

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



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

Document ID: **NSCIB_2.3.docx**
Document version: **2.3**
Date: **1 April 2017**
Number of pages: **65**
Number of appendices: **8**

Developed in cooperation with the Ministry of the Interior and Kingdom Relations (BZK)

Reproduction of this document is authorized provided the document is reproduced in its entirety.

Document History

Version	Issue	Remarks
1.0	23-02-04	Release at the beginning of the opening of the Scheme
1.1	22-03-04	Comment of RvA audit incorporated
1.2	09-12-04	Comment of RvA attendance incorporated
1.3	22-04-08	General update
1.9	18-02-09	Comments of SOG-IS audit incorporated
2.0	01-07-11	Major update to reflect TÜV Rheinland Nederland changes
2.1	01-08-11	Minor update to incorporate latest Quality Handbook references
2.2	10-08-15	Comments of CCRA audit incorporated and update to reflect extension of scope with site certification
2.3	01-04-17	Minor update to reflect TÜV Rheinland Nederland address change and to align with latest Quality Handbook

Contact Information

TÜV Rheinland Nederland BV, Arnhem

Visiting address

Westervoortsedijk 73
 6827 AV Arnhem
 The Netherlands

Postal address

P.O. Box 2220
 6802 CE Arnhem
 The Netherlands

Contact information

T: +31 88 888 7 888
 F: +31 88 888 7 879

Structure of the Scheme Documentation

Part 1: Introduction to the Scheme

This part describes the procedures of the central actor in the Scheme, the Certification Body and the relationship that this actor maintains with the other actors concerning a Certification.

Part 2: Regulations concerning a Certification

This part describes the process according to which a Protection Profile, IT product or system shall be certified, and the roles and responsibilities all actors have herein.

Part 3: Licensing of an ITSEF

This part describes the process according to which an Information Technology Security Evaluation Facility (ITSEF) shall be licensed, so that this ITSEF is subsequently authorised to perform Evaluations under the Netherlands Scheme.

Part 4: Roles in the Certification Body

This part describes the tasks and the division of roles in the Certification Body. Under the Netherlands Scheme, the roles in the Certification Body are carried out by different parties (TÜV Rheinland Nederland and the Ministry of the Interior and Kingdom Relations). The Certification Body carries out a number of tasks that are not directly related to Certification, such as taking part in international commissions.

Part 5: Appendices

This part comprises a number of templates for various reports and documents that are used under the Netherlands Scheme.

Remarks:

- § The scheme documentation does not provide any details of the criteria that are used for the issuance of Certificates (the Common Criteria). An overview of these baseline criteria and other relevant documents is provided in Part 2 of the Scheme Documentation.
- § The Quality Handbook of TÜV Rheinland Nederland [TÜV-KMS] also applies to 'Netherlands Scheme for Certification in the Area of IT Security'. To be able to distinguish the definitions used in the Quality Handbook from the specific Scheme definitions, they are printed in a typographically different way: [Times New Roman 12 pt].

CONTENTS:

Part 1 – Introduction to the Scheme

1. Introduction	8
1.1. Rationale and Scope	8
International recognition	8
European recognition	8
1.2. Scheme Status	9
1.3. Overview of an Evaluation / Certification Process	9
1.4. Editing, updating and circulation	9
2. Objectives and Tasks of the Netherlands Scheme	10
2.1. Objectives of the Netherlands Scheme	10
2.2. Tasks of the Certification Body	10
2.3. Roles in the Netherlands Scheme	11
3. Documentation Overview	12
3.1. Assessment Criteria of the NSCIB	12
3.2. Basic Documents for Scheme Documentation of the NSCIB	12
3.3. Documentation concerning the licensing of ITSEFs	12
4. Terminology	13
5. Glossary	17

Part 2 – Regulations concerning a Certification

1. Introduction	19
2. Certification Process	20
2.1. First Evaluation of a TOE/PP	20
2.2. Alternative Reporting Procedure	28
2.3. Assurance Continuity procedure	28
3. Regulation for the Certification Process	29
3.1. Premature Termination of the Certification Process	29
3.2. Configuration Management of Documents	29
3.3. Special Supervision	31
3.4. Security (Confidentiality and Integrity)	31
3.5. Cost of Certification	31
3.6. Regulations concerning Sub-contractors	32
4. Regulation Concerning Certificates	33
4.1. Certificate	33
4.2. Obligations of the Sponsor	33
4.3. Use of the International Certification Marks	33
4.4. Fees	34
4.5. Audit	34
4.6. Complaints	34
4.7. Disciplinary Measures	34

4.8.	Termination and Suspension of the Certification Agreement	35
4.9.	Publicity	35
4.10.	Validity of a Certificate	36
4.11.	Liability	36
4.12.	Objections and Appeal	36
5.	Assessment Guidelines Common Criteria	37
5.1.	Definitions and Amendments	37
5.2.	Uncertainty in the Assessment Guidelines Common Criteria	37
6.	Additional Stipulations	38

Part 3 – Licensing of an ITSEF

1.	Introduction	40
2.	Demonstrable Quality	41
2.1.	Conformance to this Requirement	41
2.2.	Maintaining Conformance to this Requirement	41
3.	Demonstrable Competence and Skills	42
3.1.	Conformance to this Requirement	42
3.2.	Maintaining Conformance to this Requirement	42
4.	Demonstrable Application of Assessment Guidelines	43
4.1.	Conformance to this Requirement	43
4.2.	Maintaining Conformance to this Requirement	43
5.	Demonstrable Security	44
5.1.	Conformance to this Requirement	44
5.2.	Maintaining Conformance to this Requirement	44
6.	The Licensing Process	45
6.1.	Start of the Licensing Process	45
6.2.	Kick-off Meeting	46
6.3.	Licensing Agreement	46
6.4.	Execution	46
6.5.	Licensing	46
6.6.	Prematurely Termination of the Licensing Process	46
6.7.	Publication	47
7.	Maintenance of the Licence	48
7.1.	Continuation of the License	48
7.2.	Suspension and Termination of the License	48

Part 4 – Roles in the Certification Body

1.	Introduction	50
2.	Roles in the CB	51

2.1.	Scheme Administrator	51
2.2.	Board of Appeal	52
2.3.	Evaluation Supervisor	52
2.4.	Scheme Supervisor	53
2.5.	Certificate Issuer	53
2.6.	License Issuer	53

3.	Internal Quality Processes	54
-----------	-----------------------------------	-----------

4.	International Recognition of Certificates	55
-----------	--	-----------

Part 5 – Appendices

1.	Application Form to Initiate a Certification Process	57
-----------	---	-----------

2.	Certification Agreement Template	58
-----------	---	-----------

3.	Work Plan Template	59
-----------	---------------------------	-----------

4.	Intermediate Report Template	60
-----------	-------------------------------------	-----------

5.	Review Report Template	61
-----------	-------------------------------	-----------

6.	Evaluation Technical Report Template (TOE)	62
-----------	---	-----------

7.	Certification Report Requirements	64
-----------	--	-----------

8.	Certificate Template	65
-----------	-----------------------------	-----------

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

Part 1 – Introduction to the Scheme

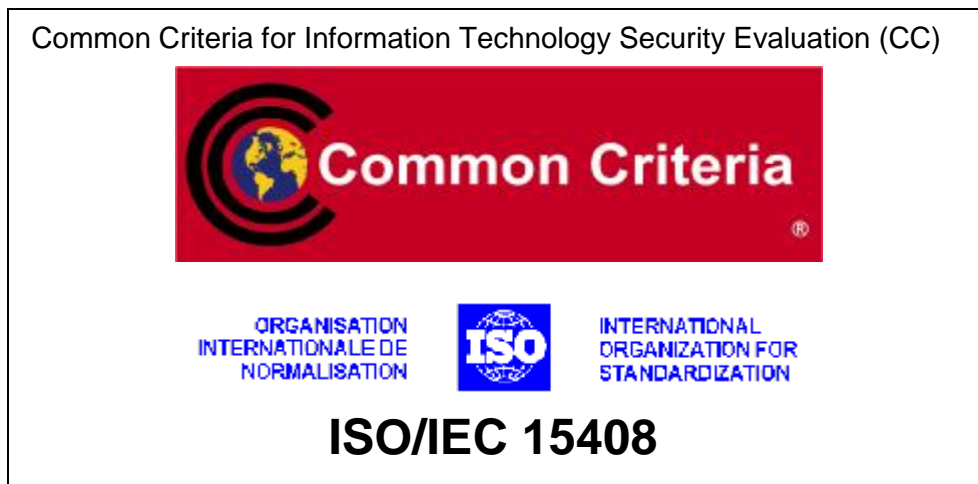


1. Introduction

This document gives an overview of the objectives, the organisation, and the procedures of the 'Netherlands Scheme for Certification in the Area of IT Security (NSCIB¹)'. This Scheme has been set up to enable the Evaluation and Certification of security aspects of information technology (IT). The objective of the Scheme is that IT products and systems in the Netherlands can be evaluated and certified in a way that conforms to the so called 'Common Criteria', an international methodology (ISO/IEC 15408 and ISO/IEC 18045) for Evaluation and Certification.

The objective of the Common Criteria is to provide a methodology to support, in an objective way, assurance that IT products and systems² in their user environment meet their security specification. To achieve this objective the Common Criteria defines:

- § The requirements IT products and systems shall meet;
- § The requirements manufacturers of IT products and systems shall meet;
- § The working method of evaluators to decide whether requirements are met;
- § The way this can be certified.



1.1. Rationale and Scope

The Netherlands government appreciates the need of Dutch consumers to gain understanding in IT security products, and also manufacturers (Dutch or otherwise) to make claims about the security functionality in their IT security products.

To deal with these needs, the Dutch government recognizes Common Criteria Certificates according to the international recognition arrangements that it signed up to. These are:

International recognition

The Common Criteria Recognition Arrangement [CCRA] has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance levels up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: <http://www.commoncriteriaportal.org>.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is

¹ NSCIB is the Dutch acronym for "Netherlands Scheme for Certification in the Area of IT Security".

² In the Common Criteria a system refers to a collection of products in a specific environment, e.g. the network of Pietersen Transport B.V.

provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: <http://www.sogisportal.eu>.

Following the initial recognition of Common Criteria Certificates from foreign countries, the Dutch government announced that it intended to issue Certificates itself that would be internationally accepted under the above mentioned international recognition arrangements. Therefore, the government has granted permission for setting up a Netherlands Scheme for the issuance of Common Criteria Certificates.

The Netherlands National Communication Security Agency (NLNCSA), which is part of the Ministry of the Interior and Kingdom Relations (BZK), was responsible for setting up of the Common Criteria Scheme in the Netherlands on behalf of the Dutch government. TÜV Rheinland Nederland has been asked to function as a Certification Body (CB) in this Scheme.

1.2. Scheme Status

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) is compliant with the requirements of both the international Common Criteria Recognition Arrangement (CCRA) and the European SOG-IS Mutual Recognition Agreement (SOG-IS).

1.3. Overview of an Evaluation / Certification Process

An Applicant (developer, distributor and/or user of an IT product/system) can apply at the CB for certification of this IT product/system. Subsequently, an evaluation shall be performed according to the Common Criteria of this IT product/system. This evaluation is performed by an independent evaluation laboratory. Such laboratory is internationally referred to as 'ITSEF' (Information Technology Security Evaluation Facility) [CCRA].

The ITSEF shall be licensed by the CB. The CB shall supervise every evaluation performed by the ITSEF.

On successful completion of an evaluation, the CB may decide to grant a certificate to the IT product/system. Certificates can be granted to IT products/systems, Protection Profiles, and Sites. These certificates will then be recognised internationally through the international agreements³.

1.4. Editing, updating and circulation

The scheme documentation is reviewed regularly for potential updates. The scheme documentation is distributed to the parties participating in the scheme and is also published on the website. All versions are stored by electronic means. The version of the scheme documentation that is published on the website is leading.

³ TOE independent Site Certificates are not yet part of international recognition within CCRA and SOGIS MRA.

2. Objectives and Tasks of the Netherlands Scheme

This chapter presents a brief overview of the objectives and tasks of the Netherlands Scheme for Certification in the Area of IT Security (NSCIB).

2.1. Objectives of the Netherlands Scheme

The objectives of the NSCIB are:

- § Quality improvement of security specifications by means of actively promoting the use and writing of Protection Profiles (PP);
- § Safeguarding the quality of IT products and systems, by means of their Certification;
- § Stimulating the Certification of IT product and systems, in order to broaden the range of definitively safe products and systems;
- § Stimulating the TOE independent Certification of Sites in order to reduce time and money for evaluations;
- § Promoting the use of certified IT product and systems in order to improve the general level of IT security.

