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 12

Project Communication

Approved.....
Technical Manager NSCIB

Instruction	12
Report title	Project Communication
Date of issue	1 June 2018
Version	1.2
Distribution	Public
Filename	NSI_12_Project_Communication_v1.2.docx

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Purpose of this document

To make sure that certification project related communication between al involved parties is done in a way that ensures that all relevant information will be exchanged in an appropriate manner.

2 Communication point-of-contacts

This NSCIB Scheme Instruction (NSI) is written to standardise the project related communication between the sponsor, the IT Security Evaluation Facility (ITSEF) and the (commercial) certifiers of Certification Body (CB).

The point-of-contacts for each certification project will be defined in the application form submitted by the sponsor and ITSEF to TÜV Rheinland Nederland. From the sponsor side these contacts are usually the project/product manager and the certification manager. From the ITSEF side these are usually the evaluation project manager and the lead evaluator.

The NSCIB works with commercial certifiers who are appointed per certification project. The name and email address of the appointed commercial certifier will be communicated by TÜV Rheinland Nederland to the sponsor and ITSEF after acceptance of the application form. A commercial certifier works under supervision of a governmental certifier whose name is also communicated after acceptance of the application form.

3 Communication arrangements

3.1 Electronic communication

All certification related information exchange by electronic means (typically emails) that is addressed to the CB shall include the (commercial) certifier, and the general email address of the governmental certifiers (nscib@nlncsa.nl). The only exception is information related to financial aspects as this is only exchanged with TÜV Rheinland Nederland.

Project related email communication to the CB shall be identified by the certification/project ID as assigned by the CB (see NSI_06_Certification_ID_numbering) in round brackets in the subject line.

3.2 Paper communication

All hard copies sent by the sponsor, the ITSEF or TÜV Rheinland Nederland shall be sent by regular mail or courier. Sending hard copies is strongly discouraged, but will be used to send the original signed certificate from TÜV Rheinland Nederland to the sponsor.

3.3 Confidential exchange of information

The commercial encryption program PGP (or open source equivalent GPG) shall be used to assure the confidentiality and integrity of information of a sensitive or proprietary nature that is exchanged by electronic means. This shall be done as an encrypted document or zip-file stored on a ITSEF operated (s)ftp server or as an attachment to an unencrypted email body. No s/mime or encrypted mail bodies shall be used.

Before sensitive or proprietary information is exchanged, PGP public keys (2.048/4.096 bit RSA/DSA) are exchanged between the identified point-of-contacts. The public keys of the commercial certifiers and the general NSCIB public key can be found on the NSCIB website. TÜV Rheinland Nederland should not receive any sensitive or proprietary information via email and will not be able to decrypt such information.

3.4 Types of information exchange

Evaluator deliverables like the Evaluation Technical Report and all other documents specified in the Evaluation Work Plan shall be submitted by the ITSEF to the (commercial) certifier, and optionally to the sponsor.

Also all information exchange between sponsor and ITSEF of evaluation related technical matters shall be copied to the (commercial) certifier using the rules as stated in sections 3.1 and 3.3 above. Examples of such information exchanges are:

- Minutes of meeting;
- Technical discussions;
- Evaluation process related issues;
- Preliminary reports/presentations.

Additionally, the (commercial) certifier shall receive monthly status updates as required by section 5 of this instruction.

At the end of a project the (commercial) certifier delivers a draft Certification Report to both the sponsor and ITSEF for technical review before the Certification Report is finalised and a certificate is issued and published.

3.5 Document format and language

All project communication and documents shall be in (UK) English or Dutch.

Documents shall be delivered in pdf format that allows to copy text from the document and to add notes. If available, a MS-Word / MS-Excel/ MS-PowerPoint version of the pdf document can be requested for practical purposes.

All documents shall be labelled with an unambiguous document number, a version number, a date, and the certification/project ID as assigned by the CB. All sensitive or proprietary information shall be labelled as such. It is not required to use this labelling on every page.

A version numbering method shall be used that uniquely identifies a document. Any changes in a document shall result in a new version number and a new date. When a new version of a document is delivered, a clear method for marking changes between two formally delivered versions shall be applied to ease determination of these changes.

4 Minutes of Meetings and actions

During a project several meetings are being held and in accordance with the scheme procedures it is expected that the ITSEF records the outcome of these meetings by taking minutes and actions. This section provides the requirements for the content of the Minutes of Meetings (MoM) and on the actions noted in them. The goal of these requirements is to have a harmonised way in which the (commercial) certifier is able to perform oversight by tracking and tracing actions and to conclude that all relevant information is included in his project dossier.

