will communicate the licensing decision to the contact person of the evaluation lab in writing.

After a positive licensing decision, the evaluation lab is licensed for two years. The evaluation lab will be listed on the Overseer's public list of licensed evaluation labs.

1.7 License monitoring

Once licensed, an evaluation lab must meet the licensing requirements continually. The Overseer monitors the evaluation lab periodically, to ensure that the obligations listed in *Appendix C: Evaluation lab obligations* are met by the evaluation lab. The Overseer can perform an audit of the evaluation lab at any time, to verify that the licensing criteria and obligations are met.

2 License scope changes

2.1 Triggers for a scope change

A scope change can be initiated:

- At the request of the evaluation lab that wishes to change the scope of its license;
- At the initiative of the Overseer, if he decides that changes in the evaluation lab's situation (skills, status, staffing etc) warrant change of the licensing.[2]

2.2 Scope change at the request of the evaluation lab

The evaluation lab sends the Overseer a request for change of the scope of its license, together with supporting evidence. This request may lead to a repeat of part of the licensing procedure (possibly restarting at the licensing step *Preliminary licensing audit* or step *Pilot evaluation*). Enlargement of the scope will most likely require a supplementary audit of the evaluation lab.

The Overseer assigned to the lab follows the procedure *Licensing decision* described above to communicate the decision.

2.3 Scope change at the initiative of the Overseer

When the Overseer is of the opinion that the licensing conditions are no longer met so that the scope of the license must change, the Overseer informs the evaluation lab of this opinion. The Overseer will give the evaluation lab a reasonable time period to implement the corrective measures.[3]

After the evaluation lab has demonstrated that the raised issues have been addressed, and have been found resolved according to the Overseer, or at the latest after the time limit determined by the Overseer has expired, the license will be reassessed by the Overseer. The result is communicated following the procedure *Licensing decision* described above.

2 For example: if members of the evaluation lab with key skills leave, the Overseer may reduce the number of product categories for which the evaluation lab is licensed.

3 For example: the evaluation lab will have one month to respond with an improvement plan from the date of being put on notice.

3 License renewal

A license can be renewed at the request of the evaluation lab. The evaluation lab shall request renewal no later than 4 months before expiry of the current license.[4]

A new audit is performed following the procedure *Licensing audit* and the relevant and necessary licensing steps are followed.[5] Deviations and issues raised in evaluations during the current licensing period will be examined, and also the re-mediation of these issues.

The Overseer assigned to the lab follows the procedure *Licensing decision* described above to communicate the decision.

4 So: not later than 20 months after receiving the license.

5 Which steps are relevant and necessary is determined by the Overseer. This depends on the behaviour, performance and results of the evaluation lab during the licensing period.

4 License suspension and revocation

4.1 Reasons for suspension or revocation

The license may be suspended and revoked by the Overseer if the evaluation lab no longer meets the obligations related to its license as listed in *Appendix A: Licensing requirements*, does not fulfil the *Appendix C: Evaluation lab obligations*, or if there is no activity, or insufficient experience or tooling within the license scope.

The Overseer follows the procedure *Scope change at the initiative of the Overseer* to inform the evaluation lab of impending suspension or revocation of the license.

During the suspension of the license, the Overseer may still decide, on a case by case basis, to allow new evaluations by the lab, taking into account the results of previous evaluations.

4.2 Revocation of the license

The Overseer may revoke the license of the evaluation lab for various reasons, including but not limited to:

- The evaluation lab no longer meeting the *Appendix C: Evaluation lab obligations*;
- The evaluation lab not addressing the items raised for the suspension in a timely manner;
- Reasons related to the interests of national defence and national security.

4.3 Consequences of losing the license

Loss of the license (by revocation or non-renewal) results in the evaluation lab being removed from the public list of licensed evaluation labs.

No new evaluations from this lab will be accepted by the Overseer. The evaluation lab must provide the Overseer with all records related to the evaluations being performed. The Overseer will decide, on a case by case basis, if ongoing evaluations can be completed or if they will be stopped without issuance of a statement of conformance.

The Overseer can prevent the Sponsors, Developers and other stakeholders access to the ongoing evaluations.