The Certification Body (CB) has an important role to play in the NSCIB. The CB shall be responsible for the Certification of Protection Profiles and Targets of Evaluation (TOE – an IT product or system) and also for the other tasks that are indicated in Section 2.2, *Tasks of the Certification Body*.

The existence of a CB is vital for (international) recognition of evaluation results. The CB is the basis for the assurance that:

- § All ITSEFs shall operate according to the same high standards: impartial, no bias towards test results, repeatability, and reproducibility;
- § The same criteria shall apply the same way so that correct and consistent results are delivered;
- § The confidentiality of proprietary or other sensitive information shall be protected adequately.

2.2. Tasks of the Certification Body

The most important tasks of the CB are:

1. Authorising of the participation in the NSCIB of ITSEFs by means of licensing those ITSEFs;
2. Monitoring those ITSEFs, especially the way the ITSEFs apply and interpret the evaluation criteria;
3. Designing procedures to ensure that sensitive information about the TOEs and PPs under evaluation is handled appropriately and that it is secured;
4. Ensuring that the above mentioned procedures are used;
5. Where necessary, the issuance of additional regulations to ITSEFs;
6. Monitoring all running evaluations in the NSCIB;
7. Reviewing the evaluation reports that are produced during an evaluation to ensure that the conclusions are consistent with the supplied TOE and supporting documentation, and that the authorised evaluation criteria are used correctly;
8. Producing a Certification Report (CR) for every Evaluation completed;
9. Publicising the Common Criteria Certificates and the relevant Certification Reports;
10. Documenting the NSCIB, the organisation, its policy, rules, and procedures;
11. Publicising and keeping up to date of the above mentioned documentation;
12. Ensuring that the rules of the NSCIB are adhered to;
13. Putting into operation and, where necessary, amend the policy and regulations of the NSCIB;
14. Protecting the interest of all parties in the NSCIB.

All of this is managed in an as much as possible efficient and effective way, by avoiding double work. The execution takes place according to the principles⁴ of applicability, impartiality, objectivity, repeatability, reproducibility, and correctness.

2.3. Roles in the Netherlands Scheme

Figure 1-1 shows an overview of the relevant roles in the NSCIB. These can be broken down into the roles directly involved in the process: CB, ITSEF, Sponsor; and the role indirectly involved in the process: Developer.

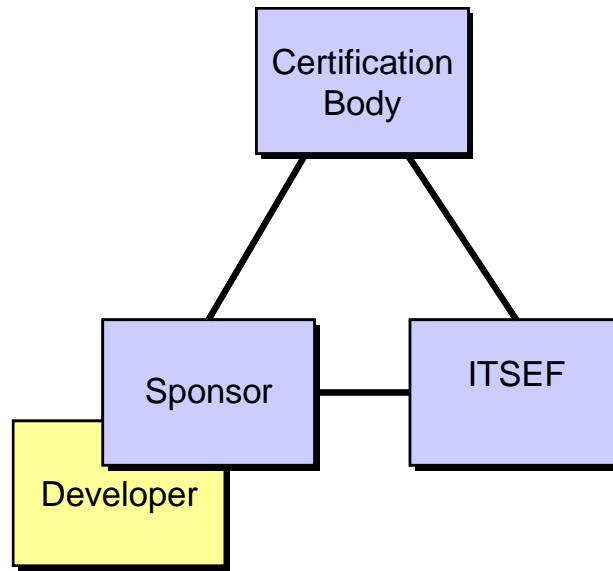


Figure 1-1, Roles in the Netherlands Scheme

2.3.1 Certification Body

The CB is the organisation authorised to issue Common Criteria certificates. In the NSCIB there is one CB operated by TÜV Rheinland Nederland with the support of BZK/NLNCSA. The tasks of the CB are described in Section 2.2, *Tasks of the Certification Body*, in this part of the document.

2.3.2 Evaluation Laboratory (ITSEF)

An ITSEF is an organisation that applies the criteria of the Common Criteria to a TOE of a Sponsor. Only an ITSEF licensed by a CB may perform Evaluations that can lead to a certificate under the NSCIB. The NSCIB allows for several ITSEFs to be licensed.

2.3.3 Sponsor

The Sponsor is the organisation that wants to have the TOE certified and pays for the Certification. A Sponsor communicates with an ITSEF about the concrete Evaluation of the TOE, and with the CB about certification of this evaluation. The Sponsor can be the Developer but this is not mandatory. For that reason the role of the developer has been defined separately. The NSCIB is open to all Sponsors - from The Netherlands as well as from foreign countries. However, restrictions may be placed on sponsors originating from countries not participating in the international recognition agreements defined in section 1.2, *Scheme Status*, in this part of the document.

2.3.4 Developer

The Developer is the organisation that develops the TOE (design, building, testing, etc.). A certain TOE may have several developers. It is possible, but not necessary, that the Sponsor and the Developer are one and the same party.

⁴ See [CEM] Chapter 2 'Universal Principles of Evaluation' for a further definition of these notions.

3. Documentation Overview

3.1. Assessment Criteria of the NSCIB

The assessment criteria of the NSCIB are published on the NSCIB website.

3.2. Basic Documents for Scheme Documentation of the NSCIB

[CCRA]	<i>Arrangement on the Recognition of Common Criteria Certificates in the Area of Information Technology Security, July 2014</i>
[SOGIS-MRA]	<i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, January 2010</i>
[TÜV-KMS]	<i>Kwaliteitsmanagementsysteem (Quality Handbook) TÜV Rheinland Nederland B.V.</i>

3.3. Documentation concerning the licensing of ITSEFs

[ISO17025]	<i>General Competence Requirements for Test and Calibration Laboratories (ISO/IEC 17025)</i>
------------	--

4. Terminology

The terminology used in this chapter is in accordance with the terminology of the Common Criteria.

Advisory Board	The independent body set up by TÜV Rheinland Nederland to assess and control the accredited certification system.
Assessment Guidelines	<p>The list of requirements, other than (harmonised) product standards, that the product or system must meet, established by the Advisory Board after proper consultation with all interested parties and that, following acceptance by TÜV Rheinland Nederland, serves as the criterion for the issuance of Certificates.</p> <p>In the NSCIB the Assessment Guidelines is the collection of requirements to be met by the PP or the TOE as defined by the Common Criteria [CC] and the relevant Methodology [CEM].</p>
Board of Appeal	An independent Board established by the Advisory Board to deliver binding judgments to the management of TÜV Rheinland Nederland regarding appeals made by third parties against the performance in certification cases of TÜV Rheinland Nederland.
Certificate	<p>A document issued by TÜV Rheinland Nederland in accordance with the rules of a certifying system to express legitimate confidence that a clearly described object of certification is in agreement with a given standard or Assessment Guidelines.</p> <p>In the NSCIB this means that by means of the Certificate, the CB shows that there is legitimate confidence that the TOE is in accordance with its Security Target (ST).</p>
Certificate Holder	<p>The organisation that has been granted a Certificate by TÜV Rheinland Nederland on the basis of the Certification Agreement and the results of the Product Certification.</p> <p>In the NSCIB the Certificate Holder is denoted as Sponsor.</p>
Certification Agreement	An agreement defining the mutual rights and obligations of an certificate applicant or a Certificate Holder and of TÜV Rheinland Nederland.
Certification Body	An organisation authorised to issue Common Criteria Certificates. In the NSCIB this is TÜV Rheinland Nederland supported by BZK/NLNCSA.
Certification ID	The reference code to a certification process.
Certification Mark	<p>A mark held by TÜV Rheinland Nederland that may be used by the Certificate Holder under the conditions of the Certification Agreement.</p> <p>In the NSCIB, the Certification Mark shall consist of the logo of TÜV Rheinland Nederland, and the right to use the Common Criteria Mark and/or SOGIS Mark. The conditions for use of the Common Criteria and SOGIS Mark are defined in [CCRA] and [SOGIS-MRA] respectively.</p>

Certification Report	A public domain report issued by the CB. This document summarises the results of an Evaluation. The report indicates that the Evaluation was performed correctly by the ITSEF and that Assessment Guidelines and the relevant Evaluation Methodology and other procedures have been applied, and, that the conclusion of the Evaluation Technical Report agrees with the investigated Developer Evidence.
Certification System	<p>The rules and procedures for the control and implementation of the certification, further elaborated for products, processes, or systems indicated.</p> <p>This document refers for this purpose to the Netherlands Scheme for Certification in the Area of IT Security (NSCIB).</p>
Developer	The organisation that develops the TOE (design, building, testing, etc.). The Developer may be the same organisation as the Sponsor but it may also be a different organisation.
Developer Evidence	The collection of documents and equipment or software necessary to test a criterion.
Evaluation Supervisor	The person that shall represent the CB during an evaluation.
Evaluation Technical Report	Final report about the application of all parts of the Assessment Guidelines to all Developer Evidence.
Work Plan	Planning document for the evaluation. This document comprises a schedule, the Developer and Evaluation evidence to be submitted, and other arrangements.
Intermediate Report	Interim report about the application of a part of the Assessment Guidelines to the relevant part of the Developer Evidence.
ITSEF	Information Technology Security Evaluation Facility. An organisation that applies the Assessment Guidelines to a PP or a TOE of a Sponsor. The ITSEF shall be licensed by the CB.
Management System	The organisational structure, responsibilities, procedures, processes, and facilities for quality assurance.
Organisation	<p>The body that has the responsibility for a product mentioned in the Assessment Guidelines.</p> <p>In the NSCIB, Organisation is denoted as Developer.</p>
Product Assessor	<p>Staff member, or subcontractor of TÜV Rheinland Nederland who tests the results of the investigation against a given standard or the Assessment Guidelines and then advises the certification manager of TÜV Rheinland Nederland for certification.</p> <p>In the NSCIB, the Product Assessor is referred to as the Evaluation Supervisor and is a party appointed by the CB for giving technical support in the area of the Common Criteria and IT security, and, for supervising the evaluations of ITSEFs. In practice this party is, or operates under the supervision of the Ministry of the Interior and Kingdom Relations (BZK).</p>

Product Certification	<p>The process that is the basis on which TÜV Rheinland Nederland states legitimate confidence that a clearly specified object for certification complies with a specific standard or Assessment Guidelines.</p> <p>In the NSCIB, the Product Certification refers to the process conducted by an ITSEF within the framework of the regulations of the Common Criteria, controlled by the CB.</p>
Product Standard	<p>Requirements to be satisfied by the product as specified in (harmonised) standards, formulated and accepted by officially recognised authorities.</p> <p>In the NSCIB, the Product Standard refers to the Common Criteria.</p>
Protection Profile	<p>An implementation independent collection of information security requirements for a type of TOE that corresponds to specific user needs.</p>
Quality	<p>Technical and functional requirements related to effectiveness, durability, and practical value of a product or a product group.</p>
Review Report	<p>Report by the CB, i.e. the Evaluation Supervisor, in which a judgement is given about the reports delivered by the ITSEF.</p>
Security Target	<p>A collection of information security requirements and specifications on which the evaluation of an identified TOE is based.</p>
Site	<p>A part of the development environment of one or more TOEs.</p>
Sponsor	<p>The party that initiates the Certification Process for the Evaluation of a PP or a TOE. The Sponsor communicates with the licensed ITSEF about the concrete Evaluation and with the CB about the Certificate and certification process.</p>
Target of Evaluation	<p>An IT product or system together with the relevant support and user documentation that is going to be evaluated.</p>
TÜV Rheinland Nederland	<p>The independent legal body established by TÜV engaged in certification.</p>
TÜV	<p>Technische Überwachungs Verein</p>

Table 1-1: Cross reference between different notions in Common Criteria and TÜV Rheinland Nederland

Notions Common Criteria	Notions TÜV Rheinland Nederland
Certification Body	<i>TÜV Rheinland Nederland</i>
Certification Report	-
Common Criteria	<i>Assessment Guidelines</i> <i>Certification Mark</i> <i>Quality</i> <i>Product standard</i>
Developer Evidence	-
Evaluation Evidence	-
Evaluation Technical Report	-
Work Plan	-
Intermediate Report	-
ITSEF	-
NSCIB	<i>Certification Scheme</i>
Developer	<i>Organisation</i>
Protection Profile	<i>Product</i>
Review Report	-
Security Target	-
Sponsor	<i>Certification applicant</i> <i>Certificate Holder (when certificate issued)</i>
Target of Evaluation	<i>Product or System</i>
Evaluation Supervisor	<i>Product Assessor</i>

5. Glossary

BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministry of the Interior and Kingdom Relations
CB	Certification Body
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CR	Certification Report
ETR	Evaluation Technical Report
WP	Work Plan
IR	Intermediate Report / Intermediate Evaluation evidence
ITSEF	Information Technology Security Evaluation Facility
NLNCSA	Netherlands National Communication Security Agency
NSCIB	Netherlands Scheme for Certification in the Area of IT Security
NSI	Netherlands Scheme Instruction
NSP	Netherlands Scheme Procedure
PP	Protection Profile
RvA	Raad voor Accreditatie, Dutch Accreditation Counsel
ST	Security Target
TÜV	Technische Überwachungs Verein
TOE	Target of Evaluation

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

Part 2 – Regulations Concerning a Certification



1. Introduction

This part of the Scheme Documentation defines the conditions that apply to Certification Agreements that TÜV Rheinland Nederland enters into for the assessment of TOEs and PPs and the subsequent issuance of Certificates.