4.1 Requirements on MoMs

For all Minutes of Meetings, the following requirements apply:

- The date, time, location and attendees of the meeting shall be recorded.
- All documents and presentations that the lab has delivered for discussion at the meeting shall be listed by name and version;
- All revised documents and presentations coming out of the meeting shall be listed by name and version. Ideally, outputs of a meeting, should be attachments to the MoM;
- Certifier notes that go into the meeting and the certifier notes as a result of the meeting shall be listed;

- The final conclusion of the meeting shall be recorded (see also NSP#6 for the 4 possible outcomes). This also includes a verdict on each of the documents presentations discussed at the meeting.

4.2 Requirements for notation of actions

For the notation of actions, the following requirements apply:

- One identifier per action item in order to trace the action in the monthly reports;
- When the action relates to a document or presentation, the action item should refer to that document or presentation, including its version;
- Also, when an action is closed, the action item should clearly state how the actions was closed, e.g. by reference to the document or presentation where the action was closed;
- Per action item it shall be noted, if the certifier has approved its closure.

5 Evaluation Work Plan and monthly project status updates

According to the NSCIB documentation rules an Evaluation Work Plan must be agreed upon during the preparation phase of the certification process. This Evaluation Work Plan shall contain the elements described in Annex B of the NST_01_NSCIB_Application_Form template and forms the baseline for the evaluation and certification work.

As projects usually continue for several months it is expected that the agreed Evaluation Work Plan becomes outdated due to changes in scope, staffing, priorities and/or scheduling. This section provides the rules an ITSEF has to follow for informing the CB on relevant changes to the Evaluation Work Plan and requires a monthly project status update.

5.1 Changes related to the Evaluation Work Plan

An Evaluation Work Plan forms the baseline for the evaluation and certification work. As it is agreed upon by all involved parties it cannot be changed or executed in a different way by a single party. Possible changes that might have an impact can be categorised as follows:

- *Re-scheduling of milestones; these include both deliverables and review meetings;*
  The assigned certifier(s) expects to review documents and attend review meetings based on the agreed planning. They reserve time in their agenda which is difficult to re-allocate if deliverables are not submitted at the agreed date. The same is also true for any re-scheduling of meetings.
- *TOE scope changes;*
  The TOE scope is discussed at the project kick-off meeting and is accepted as being a valid TOE scope by the Certification Body. Changes to the TOE scope mostly have an impact on the evaluation work already performed and could in extreme cases even result in inappropriate removal of security features or inappropriate additions of assumptions. In any case these changes must be reported as soon as possible so that their impact can be determined. This may potentially lead to additional certification costs.
- *Evaluation scope/approach changes;*
  Changes to the evaluation scope (e.g. more or less development sites to be audited), additional/different deliverables or when additional review meetings are needed always have an impact on the certifiers oversight activities and could lead to additional certification costs.
- *TOE name/identifier changes;*
  Changes to the TOE naming or its identifier must officially be reported by the developer to TÜV Rheinland NL in copy to the assigned certifier(s). Such changes are relevant for the Certificate and its related Certification Report. As these changes might also have an impact on existing deliverables, the ITSEF must also be aware.
- *Project staffing/ITSEF personnel assignment changes.*
  The certifier(s) only accept deliverables that are authored by the evaluators listed in the Work Plan. NSCIB rules require the ITSEF to only assign qualified CC evaluators who are known to the Certification Body and have successfully passed the NSCIB CC examination.

5.2 Monthly project status updates

The ITSEF Project manager who is responsible for the evaluation work is required to provide a monthly status update of his project. This status update is a document with a unique title and date and shall contain sections as follows:

- *Section one:* provides administrative project details, including the time period on which the project status updates reports on and the latest approved Evaluation Work Plan;
- *Section two:* lists the status of outstanding action items derived from the MoM of previous evaluation meetings. The requirements on the notation of actions in section 4.2 also apply here;
- *Section three:* provides a progress summary on the deliverables identified in the Evaluation Work Plan. It shall also describe any issues in the developer deliverables that are found during the evaluation activities and either ITSEF or developer need to address/have addressed;
- *Section four:* describes proposed changes structured along the categories defined above in section 5.1, whereby changes reported in earlier project status updates shall be retained as far as they have not been incorporated in a newer version of the Evaluation Work Plan.

The Project status update shall be submitted to the assigned certifier(s) ***on the first working day of every month*** as long as the monitoring phase continues. The certifier shall endeavour to provide written feedback within 3 working days.