5 Appendix A: Licensing requirements

5.1 Independence and impartiality of evaluations

The evaluation lab must provide evidence and commitments to ensure that the evaluations are performed in an independent and impartial manner:

- Independence: the evaluation lab does not perform evaluations that could lead to a conflict of interest with the developer, distributor or importer of the product.
- Impartiality: the evaluation lab can not be influenced to change the results of the evaluation;

5.2 Confidentiality

The evaluation lab must demonstrably be able to guarantee the confidentiality of the evaluations and their results.

5.3 Staff requirements

Staff assigned to evaluations must be competent in information technology, as well as trained and experienced in security evaluations. The staff competence must be aligned with the product categories for which the evaluation lab is licensed. The Overseer determines whether the competence is sufficient for the security evaluations.

Staff assigned to evaluations must be identified by name. The evaluation lab must manage the skills and experience of the staff, including keeping a record for each product evaluation of the specific tasks, in that evaluation, that a staff member has participated in.

The Overseer may deny individual staff members to be part of an evaluation.

5.4 Contractual requirements

The commercial aspects of a product assessment should be arranged between the evaluation lab, the Sponsor, and in some cases the Developer.

All product assessment contracts must specify that the Overseer receives all information about the assessment process.

5.5 Technical skills

At the request of the Overseer, the evaluation lab must be able to demonstrate the knowledge, skills, tools and equipment matching the license scope. This demonstration must be performed within a reasonable time limit set by the Overseer.

5.6 Working procedures

Evaluation technical reports must pass an internal quality control process before being sent to the Overseer.

The evaluation technical report must be approved by an authorized representative of the evaluation lab.

6 Appendix B: Scope of licensing

6.1 Definition of the scope of licensing

The licensing scope is defined in terms of product categories. The Overseer may grant waivers for special cases that are not explicitly covered by the licensing scope or product categories.[6]

6.2 Licensing domains – scope of the license

The following product categories are defined for BSPA services:

	Product category[7]	Examples[8]
01	Network security	VPN, link encryptor, WiFi access point, etc.
02	Network filtering, detection and response	IDS, firewall, SSL proxy, etc.
03	Secure messaging	Secure mail, secure chat-app, secure voice-call-app etc.
04	Media and file security	Full disk encryption, container encryption, file encryption, data erasure, etc.
05	Identity and access management	Password manager, keymanagement and distribution, two-factor authentication, access control and federation, etc.
06	Secure OS execution environment	Secure-OS, secure-hypervisor, micro-kernel, separation kernel, etc.
07	Hardware and embedded software	HW-based encryption, HW-based secure-boot, USB device, keyboard (KVM-) switch, smart-meter, tamper resistant device, etc.
08	Smart cards and similar devices	Secure ICs, JavaCards, transportation/access cards, etc.

Within each category, restrictions may be issued by the Overseer on the types of product that the evaluation lab may evaluate.

6.3 Licensing scope publication

The evaluation lab, together with its product categories, will be listed on the Overseer's public list of licensed evaluation labs.

6 Product categories and their boundaries can never be defined with 100% precision so discussions about scope are to be expected. The Overseer has final say in all discussions concerning product catgegories.

7 A specific security product can be part of several domains. For example: a Mobile Device Management product might contain Network security, Network filtering, Secure messaging, Media and file security and Identity and access management.

8 The examples are not limitative and are for orientation only.

7 Appendix C: Evaluation lab obligations

The evaluation lab must follow the procedures set by the Overseer. The evaluation lab must comply with all licensing requirements, especially, but not limited to:

1. Refusing any evaluation that could lead to a conflict of interest, and informing the Overseer as soon as such a conflict of interest becomes apparent;
2. Only outsource any part of the evaluation with prior approval by the Overseer;
3. Ensuring that evaluators assigned to an evaluation have not been part of the development or production of that product, e.g. no consulting, co-design or implementation support;
4. Report any important change of the structure of the evaluation lab, its organization or staff, and provide supporting documentation of such changes;
5. Allow the Overseer full access to the evaluation lab premises, evaluation documentation, tools and equipment that are within the license scope;
6. Allow the Overseer to check any evaluation activity, including witnessing of evaluation work performed and checking the compliance with the licensing requirements;
7. Follow any confidentiality requirements imposed permanently or temporarily by the Overseer;
8. Attend meetings organized by the Overseer.