The CB will provide information, to any interested party, about this Certification Scheme, the TÜV Rheinland Nederland Advisory Board Regulations and the members of the Advisory Board.

TÜV Rheinland Nederland shall in principle be prepared to grant to Sponsors whose TOE or PP have been evaluated successfully according to the Common Criteria (CC), the right to use a TÜV Rheinland Nederland Certificate and the use of the Certification Mark. This Certification Mark shall consist of the logo of TÜV Rheinland Nederland, and the right to use the Common Criteria Mark and/or SOGIS Mark. The conditions regarding this right are defined by this Schema Documentation (Part 2), in the particular certificate, and in everything else that is explicitly agreed in writing between parties.

2. Certification Process

This chapter gives an overview of the possible procedures that apply for the certification process. Depending on the nature of the evaluation, different procedures could apply as described in the following sections. However in all cases the evaluation shall be performed by an ITSEF that is licensed by the CB to operate under this scheme (see also part 3 - Licensing of an ITSEF).

2.1. First Evaluation of a TOE/PP

This chapter gives an overview of the steps normally⁵ taken in a certification process, in which a TOE/PP is evaluated for the first⁶ time.

The certification process comprises three phases:

- The *preparation phase*: in which the formal Application shall be submitted and processed, resulting in a Certification Agreement;
- The *monitoring phase*: in which the actual evaluation is performed under supervision of the Certification Body (CB), resulting in an Evaluation Technical Report (ETR);
- The *certification phase*: in which the concluding actions are performed, resulting in a Certificate.

In each of these phases, the actors discussed in Part 1 are active.

2.1.1 Preparation Phase

The preparation phase is the first phase in the certification process. This phase starts with the Application of the Sponsor to the CB and ends with entering into a formal Certification Agreement.

Start of the preparation phase: the Application

This phase starts⁷ when the Sponsor applies for a Certification at the CB. An Application consists of a completed and signed Application form (see Part 5) accompanied by (a draft of) the Security Target (ST) in case of a TOE evaluation, or, (a draft of) the Protection Profile in case of a PP evaluation.

The Sponsor may optionally submit the Application together with an ITSEF. If requested, the CB provides the Sponsor with an overview of all ITSEFs licensed under the NSCIB. It is the responsibility of the Sponsor to enter into an agreement with a licensed ITSEF.

In the NSCIB there is regulated interaction between CB, Sponsor, and ITSEF. This implies that the rules below in this Scheme Documentation (Part 2) shall be extended by tripartite agreements between CB, Sponsor, and ITSEF.

⁵ An Abridged Procedure for the certification of TOEs is described in Section 2.2.

⁶ A re-evaluation of earlier evaluated TOEs/PPs is handled differently as described in Section 2.3.

⁷ Possibly there has already been contact between the Sponsor and the ITSEF, however, this is beyond the scope of the Certification Process.

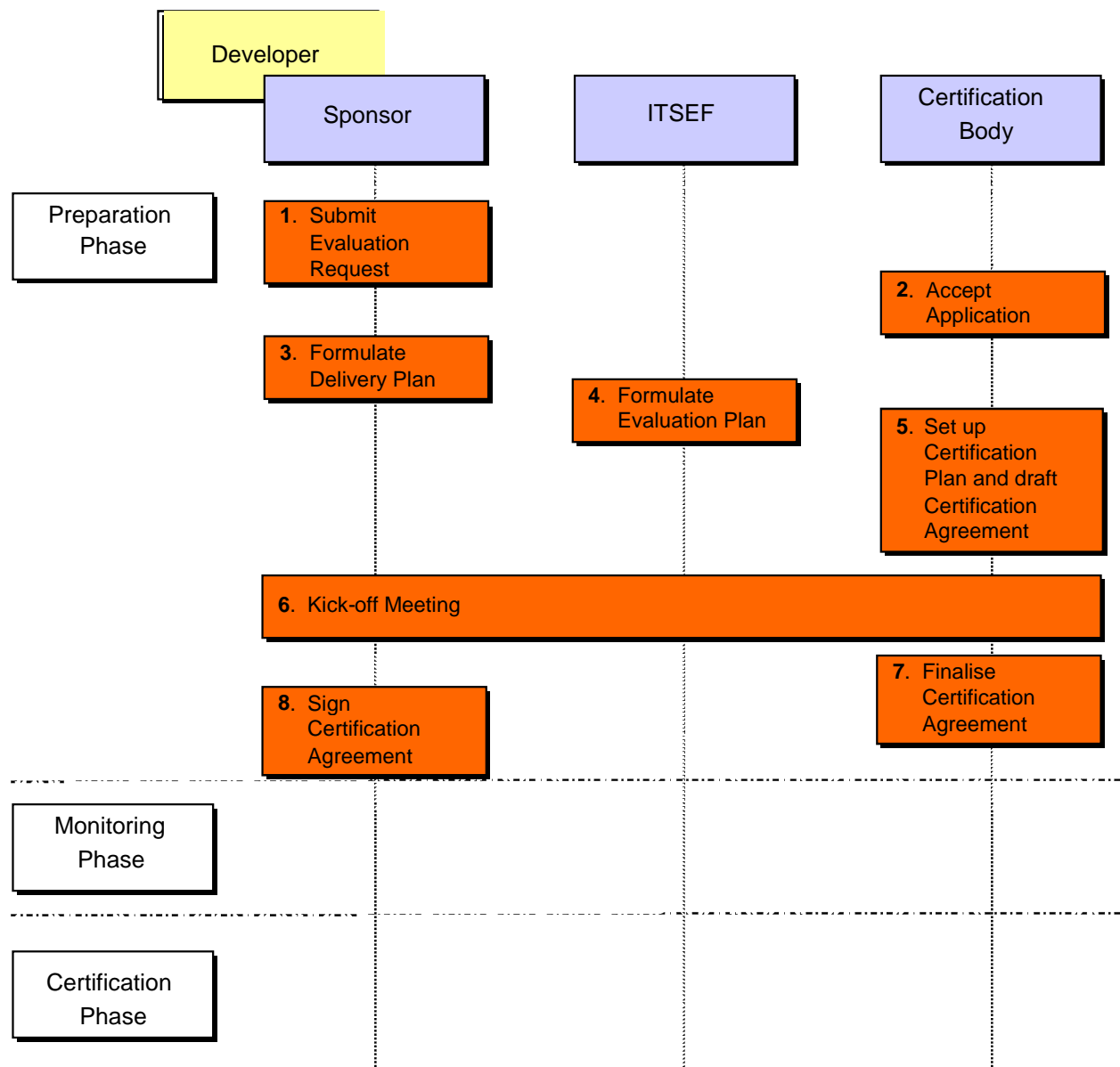


Figure 2-1, Activities and actors in the preparation phase.

Assessment of the Application

The CB assesses the Application on the following items:

- *Clarity:* is the ST or PP clear and understandable, is the TOE scope well defined?
- *Meaningfulness:* comprises the ST or PP sufficient functionality to come to a meaningful certificate and is the 'assurance' sufficient to warrant this functionality?
- *Competence ITSEF:* is the ITSEF that is going to perform the evaluation sufficiently competent to evaluate this specific TOE?
- *License:* is the ITSEF licensed under NSCIB?

When the CB approves the Application, the CB shall confirm this to the Sponsor in writing together with a quotation for performing the Certification assessment, the incurred costs, and any expenses of

auditing, produced as a draft contract proposal.⁸ Also the Sponsor will be informed about a Certification-ID⁹ and the name of the assigned Evaluation Supervisor¹⁰.

If the CB finds the information provided inadequate, it may inform the Sponsor that extra information is required.

Should the CB reject an Application then it shall send a notification in writing, including their motivation for this to the Sponsor. The options for making an appeal against this rejection are described in Section 4.12, *Appeal*. When an Application has been rejected, the CB shall not consider a renewed Application of the same Sponsor for a revised TOE/PP, unless the Sponsor can plausibly argue that the issues that led to the rejection of the earlier Application, have been dealt with.

Should the CB have any doubt concerning one of the assessment items it shall consult the Advisory Board before rejecting or accepting.

Kick-off Meeting

In case of an Application concerning a TOE evaluation, the CB shall organise a Kick-off Meeting with CB, Sponsor, and ITSEF. No Kick-off meeting is required in case of a PP evaluation or if deemed unnecessary by all parties.

The following items shall be discussed in this kick-off meeting:

- *Information to the Sponsor*, to ensure that he is informed about the Evaluation Process, the roles and the responsibilities;
- *The draft Certification Agreement*, in which the above mentioned shall be defined by contract;
- *The basis of the evaluation*, which version of the Common Criteria shall be used and which Scheme Instructions;
- *Measures to ensure confidentiality*, between all parties;
- *Possible restrictions concerning cryptography, TEMPEST (TEMPorary Emission and Spurious Transmission), etc.* The assessment of these matters is beyond the scope of the Common Criteria. When necessary, specific tests can be agreed upon that can subsequently be included in the (CC) evaluation;
- *Possible technical peculiarities of the TOE/PP*;
- *Sites to be visited*. The rules that are applied to decide which developer site(s) involved in the construction of the TOE have to be audited. Also see NSI_07 Site audits.
- *How the Sponsor shall gather the necessary Developer evidence*¹¹, if the Sponsor is not the Developer of the TOE, or if the TOE is built up of products of a number of developers;
- *The provisional Work Plan of the certification*.
The Work Plan of the Certification is written by the ITSEF and defines the schedule for the Certification Process. The work plan must address the following four points:
 1. *Delivery Plan*: this is the schedule for the submission by the Sponsor to the ITSEF of all Developer evidence required for the Evaluation. Keeping this up to date is the responsibility of the Sponsor;
 2. *Evaluation Plan*: this is the schedule for the delivery of all Intermediate Reports or Intermediate Evaluation evidence (IR – see further on) and the ETR (see further on). Keeping this up to date is the responsibility of the ITSEF;

⁸ The Certification assessment may involve the engagement of an commercial technical expert. A specification of these additional costs is included in the contract proposal.

⁹ The reference code for the Certification Process of this TOE/PP.

¹⁰ The contact from the CB during the Certification Process.

¹¹ This is not applicable for low levels of assurance: e.g. for EAL1 no help from the developer is required.

3. *Staff involved in Consultancy and Evaluation:* in this section, the ITSEF must identify and describe any consultancy services that have been provided to the sponsor and list the employee(s) involved. This is of particular importance when the consultancy has involved writing documentation on behalf of the sponsor. Employees involved in consultancy may not perform evaluation activities or mentor other employees during the evaluation. The ITSEF must also identify the names and roles of employees involved in evaluation
4. *Certification Plan:* this is the schedule for reviewing of all IRs and the ETR, as well as the delivery of the Certification Report (CR – see further on), and the Certificate (see further on). Keeping this up to date is the responsibility of the CB. In principle, a time period of two weeks shall be used for review activities. Additionally, the CB has the option of indicating special supervision in the Certification Plan.

The template for a Work Plan is included in Part 5.

Certification Agreement

Before the Kick-off meeting the CB shall produce a draft Certification Agreement and send this to the Sponsor. This draft Certification Agreement is a quotation for performing the Certification and serves as the basis for the discussion.

Following the meeting the CB will finalise the Certification Agreement. The CB reserves the right not to issue a Certification Agreement, in which case the CB shall send to the Sponsor a notification, in writing, including their motivation for this. The options for making an appeal have been described in Section 4.12, *Appeal*.

