

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 September 2017
Version	1.1
Distribution	Public
Filename	NSI_12_Project_Communication_v1.1.docx

1 Purpose of this document

To make sure that certification project related communication between all 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-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 NSI_13_Reporting_monthly_project_status_updates.

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.