The agreed Work Plan forms part of the Certification Agreement. After receipt of an unchanged Certification Agreement signed by the Sponsor, the CB updates the list of product under Certification (see Section 4.9.2, *During the certification Process*). Then the Preparation Phase has ended and the Monitoring Phase may start.

The CB reserves the right to decline a Certification Agreement received more than thirty (30) days after the Kick-off Meeting was held (or in absence of such a meeting: after the draft Certification Agreement was submitted to the Sponsor).

2.1.2 Monitoring Phase

During the Monitoring Phase the Work Plan is executed by the CB, Sponsor, and ITSEF.

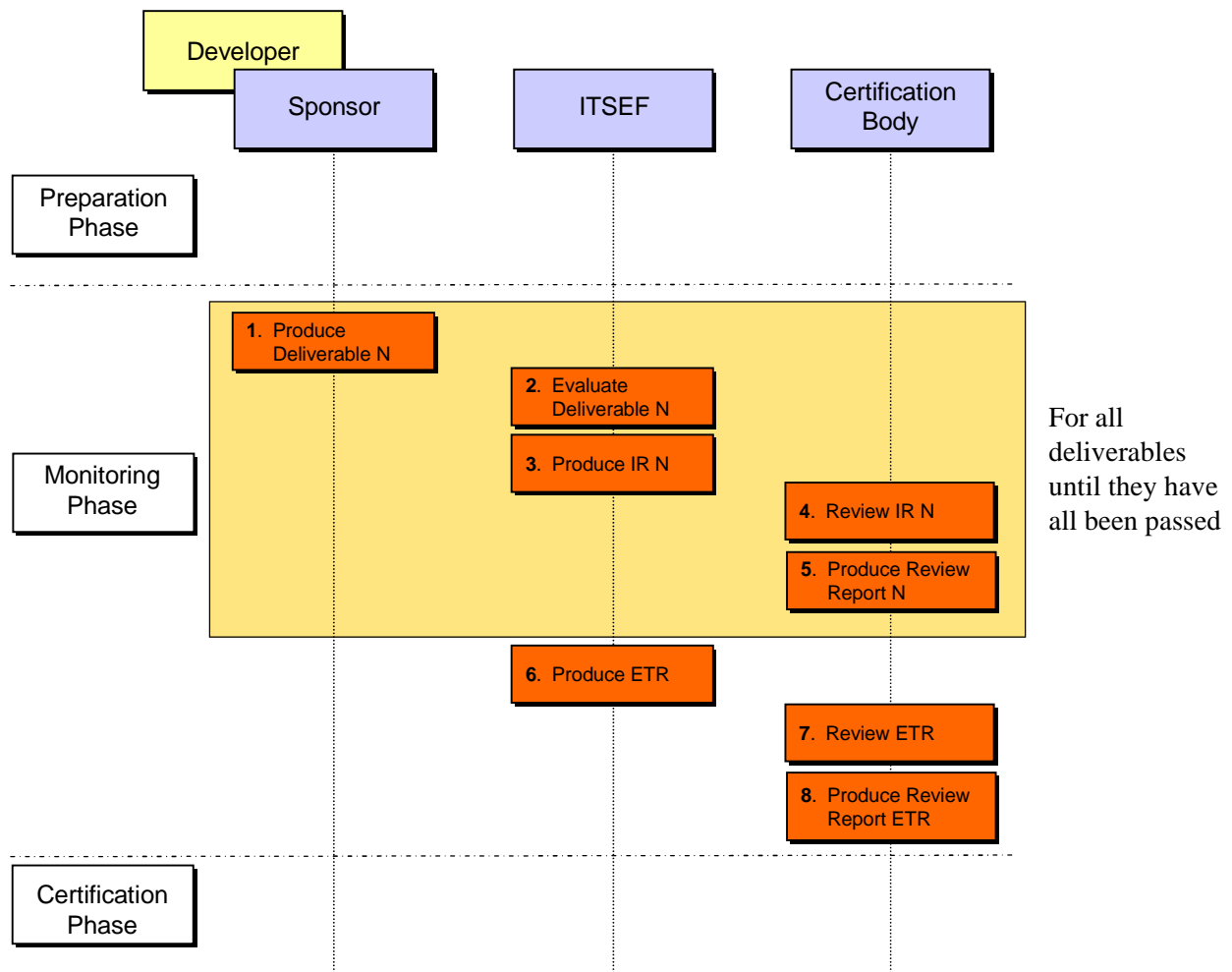


Figure 2-2, Activities and Actors in the Monitoring Phase

Developer evidence

During the Monitoring Phase, the Sponsor delivers a number of items to the ITSEF. This comprises documents (a PP, or an ST, design documents, test documents, quality plans etc.) as well as equipment or software (the TOE, test environment) etc. The ITSEF may also carry out a 'site visit' to the Developer, which may also be regarded as Developer evidence. The collection of documents etc. that is required for testing a criterion is denoted as Developer evidence.

The exact Developer evidence that shall be submitted is:

- In case of a PP Evaluation: the Protection Profile;
- In case of a TOE Evaluation: the ST, and all Developer evidence that results from the Assurance Criteria in the ST.

All Developer evidence shall be submitted according to the Delivery Plan. In case this Plan is not adhered to, the Sponsor has to produce a new Delivery Plan that shall be basis for adjusting the Evaluation Plan of the ITSEF and the certification Plan of the CB (also see Section 3.1, *Premature Termination of the Certification Process*).

Developer evidence shall be submitted to the ITSEF by the Sponsor. In general, the Developer evidence is not submitted to the CB, but the CB will make regular spot checks on the Developer evidence. In such cases, the CB reserves the right to request certain Developer evidence and both the ITSEF and the Sponsor shall have to cooperate to make it available.

Intermediate Report / Intermediate Evaluation evidence

Every part of the Developer evidence shall be evaluated by the ITSEF according to the appropriate criteria as described in Section 5, *Assessment Guidelines Common Criteria*. The ITSEF applies these criteria and delivers an Intermediate Report or Intermediate Evaluation evidence (IR) to the CB, based on its findings.

An Intermediate Report for a selected part of the Developer evidence comprises of a list of all relevant criteria; and for each criterion it shall indicate:

- A motivated judgement why the Developer evidence does or does not conform to the criterion;
- A reference to and an adequate summary of the underlying parts of the Developer evidence which led to this judgement;
- Date and name of the Evaluator.

The template for an IR is included in Part 5.

All IRs shall be delivered according to the Evaluation Plan. If this Plan is not adhered to, the ITSEF shall produce a new Evaluation Plan that shall be the basis for adjusting the Delivery Plan of the Sponsor and the Certification Plan of the CB (see also Section 3.1, *Premature Termination of the Certification Process*).

If during the Evaluation any problems arise regarding the interpretation of the criteria, then the procedures in Section 5.2, *Unclarity in the Assessment Guidelines Common Criteria* apply.

Review report

The ITSEF shall send the IRs to the CB. The CB shall review every IR and produce a review report based on its findings.

A Review Report of an IR states the opinion of the CB about the IR: has the ITSEF done a good job according to the CB – in case of a negative Review a motivation is required. Feedback in the review report is structured so as to indicate the severity of the comment. The presence of major comments will always lead to rejection of the IR by the CB. The presence of minor comments may lead to rejection at the discretion of the CB based upon their nature and number.

The Review Report may also request actions, according to Table 2-1.

The template for a Review Report is included in Part 5.

Table 2-1: Actions following the Review of an Intermediate Report

	ITSEF thinks the Developer evidence conforms to the Criteria	ITSEF thinks the Developer evidence does not conform to the Criteria
CB thinks ITSEF has done well in the Evaluation of the Developer evidence	The CB accepts the IR	The CB does not accept the IR. Sponsor has to deliver a new version of the Developer evidence.
CB doubts whether ITSEF has done well in the Evaluation of the Developer evidence	The CB does not accept the IR. The CB may ask ITSEF to perform additional evaluation work, or to repeat evaluation work. The CB may also request Developer evidence for auditing. The ITSEF has to deliver a new version of the IR, and possibly, the Sponsor has to deliver new Developer evidence.	

Regardless of any acceptance or rejection, the CB shall make the Review Report available to the ITSEF and the Sponsor if the Sponsor so desires. The ITSEF subsequently performs the actions demanded in the Review Report.

- When an ITSEF delivers a new version of an IR, this shall again be sent to the CB who produces a new Review Report.

- When the Sponsor delivers new versions of the Developer evidence¹², these have to be evaluated by the ITSEF anew; the ITSEF sends the new IR to the CB who produces a new Review Report. If Developer evidence depends on new part of the Developer evidence¹³, this Developer evidence also has to be re-evaluated i.e. the ITSEF has to produce new IRs which in turn could result in new Review Reports.

This cycle of Developer evidence, IRs, and Review Reports shall be pursued until all required IRs have been accepted by the CB.

It should be noted that changes in the Developer evidence en/or IRs may also bring about changes in the Delivery Plan and the Evaluation Plan, which in turn may change the Certification Plan (see also Section 3.1, *Premature Termination of the Certification Process*).

Evaluation Technical Report

When all required IRs have been accepted by the CB, the ITSEF produces an ETR.

An Evaluation Technical Report of an Evaluation shall comprise:

- All parts as indicated in the CEM Chapter 2, General Evaluation Tasks;
- The final versions of the IRs.

The template for an ETR is included in Part 5.

The ITSEF sends this ETR to the CB. The CB produces a Review Report analogously to a Review report for an IR, using identical procedures. The Monitoring Phase ends when the CB accepts the ETR, at which point the Certification Phase starts.

2.1.3 Certification Phase

In this phase the CB shall produce a CR and a certificate based on the ETR.

¹² This may happen because the Review Report requests so, but also for other reasons such as small modifications to the TOE.

¹³ See the dependency matrix in Annex A of [CC] Part 3.

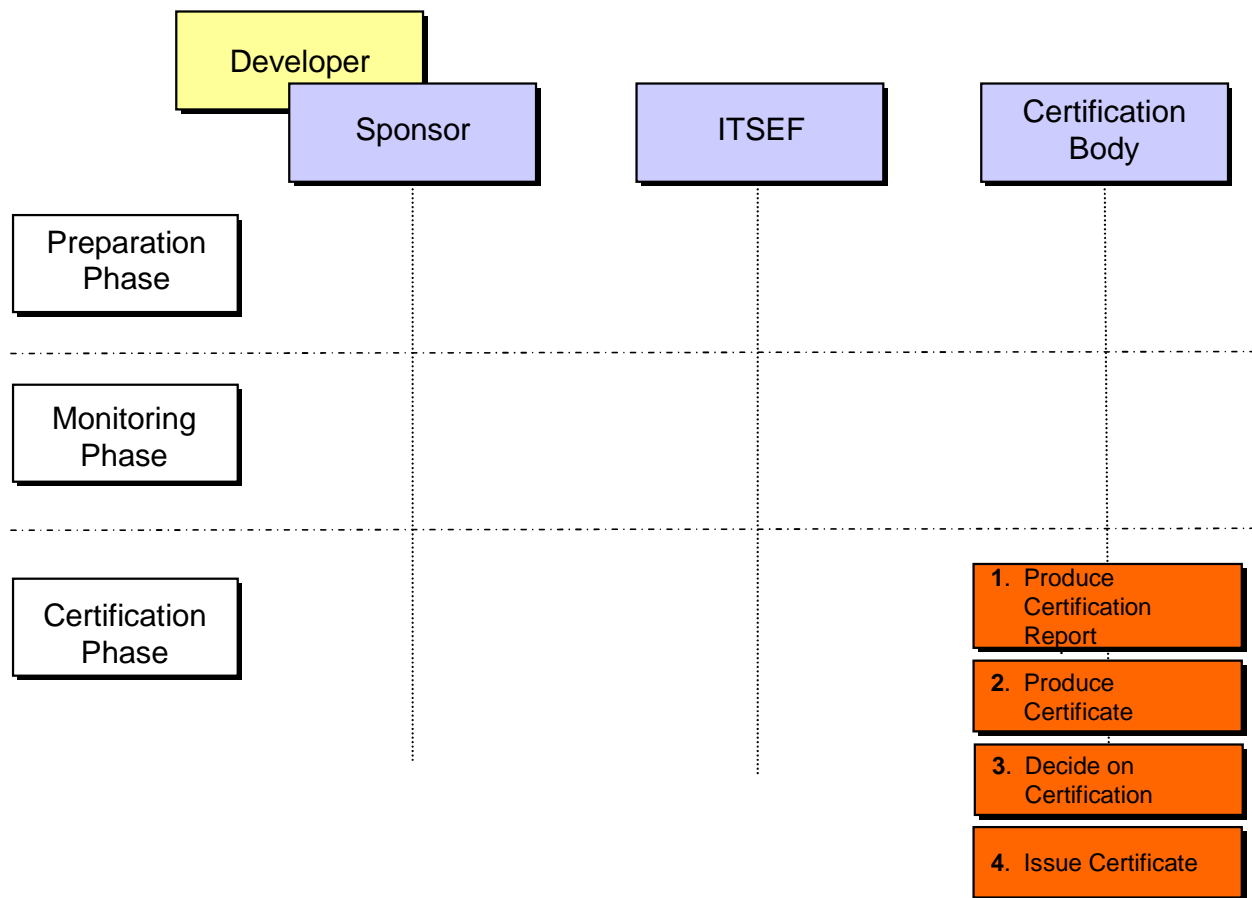


Figure 2-3 Activities and Actors in the Certification Phase

Remarks:

- The Certification Report shall be produced by the Supervisor of Evaluations.
- A draft of the Certification Report shall be submitted to the ITSEF and sponsor in order to support the verification that no proprietary information is present in the Certification Report.
- The certification manager of the CB shall take the responsibility for issuing the Certificate.

For further information see Part 4 - Roles in the Certification Body, Section 2.5, *Certificate Issuer*.

A CR of a Certification consists of a summary of the ETR, containing all relevant information about the certificate for potential users of the certified TOE/PP. Its contents shall contain all information demanded by the international recognition agreements.

The template for a CR is included in Part 5.

A Certificate is the formal declaration of the CB that the TOE/PP meets the assessment guidelines. It shall contain all information demanded by the international recognition agreements.

The template for a Certificate is included in Part 5.

The CB shall file all relevant information according to the procedure in Section 3.2, *Configuration Management of Documents*, and update the List of Certified Products (see Section 4.9.3, *Following granting a Certificate to the Sponsor*).

The Certification Phase is ended by the issuance of the Certificate and the CR to the Sponsor.

2.2. Alternative Reporting Procedure

Sponsor and ITSEF may in the Preparation Phase indicate collectively that they want to use the Alternative Reporting Procedure.

The advantage of the Alternative Reporting Procedure is that it is more efficient by supporting the evaluator to extract information from developer documentation and interviews with the developer rather than having the developer/consultant rewrite the documentation into specific CC documentation. It furthermore streamlines the reporting activities from ITSEF to CB by reporting in a different style.

The scheme procedure “Alternative Evaluator Reporting” describes this procedure in detail.

2.3. Assurance Continuity procedure

Making any alterations to the TOE (inclusive of documentation) and thereby causing a change in the TOE identification (i.e. version number) shall cause the Certificate to be no longer applicable for that modified TOE. In accordance with the CCRA supporting document “Assurance Continuity” the sponsor can apply for either a re-certification or for assurance maintenance, depending on the nature of the changes.

At the moment the following procedure applies:

- The Sponsor submits an application form to the CB with his request for re-certification or for assurance maintenance;
- The application form shall refer to an Impact Analysis Report (IAR) as defined in the CCRA supporting document “Assurance Continuity: CCRA Guidelines”;
- The CB assesses the IAR in consultation with the original ITSEF and decides on the procedure to be followed: re-certification or assurance maintenance.

Remarks:

- In case of assurance maintenance the related procedure as defined in the CCRA supporting document “Assurance Continuity” applies.
- In case of re-certification the standard procedure defined in section 2.1, First Evaluation of a TOE/PP is applied in an abbreviated form. In this case a number intermediate stages in the Monitoring Phase are skipped which might speed up the process. Also, depending on the nature of the alterations, it is possible that items from the earlier certification (of the ‘same’ TOE) are re-used. The details of the certification procedure and the options for re-use shall be discussed at the Kick-off Meeting of the new Evaluation.

3. Regulation for the Certification Process

3.1. *Premature Termination of the Certification Process*

The Certification process can be terminated prematurely by each of the three parties: CB, Sponsor, and ITSEF.

3.1.1 By the Certification Body

If:

- The Sponsor seriously or repeatedly fails to meet the Delivery Plan, or
- The Sponsor fails to pay the invoices or advance invoices in time (see Section 3.5, *Cost of Certification*),
- The ITSEF seriously or repeatedly fails to meet the Evaluation Plan, or
- The quality of the Intermediate Reports is insufficient, or if the Intermediate Reports have to be corrected too often.

If in the opinion of the CB the likelihood of a positive Certification result is at risk, the CB may decide:

- To contact the Sponsor and/or to make inquiries;
- To warn the Sponsor and/or ITSEF that if this situation persists the Certification Process shall be terminated;
- To terminate the Certification Process. In this case the CB shall inform the Sponsor and the ITSEF about the termination, in writing, including their motivation for this.

If the CB terminates the Certification Process, the CB shall not accept a new Application for a renewed TOE, unless the Sponsor demonstrates that sufficient measures have been taken to improve the issues that were reason for termination.

3.1.2 By the Sponsor

The Sponsor may terminate the Certification Process at all times by informing the ITSEF and the CB in writing without prejudice to its obligation to pay the expenses already incurred by the CB.

3.1.3 By the ITSEF

The ITSEF may, at all times, terminate the Certification Process by informing the Sponsor and the CB in writing. It is expected that this situation is covered by the contract between Sponsor and ITSEF but this is beyond the responsibility of the CB. Should the Sponsor desire to start a new Certification with a new ITSEF then the Sponsor shall have to submit a new Application. Re-use of results obtained at that time shall be agreed in the Work Plan as part of the new Certification Agreement.

3.2. *Configuration Management of Documents*

3.2.1 Which documents shall be managed?

An overview of documentation generated during a Certification Process is shown in Table 2-2:

Table 2-2: Overview of Documentation in a Certification Process

Document	Possible Media	Distribution
Certification Application	Paper Electronically	Sponsor to CB
Certification Agreement	Paper Electronically (drafts)	CB to Sponsor

Work Plan (Delivery Plan, Evaluation Plan, and Certification Plan)	Electronically	CB/ITSEF/Sponsor
Developer evidence (including Security Target or Protection Profile)	Electronically Paper (optionally)	Sponsor to ITSEF ITSEF to CB (if requested)
Intermediate Report / Intermediate Evaluator evidence	Electronically	ITSEF to CB ITSEF to Sponsor (dependent on the Work Plan)
Evaluation Technical Report	Electronically	ITSEF to CB ITSEF to Sponsor
Review Report	Electronically	CB to ITSEF CB to Sponsor (dependent on the Work Plan)
Certification Report	Electronically	CB to ITSEF CB to Sponsor CB to Certified Product List (dependent on the Work Plan)
Certificate	Paper	CB to Sponsor
Certified Product List	Electronically	Website
List of development sites covered by the Certificate	Electronically	CB to certificate user (on request)

3.2.2 Documentation rules

- All documents shall be written either in English or in Dutch. Deviations of this are only possible with consent of the CB.
- The CB, Sponsor, and ITSEF shall mutually agree on the file formats and graphical formats (on paper as well as electronically, inclusive e-mail).
- All documents shall be labelled with an unambiguous document number, a version number, a date, and the Certification-ID assigned by the CB to the Sponsor (see Section 2.1.1, *Preparation Phase*). All confidential information shall be labelled as such¹⁴. It is not required to use this labelling on every page.
- Changes in the document shall result in a new version number and a new date.
- All documents shall be filed for the time of the validity of the Certificate. After expiration, all documents shall be archived for a period of 5 years. All documents shall be stored by the CB except the Developer evidence which is stored by the ITSEF.

¹⁴ This leaves other obligations e.g. concerning classified material unchanged.

3.3. Special Supervision

The CB may besides reading the IRs, at its own discretion, conduct additional supervision of the Evaluation. This can be realised by having a member of the CB sitting in at the evaluation activities. Activities that are particular suitable for this are:

- Site Visits;
- (Penetration) tests by the ITSEF.

It is the responsibility of the CB to:

- decide to conduct 'special supervision';
- gather, if required, input to be able to take this decision (site visit plans, (penetration)-test plans etc.);
- inform the Sponsor and the ITSEF well in advance, and
- include the decision in the Certification Plan.

3.4. Security (Confidentiality and Integrity)

The CB shall ensure, by any and all means available to it, that all staff and all other external experts involved in certification, shall agree to confidentiality towards third parties about all information which may come to their knowledge in the course of implementing the Certification Agreement.

The ITSEF shall arrange its own pledge of confidentiality with the Sponsor and/or the Developer. The ITSEF shall submit this pledge to TÜV Rheinland Nederland when so required.

The following conditions apply:

- The Sponsor shall not be permitted, under any name or title whatsoever, to induce or attempt to induce CB or ITSEF staff and other staff employed by TÜV Rheinland Nederland who, in the course of their duties, may have become acquainted with information as a result of implementing the Certification Agreement, to act as consultants, nor shall it appoint such staff as its consultants within two years after termination of their employment.
- The security of the ICT-infrastructure of the CB and the ITSEF shall be in accordance with the value of the information that has to be secured.
- The CB, the Sponsor and the ITSEF shall take measures to ensure verifiable confidentiality and integrity of the information exchanged. This shall apply to the Developer evidence (inclusive Security Target), Intermediate Reports, Evaluation Technical Reports, and Review Reports, which are exchanged between:
 - ITSEF and the Evaluation Supervisor: Secure e-mail shall be used. This shall be laid down in the License Agreement with the ITSEF.
 - Evaluation Supervisor and TÜV Rheinland Nederland: By the end of the Evaluation, the Evaluation Supervisor shall submit to the CB all relevant documents, on CD-R and/or paper.

The scheme instruction "Exchange and Handling of proprietary information" defines how the confidentiality and integrity of the information is achieved.

- The other regulations are at least covered by ISO/IEC 17025.

3.5. Cost of Certification

TÜV Rheinland Nederland shall charge the Sponsor the cost of the certification investigation based on the quotation submitted while deducting the originally invoiced advance. The final invoices shall be paid within thirty (30) days after receipt.

If the Applicant fails to settle the (advance) invoice in time, TÜV Rheinland Nederland may suspend or cancel the Certification Agreement. A Certificate shall only be issued after all outstanding invoices have been paid in full.

Unless stated otherwise, all amounts stated in TÜV Rheinland Nederland's tender are exclusive of Value Added Tax (VAT).

The validity of a Certificate is 5 years.¹⁵ Remarks:

- The Certificate shall expire when the TOE is altered in which case a new Certificate has to be applied for.
- In case of withdrawal or not granting a Certificate, no credit invoice shall be sent out.
- The Certification Application shall not be processed unless the Sponsor has paid the invoice.

3.6. Regulations concerning Sub-contractors

The regulations of the [CCRA] concerning sub-contractors are as follows:

Where Participants propose to involve contractors in the implementation and operation of this Arrangement, particularly the procedures set out in Annex D or in Annex G.3 or G.4 or Annex H of this Arrangement [CCRA], they should ensure that these contractors have appropriate expertise and should notify the other Participants. Protected information should be passed to contractors only with the agreement of the originator, as laid down in Annex F.4.

The above regulations concerning sub-contractors is comparable to the related regulations of the [SOGIS-MRA]:

Where Participants propose to involve contractors in the implementation and operation of this Agreement, they shall ensure that these contractors have appropriate expertise. Contractors shall not be responsible to carry out the procedures set out in Annex D, in Annex G or in Annex H of this Agreement. Protected information shall be passed to contractors only with the agreement of the originator, as laid down in Annex F.4.

¹⁵ The validity of a Site Certificate is 2 years.

4. Regulation Concerning Certificates

4.1. Certificate

Granting Certificates shall be based on the positive outcome of the certification investigation. A positive Evaluation result is vital and related to the acceptance of the ETR by the CB.

The continuation of the Certificate may be affected if the Assessment Guidelines or the products are changed or if the production volume is too low or irregular.

On the basis of the assessment reports, the Evaluation Supervisors recommendations and any comments by the Sponsor, TÜV Rheinland Nederland shall decide whether the Sponsor is qualified to receive a Certificate and use the Certification Mark.

If the results of the certification investigation are negative, TÜV Rheinland Nederland shall decline certification while providing written reasons for such decision.

The Certificate shall list the following:

- the Sponsor's name and address
- identification of the certified product or product group¹⁶
- the standard or Assessment Guidelines governing the Certification investigation
- the date of issue
- the period of validity

4.2. Obligations of the Sponsor

The Sponsor shall ensure that all TOEs delivered with reference to the Certificate and/or the Common Criteria Marks, manufactured or produced by the companies specified in the Evaluation Technical Report, conform to the specifications in the Certificate at delivery.

The Sponsor shall provide a copy of the concerned Certificate as well as a copy of the CR and the ST to every purchaser requesting so.

The Certificate only concerns the version of the TOE that was considered during the Certification Process. The certificate does not concern earlier versions of the TOE, parts of the TOE, and systems of which the TOE is part of.

Every alteration to the TOE results in a new version of the TOE not concerned in the Certificate. A Certificate for this new version may only be obtained by re-certification (see Section 2.3, Assurance Continuity procedure).

The Certificate only concerns the version of the Common Criteria and Common Evaluation Methodology Assessment Guidelines that were used during the Certification Process. A Certificate according to a new version of the Common Criteria and/or the relevant Methodology [CEM] can only be obtained by re-certification (see Section 2.3, Assurance Continuity procedure).

4.3. Use of the International Certification Marks

TÜV Rheinland Nederland may grant Sponsors the right to use the Certification Mark.

Any actions against third parties to protect the Certification Mark shall be undertaken by TÜV Rheinland Nederland with the provision that Sponsors entitled to the use of this mark may submit a joint claim with TÜV Rheinland Nederland, or that TÜV Rheinland Nederland may include its interest in any claims against third parties.

Additionally TÜV Rheinland Nederland shall protect the use of the international CCRA and SOGIS marks against unauthorised use by third parties. The conditions for use of the Marks are defined by the [CCRA] and [SOGIS-MRA]. The figure below illustrate these Marks.

¹⁶ or certified Site



Figure 2-4, The CCRA and SOGIS Marks

4.4. Fees

The Sponsor shall pay TÜV Rheinland Nederland a fee for the right to use the Certificate and the Certification Mark as well as the costs of setting up and maintaining the Scheme. Payment of such fee is due on TÜV Rheinland Nederland's invoice, see Section 3.5, *Cost of Certification*.

The amount of the fee shall be determined by TÜV Rheinland Nederland and shall be specified in the Certification Agreement.

4.5. Audit

Audits are parts of the Certification Process. The Scheme complies with the international practice to conduct no additional periodical audit after issuing the Certificate. However, the following exception applies:

- There is a complaint giving ground to serious doubt about the specified characteristics and pre-conditions of the TOE as described in the Certification Report.

In this case the audit shall be carried out by or on behalf of the CB. The Sponsor shall fully cooperate with the audit. It shall provide the CB with the required samples, equipment, and information, free of charge, and it shall grant investigation of the records of complaints about the certified product.

The severity of any deviations revealed by audits shall determine whether or not the CB will impose disciplinary measures.

In case of deviations, as referred to above, the Sponsor shall indicate and specify to the satisfaction of the CB any corrective measures taken and the procedures followed for any deviating goods or products.

4.6. Complaints

It is the responsibility of the Sponsor to inform the CB about relevant vulnerabilities in the TOE that have been found after the date of certification. Additionally, if the TOE has been altered, the procedures for re-certification apply (see Section 2.3, *Assurance Continuity procedure*).

The Sponsor shall record and immediately inform the CB of serious or structural purchasers' complaints about the certified products. The Sponsor shall record any and all complaints and the corrective measures taken with respect to the product for which a Certificate has been granted.

In the event of the Sponsor and the purchaser being unable to reach agreement on a complaint concerning products supplied with the Certification Mark, the CB shall investigate the nature and the details of the shortcoming observed, and report to the complainant and the Sponsor. The cost of this procedure may be charged to the party found to be at fault.

A complaint found to be justified may result in a further discussion between the CB and the Sponsor about changes in the internal quality control system or the quality system and, if necessary, in disciplinary measures.

If the Sponsor is found to have supplied certified products not meeting the relevant specification, the Sponsor shall promptly inform the purchasers, taking these products back if so requested.

The CB shall not participate in any discussions on the financial consequences of products supplied with the TÜV Rheinland Nederland Mark not meeting the quality standards, unless expressly so requested by both the purchaser and the Sponsor, with the CB receiving full reimbursement of expenses.

4.7. Disciplinary Measures

In case of a justified complaint the CB has the right to initiate the following disciplinary actions:

- A warning to the Sponsor in writing and/or
- Withdrawal of the Certificate.

Such an action shall be communicated with the Sponsor.

The Sponsor may submit an appeal to the Board of Appeal against the decisions of the CB within thirty (30) days after receipt of the notice.

4.8. Termination and Suspension of the Certification Agreement

If either party has seriously failed in the performance of one or more obligations of the Certification Agreement and the conditions laid down therein, the other party shall be entitled to terminate with immediate effect the Certification Agreement because of this mere fact. In other cases termination of the Certification Agreement may only take place on the final day of any month, subject to three-month notice.

In case of one party wishing to terminate the Certification Agreement, this party shall notify the opposite party in writing, stating reasons, while mentioning the date on which termination is to be effective, thus cancelling the Certificate.

Cancellation shall leave unimpaired the Sponsor's financial obligations toward TÜV Rheinland Nederland. Also, after termination, TÜV Rheinland Nederland's confidentiality shall remain in force.

In the event of the Sponsor failing to meet its obligations, the CB may decide to suspend the Sponsor's right to use TÜV Rheinland Nederland's product Certificate, Certification Mark or the International Certification Marks. The CB's decision to suspend shall become effective upon TÜV Rheinland Nederland's notice to the Sponsor, by registered or certified mail, while stating its reasons.

On satisfactory evidence being provided that the previously observed failure of compliance with obligations has been permanently removed by the Sponsor, the CB shall lift the suspension.

The CB shall be entitled to remove the entry from the certified products list on the NSCIB website and any other international website to reflect its decision to terminate the Certification Agreement and to suspend the Sponsor's right to use TÜV Rheinland Nederland's Certificate, Certification Mark or the International Certification Marks.

On termination of the Certification Agreement as well as on suspension of the Sponsor's right to use the Certificate, Certification Mark or the International Certification Marks granted by TÜV Rheinland Nederland, the Sponsor shall refrain from any use thereof as of the date that the termination or suspension became effective and shall not in any way convey the impression that it is still entitled to such use, all this subject to an immediate penalty of € 12,500 (twelve thousand five hundred euros) in the event of a violation of this stipulation, plus € 2,500 (two thousand five hundred euros) per day for each day of such violation.

Within thirty (30) days after receipt of the notification the Sponsor may appeal to the Board of Appeal against the CB's decision of termination or suspension.

4.9. Publicity

In the NSCIB a distinction is made between different kinds of publications depending on the phase of the Certification Process.

4.9.1 Prior to the start of the Certification Process

Parties shall not associate the TOE with the CB (or parties within the CB) until a Certification Agreement has been entered into.

4.9.2 During the Certification Process

The Sponsor may, for the time that he has a Certification Agreement with the CB, publicly state that his TOE is 'under Common Criteria certification', possibly provided with details such as the ST Assurance Level.

The CB shall publish (on the NSCIB website) an overview of all TOEs for which a Certification Agreement is active, unless the Sponsor objects in the application or during the kick-off meeting.

4.9.3 Following granting a Certificate to the Sponsor

The Sponsor is free to publish its right to use the Certificate and the International Certification Mark for the TOEs referred to in the Certification Agreement. The Sponsor requires permission from the CB for publications in which the CB (or parties within the CB) is related to the TOE in any other way. The content of the Certification Report shall only be made available to third parties unabridged and in the original language. No written permission by the CB is required.

The CB shall publish (on the NSCIB website) an overview of all TOEs that have been certified by the CB, and per TOE:

- The Certification Report
- The ST

unless the Sponsor objects, in which case the Certificate cannot be recognised under the international recognition arrangements and the right to use the international certification marks (see section 4.3, *Use of the International Certification Marks*) is forfeited.

The NSCIB website will link to applicable international lists of certified TOEs and PPs. NLNCSA as participant in the international agreements CCRA and SOGIS MRA shall regularly update the NL entries to these lists.

4.10. Validity of a Certificate

The period of validity of the Certificate starts on the date of issuance and terminates if:

- The Certification Agreement is terminated because the Sponsor no longer complies with the conditions that the CB imposes under the Scheme Documentation (Part 2);
- The period of validity expires i.e. after the expiry date mentioned on the Certificate.

During the period of validity, the Sponsor shall immediately inform the CB if there were any alterations made to the certified version of the product or if he becomes aware of relevant vulnerabilities that have been found after the date of certification. If so, re-certification is required and the CB reserves the right to revoke the certificate's status.

4.11. Liability

TÜV Rheinland Nederland shall not be liable for any loss incurred by the Sponsor resulting from the use of a Certification Agreement or its termination, or in the event of TÜV Rheinland Nederland showing culpable negligence in implementing its obligations for direct losses to the client up to a maximum of the amount owed by the client for the certification procedure.

The Sponsor shall hold the CB harmless against any claims by third parties regarding defects in the TOE certified by the CB.

4.12. Objections and Appeal

TÜV Rheinland Nederland shall set up a Board of Appeal in charge of judging appeals against decisions or measures taken by the CB, particularly against:

- rejection of an Application;
- disciplinary action;
- termination or suspension;
- not entering into a Certification Agreement.

The procedure for approaching the Board of Appeal, the manner in which a judgment is to be arrived at and announced, are laid down in the Regulations of TÜV Rheinland Nederland's Board of Appeal.

The Sponsor may appeal against a negative certification decision within thirty (30) days observing the procedure laid down in the Regulations of the TÜV Rheinland Nederland Board of Appeal.

5. Assessment Guidelines Common Criteria

5.1. Definitions and Amendments

The Assessment Guidelines used in the NSCIB for the certification of security in TOEs are the Common Criteria for Information Technology Security Evaluation (CC), the relevant Common Evaluation Methodology (CEM) as well as internationally agreed Supporting Documents and Netherlands Scheme Instructions [NSI].

The Common Criteria, their methodology and their Supporting Documents shall be specified by an international group of experts, as defined by [CCRA] or [SOGIS-MRA]. This international group shall also decide on the release of any new versions.

When this group releases a new version of the CC, the CEM, or Supporting Documents, then these shall immediately become binding for all evaluations starting from that date on. For running Evaluations this is decided on an individual basis by the CB in cooperation with the Sponsor and ITSEF.

If the CB decides on a new Netherlands Scheme Instruction, then this shall immediately become binding for all evaluations starting as of that date. For running Evaluations this is decided on an individual basis by the CB in cooperation with the Sponsor and ITSEF.

5.2. Uncertainty in the Assessment Guidelines Common Criteria

If any uncertainty in the assessment guidelines arises during an Evaluation, the CB, Sponsor, and ITSEF shall find an acceptable interpretation of the criterion. If the uncertainty is not TOE specific, a change request may be sent to an international group of experts. If the ITSEF, Sponsor, and CB are unable to decide on an acceptable interpretation, the ITSEF shall submit a Request for Interpretation (RI) at the CB. The CB shall then make a binding judgement about the interpretation, based on comparable cases.

If the CB cannot answer the RI based on comparable cases the CB shall, after making the Request anonymously, ask other ITSEFs, other CBs, or the international group of experts to make a judgement. The CB shall make binding judgement based on the received interpretations.

The interpretation shall be added to the Netherlands Scheme Instructions.

The interpretation may, to the discretion of the CB, be presented to the international group of experts for validation. If they change the interpretation then this new interpretation shall be binding rendering the old interpretation null and void.

6. Additional Stipulations

Any dispute arising between parties in connection with the Certification Agreement, or as a result of other agreements arising thereby, which cannot be settled by mutual consent or do not fall within the competence of the Board of Appeal, shall be settled in accordance with the laws of The Netherlands by competent courts in The Hague.

Any disputes shall be governed in accordance with the laws of The Netherlands.

The CB reserves the right to alter the regulations as defined in the NSCIB Scheme Documentation. Sponsors having concluded a Certification Agreement shall be kept informed of any alterations in the regulations if these alter the conditions of their Certification Agreement. Sponsors not agreeing with the alterations shall be deemed to have terminated their Certification Agreement, whereupon the CB will cancel the Certificate.

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

Part 3 – Licensing of an ITSEF



1. Introduction

In this part of the Scheme Documentation, the conditions that apply for a Licensing Agreement that a Certification Body (CB) enters into with an ITSEF are defined. Only ITSEFs that have a license from the CB are authorised to perform Evaluations under the CB.

The CB requires the following from the ITSEF to be licensed:

1. The ITSEF shall have a demonstrable functioning quality system;
2. The ITSEF shall employ staff having demonstrable general technical skills, IT skills, and Common Criteria knowledge;
3. The ITSEF shall be demonstrably able to handle the Common Criteria and the Common Evaluation methodology;
4. The ITSEF shall demonstrate that the organisation, the staff, and the processes are sufficiently secure.

This part of the Scheme Documentation defines how the conformance of ITSEFs to the above requirements can be assessed.

2. Demonstrable Quality

The ITSEF shall have a demonstrable functioning quality system.

2.1. Conformance to this Requirement

An ITSEF conforms to this requirement if it has an ISO/IEC-17025 accreditation with relevant scope, meaning a scope sufficiently related to IT Security Testing, either related to the Common Criteria or not.

The CB shall assess whether the scope is sufficient; if not, then the scope shall be broadened to the extent deemed sufficient by the CB.

Obtaining the ISO/IEC-17025 Certificate is in principle beyond the scope of these regulations, and is a matter between the ITSEF and an internationally recognised accreditation body (in The Netherlands: the Dutch Accreditation Counsel, RvA). However, the CB can support this process by:

- Acting as an expert
- Accepting the test evaluation (see Section 4, *Demonstrable Application of Assessment Guidelines*) as a test performance for the ISO/IEC-17025 accreditation.

2.2. Maintaining Conformance to this Requirement

Maintaining conformance to ISO/IEC-17025¹⁷ by an ITSEF is an absolute condition for retaining the license.

An ITSEF shall keep the CB informed, without delay, of all changes (e.g. cancellation) in its ISO/IEC-17025 accreditation status. The CB shall subsequently contact the body that has cancelled the ISO/IEC-17025 accreditation to be informed about the reasons. Based upon these reasons, the CB shall decide to:

- Either, suspend the Common Criteria license until the ISO/IEC-17025 has been granted anew. Any Evaluations run by the concerned ITSEF shall also be suspended and no new Applications shall be considered by this ITSEF. The CB shall inform the relevant Sponsors about the suspension. The CB shall also agree with the ITSEF a period of time in which the accreditation shall be obtained anew. In case this is not obtained, the Common Criteria shall be suspended and the procedure below shall apply.
- Or, suspend the Common Criteria if it is deemed improbable that the ITSEF will obtain the ISO/IEC-17025 accreditation anew within a reasonable time. All running Evaluations shall be terminated according to the procedure in Section 3.1.1, *By the Certification Body*, from Part 2 of the Scheme Documentation.

¹⁷ Or, when this standard is replaced, the successor.

3. Demonstrable Competence and Skills

The ITSEF shall employ staff having demonstrable general technical skills, IT skills, and Common Criteria knowledge.

3.1. Conformance to this Requirement

This requirement is partly fulfilled by the ISO/IEC 17025 accreditation that supervises the possession of competence and skills. The CB is responsible for ensuring that the ITSEF employs evaluators that have a general knowledge of the Common Criteria. This can be achieved in one of the following ways:

- The CB organises a CC training course;
- An external or third party that is approved by the CB organises a CC training course.

The CC training course is concluded with an examination organised under the responsibility of the CB. A candidate can only become a licensed Evaluator by passing this exam.

Generally, the course is only started when the ITSEF is relatively well on its way with the ISO/IEC-17025 accreditation or when this has been completed.

Should ITSEF staff have done an alternative course with a different CB, the CB may decide to recognise this course as being equivalent. ITSEF staff that have done this course are, in that case, not obliged to do the course.

When a new ITSEF applies at the CB for a licence, the ITSEF shall:

1. Ensure that all staff that are going to conduct evaluations do a CC course,
2. Submit a Work Plan to the CB,
3. Submit a Training Plan to the CB for all staff with the ITSEF. This plan shall include the knowledge that has already been built up. For staff involved in technical areas (i.e. staff participating in evaluations rather than staff involved in the 'business' of running the ITSEF), the Training Plan will describe the technical competences of each staff member. NLNCSA technical experts will review the plan and state if any ITSEF staff members should receive additional training within the following year. Particular attention must be paid to detailing the competences of staff members involved in product types "smart card and similar devices" and "hardware devices with security boxes" and their competences in the areas of RNG evaluation, cryptography, side channel assessments and formal methods.
4. The CB shall decide whether this knowledge is sufficient.

3.2. Maintaining Conformance to this Requirement

Maintaining conformance to this requirement shall be tested according to the following points:

- Adhering to ISO/IEC-17025 by the ITSEF is an absolute condition for retaining the license.
- The quality of the IRs and the ETR shall be tested during the Monitoring Phase of the Certification Process (see Part 2, Section 2.1.2, *Monitoring Phase*).
- Relevant complaints to the CB about the ITSEF.

4. Demonstrable Application of Assessment Guidelines

The ITSEF shall be demonstrably able to handle the Common Criteria and the Common Evaluation methodology in general. Furthermore the ITSEF shall be demonstrable able to handle the Common Criteria and Common Evaluation methodology as specified in Supporting documents for the technical domains the license is meant for.

4.1. Conformance to this Requirement

To conform to this requirement, the ITSEF shall perform a Test Evaluation of a Test TOE with Test Documentation, to be delivered by the CB. This Evaluation shall have an Assurance Level of EAL3+. The Test Evaluation shall be performed completely according to the procedures in Part 2, with one exception: the Evaluation evidence shall be evaluated only once instead of until passing Evaluation evidence.

Generally, the Test Evaluation shall only be started when:

- At least 3 ITSEF staff members have completed a CC training course successfully;
- A documentation investigation as part of the ISO/IEC-17025 accreditation has been completed successfully. The ITSEF shall submit the results of this documentation investigation.

If the ITSEF has performed an alternative Test Evaluation or a real Evaluation with a different CB for EAL3+ or a higher Assurance Level, in which staff of the CB was involved, then the CB may decide to recognise this Evaluation as being equivalent to its own Test Evaluation. An ITSEF that has done such an alternative Test Evaluation is, in that case, not obliged to do the Test Evaluation.

4.2. Maintaining Conformance to this Requirement

Maintaining conformance to this requirement shall be tested according to the following points:

- The quality of the IRs and the ETR shall be tested during the Monitoring Phase of the Certification Process (see Part 2, Section 2.1.2, *Monitoring Phase*).
- Every ITSEF staff member allowed to work as an Evaluator shall take part in at least one (1) Common Criteria Evaluation per year.
- Every ITSEF shall employ a minimum of three (3) Evaluators, who have - at least - done the CC training course.
- Yearly the CB shall perform an audit to verify the ITSEFs capabilities for the technical domains it has be licensed for.

5. Demonstrable Security

The ITSEF shall demonstrate that the organisation, the staff, and the processes are sufficiently secure.

5.1. Conformance to this Requirement

To conform to this requirement the ITSEF shall submit a Security Document to the CB. This document shall define the way the ITSEF facilitates:

- Confidentiality of Sponsor and CB information.
- Integrity of documents and reports.

Special attention shall be paid to electronic storage and exchange of information. The Security Document shall be part of the Quality Documentation according to ISO/IEC-17025.

The security shall be in accordance with the Security Requirements for TOE Developers in relation to achieving a certain EAL (ALC_DVS). The CB shall decide whether this security is sufficient.

5.2. Maintaining Conformance to this Requirement

Maintaining conformance to this requirement shall be tested according to the following points:

- Adhering to ISO/IEC-17025 by the ITSEF is an absolute condition for retaining the license.
- Relevant complaints to the CB about the ITSEF.

6. The Licensing Process

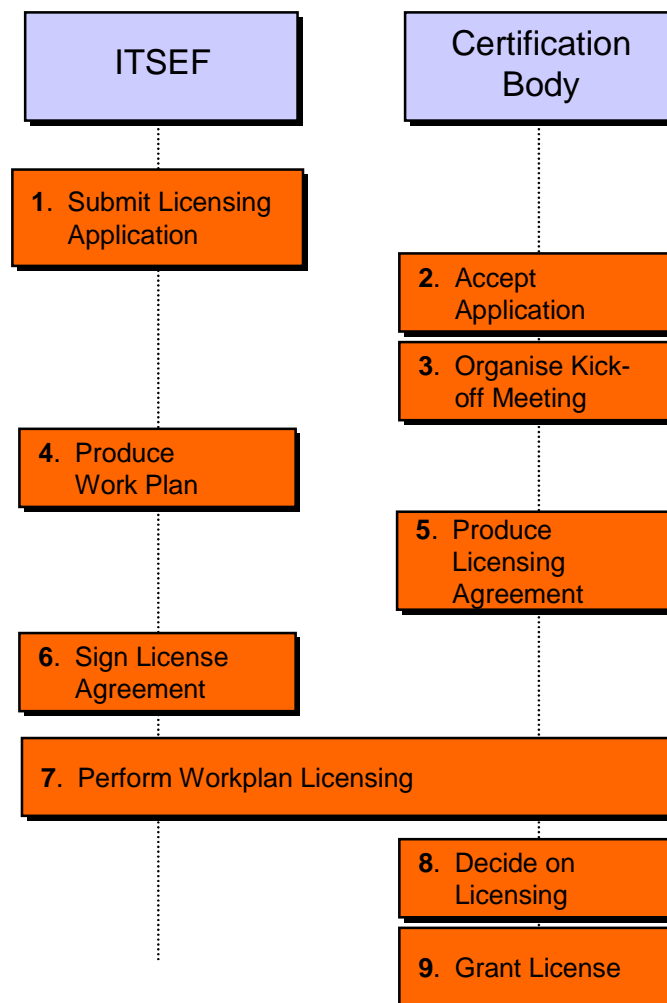


Figure 3-1, Activities and Actors in the Licensing Process

6.1. Start of the Licensing Process

The Licensing Process shall start with the submission at the CB of an Application by the ITSEF. The CB shall assess the Application on the following points:

- Existing Quality Procedures;
- Existing IT knowledge and skills;
- Existing acquaintance with Common Criteria;
- Existing Security Procedures;
- A Work Plan containing the realised steps to evolve from the existing situation to a licensed Evaluation Facility.

In case the CB rejects the Application, it shall send to the ITSEF a notification about this matter, in writing, including their motivation for this. The options for making an appeal are described in Part 2, Section 4.12, *Objections* and *Appeal*.

When an Application has been rejected, the CB shall not consider a renewed Application of the same ITSEF, unless the ITSEF can plausibly argue that the issues that led to the rejection of the earlier Application, have been dealt with.

If the CB accepts the Application, then the CB shall confirm this to the ITSEF in writing and at the same time inform the ITSEF about the Licensing-ID¹⁸ and the assigned Evaluation Supervisor¹⁹.

6.2. Kick-off Meeting

The CB shall subsequently organise a Kick-off Meeting with CB and ITSEF. At this Kick-off Meeting the following items shall be discussed:

- Information to the ITSEF, to ensure that this is aware of the Licensing Process, the roles, the responsibilities, and the cost;
- The status of the ITSEF in relation to the ISO/IEC-17025 accreditation (or possibly similar accreditations obtained earlier such as ISO-9002);
- The status of the ITSEF in relation to training (has a regular or an alternative course been done) to enable the CB to adapt its course;
- The status of the ITSEF in relation to the Test Evaluation (has a regular or an alternative Test Evaluation been done) to enable the CB to adapt its Test Evaluation;
- The preliminary Licensing Work Plan, addressing the three requirements: ISO/IEC-17025, training, and Test Evaluation;
- The draft Licensing Agreement, in which the above shall be defined by contract.

6.3. Licensing Agreement

Following the Kick-off Meeting the CB shall produce a Licensing Agreement and send this to the ITSEF. This Licensing Agreement is a quotation for performing the Licensing. The CB may reserve the right not to enter into a Licensing Agreement, unless the CB has an obligation to do so. The CB shall send to the ITSEF a motivated notification about this matter. The options for making an appeal are described in Part 2, Section 4.12, *Objections* and *Appeal*.

The CB reserves the right to reject the Licensing Agreement after all when this is returned later than thirty (30) days after sending out to the ITSEF.

6.4. Execution

ITSEF and CB shall subsequently execute the Licensing Plan until the ITSEF fulfils all of the requirements, or until the process is terminated prematurely.

6.5. Licensing

When the ITSEF fulfils all of the requirements, according to the CB's judgement, the CB shall license the ITSEF by issuing a License. From that moment on, the ITSEF is authorised to perform Evaluations under the NSCIB.

In the License it shall clearly be stated for which Technical Domains the ITSEF is authorised to perform Evaluations under the NSCIB.

If the ITSEF wants to be licensed for a new Technical Domain, a Test Evaluation with a suitable product has to be performed in order to demonstrate the skills in the new technical domain (see also paragraph 4.1.)

6.6. Prematurely Termination of the Licensing Process

The Licensing Process can be terminated prematurely by both parties: ITSEF and CB.

6.6.1 By the CB

If either of the following conditions apply:

- The ITSEF seriously or repeatedly fails to meet the Licensing Plan;

¹⁸ The reference to the Licensing Process of this ITSEF.

¹⁹ The contact of the CB during the Licensing Process.

- Not the minimal 3 ITSEF staff members pass the course examination;
- The Test Evaluation is not up to level;

If in the opinion of the CB the likelihood of a positive Licensing result are at risk, the CB may decide:

- To warn the ITSEF that if this situation persists the Licensing Process shall be terminated;
- To terminate the Licensing Process. In this case the CB shall inform the ITSEF about the termination, in writing and with a motivation.

If the CB terminates the Licensing Process, the CB shall not accept a new Application for the same ITSEF, unless the ITSEF can plausibly argue that the issues that led to the rejection of the earlier Application, have been dealt with.

6.6.2 By the Evaluation Laboratory (ITSEF)

The ITSEF may, at all times, terminate the Licensing Process by informing the CB in writing.

6.7. Publication

In the NSCIB a distinction is made between different kinds of publications depending on the phase of the Licensing Process.

6.7.1 Prior to the Licensing Process

The ITSEF shall not associate itself with the CB (or parties within the CB) until a Licensing Agreement has been entered into.

6.7.2 During the Licensing Process

The ITSEF may, for the time that it has a Licensing Agreement with the CB, publicly state that it is 'under Licensing' with the CB, possibly provided with details.

The CB shall publish (on its website) an overview of all ITSEFs for which a Licensing Agreement is active, unless the ITSEF objects.

6.7.3 Following obtaining the Licence

The ITSEF is free to publish that it has been licensed under the NSCIB.

The CB shall publish (on its website) an overview of all ITSEFs that have been licensed by the CB.

The CB shall regularly add this overview to applicable international lists of licensed ITSEFs.

7. Maintenance of the Licence

7.1. Continuation of the Licence

In order for the ITSEF to continue their license the following information needs to be provided:

- An ITSEF is required to submit a copy of the ISO/IEC-17025 certificate to the CB subsequent to any changes to the previous ISO/IEC-17025 certificate in order to demonstrate its compliance to section 2.2, *Maintaining Conformance to this Requirement* (Demonstrable functioning quality system).
- An ITSEF is required to annually submit a list to the CB describing the qualified evaluators currently employed by the ITSEF and their associated “General and Specialised IT” competences in order to demonstrate compliance to section 3.2, *Maintaining Conformance to this Requirement* (Demonstrable competence and skills).
- An ITSEF is required to annually submit a list to the CB describing the qualified evaluators currently employed by the ITSEF and their associated “Common Criteria and Common Evaluation Methodology” competences in order to demonstrate compliance to section 4.2, *Maintaining Conformance to this Requirement* (Demonstrable application of assessment guidelines).
- An ITSEF is required to inform the CB of changes to its technical infrastructure and measures employed to enforce security in order to demonstrate compliance to section 5.2, *Maintaining Conformance to this Requirement* (Demonstrable security).

The Certification Body will perform an annual formal technical assessment of the ITSEF focussing on the verification of the technical competence of its personnel and test equipment within the scope of assurance levels beyond EAL4 in the technical domains for which the CB is internationally qualified. The scheme reserves the right to involve technical experts related to specific tasks such as formal methods, smart card attacks and cryptographic assessments.

The scheme instruction “Demonstrable Application of Assessment Guidelines” defines how the ITSEFs capabilities to handle the Common Criteria and Common Evaluation Methodology is maintained by the CB.

7.2. Suspension and Termination of the Licence

In case either the Certification Body or ITSEF wishes to terminate the license, the relevant party shall notify the opposite party in writing, stating reasons, while mentioning the date on which termination is to be effective.

If an ITSEF fails in meeting the requirements for maintaining their license, the Certification Body shall be entitled to suspend the license. The Certification Body will provide an advance indication of their intention of suspension (e.g. multiple warnings) with the possibility to solve the issues before taking a formal decision on suspension of the license. The Certification Body’s decision to suspend shall become effective on the date of communication to the ITSEF by registered or certified mail. The communication notice will state the Certification Body’s reasons and the period of time the ITSEF is granted to address the failure to meet the requirements.

During the period that an ITSEF’s license is suspended, the certification body will not accept any new certification applications for evaluations that will be performed by said ITSEF.

Once satisfactory evidence being provided that the previously observed failure of compliance with requirements has been permanently removed by the ITSEF, the Certification Body shall lift the suspension. Failure to provide satisfactory evidence within the suspension time period shall result in termination of the license.

The Certification Body shall be entitled to publish its decision to terminate the license (on its website) and to request to removal of the ITSEF from applicable international lists of licensed ITSEFs.

The options for making an appeal are described in Part 2, Section 4.12, *Objections* and *Appeal*.

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

Part 4 – Roles in the Certification Body



1. Introduction

This part of the Scheme documentation describes for the NSCIB, the activities, the obligations, and the rights of the Certification Body (CB) insofar as these are no part of the Certification or the Licensing Process.

2. Roles in the CB

The roles in the CB can be distinguished into:

- Scheme Administrator
- Board of Appeal
- Evaluation Supervisor
- Scheme Supervisor
- Certificate Issuer
- License Issuer

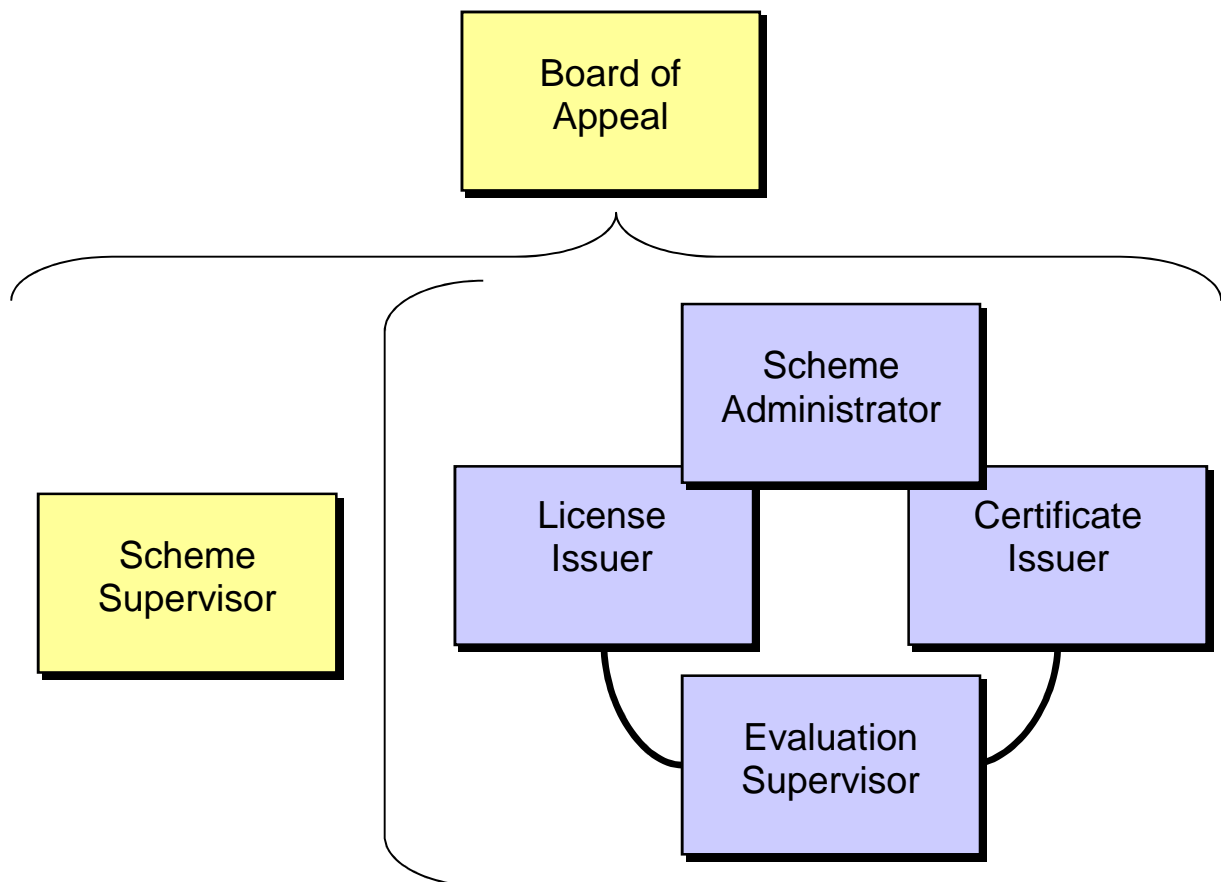


Figure 4-1, Roles in the CB

2.1. Scheme Administrator

This role shall be performed by TÜV Rheinland Nederland, an organisation that administrates several Schemes and conforms to ISO/IEC 17065.

The Objective of this role is to warrant the continuity of the NSCIB and to maintain the relevant Quality System. The Administrator has the following tasks:

- Managing contractual matters with Sponsors and ITSEFs;
- Ensuring that Certification and Evaluation Processes are performed correctly. This includes a periodical scheme audit;
- Maintenance and Publication of the NSCIB regulations and the related documents including (updates to) the Scheme Documentation.

Once a year, the scheme documentation is reviewed for potential updates. Updates of the scheme documentation are generally prepared by the Evaluation Supervisor, checked by the Scheme Administrator, approved by the head of the Certification Body and validated by the Scheme Supervisor.

2.2. Board of Appeal

This role shall be performed by a Board of Appeal established by the Advisory Board of TÜV Rheinland Nederland. This role operates independently of other roles.

The objective of this role is to give binding judgements about Appeals lodged by third parties concerning the functioning of the CB with regard to Certification matters of the NSCIB.

Part 2 of this Scheme Documentation describes the cases for which the Board of Appeal may be called in.

2.3. Evaluation Supervisor

This role shall be performed by a staff member of the Ministry of the Interior and Kingdom Relations, Netherlands National Communication Security Agency, or someone that operates under their supervision. The representative of the BZK/NLNCSSA who delivers expertise to the TÜV Rheinland Nederland shall be independently authorised to give judgements. The relationship between BZK/NLNCSSA and TÜV Rheinland Nederland shall be based solely on Certification Activities.

The objective of this role is to support the Issuer of Certificates in making assessments concerning the content of Evaluations performed under the NSCIB. The Evaluation Supervisor shall monitor the Evaluations by the licensed ITSEFs of the NSCIB according to the scheme instruction "Performing technical oversight" and has the following tasks:

- Validating certification applications and licensing applications;
- Organising Kick-off Meetings at the start of a Certification or a Licensing Process;
- Review of the Work Plan (WP) and its updates as produced by the ITSEF;
- Review of Evaluation evidence and/or Reports produced by the ITSEF, i.e. IRs, and ETRs;
- Giving advice to the Issuer of Certificates on IRs and ETRs. This advice may mean acceptance or modification of documents;
- Giving advice whether a Certificate for a certain Application shall be granted or not by composing a Certification Report. Only when a positive advice is given (no objection against granting a Certificate) may TÜV Rheinland Nederland grant a certificate;
- A statement, indicating that the Evaluation Supervisor has neither taken part in the assessment in the Evaluation nor in the development of the TOE, will accompany the positive advice (no objection against granting a Certificate);
- Issuing Netherlands Scheme Instructions in case of an unclarity in the Assessment Guidelines that is not covered by International Interpretations;
- Organising meetings between the licensed ITSEFs about the interpretation of criteria or a certain way of working of the licensed ITSEF. The Scheme Administrator shall be informed about this;
- Preparing updates of the scheme documentation;
- Participating in commissions in which the content of the Common Criteria is discussed.

In addition the Evaluation Supervisor will assure the reliability of the performed activities of each ITSEF according to the scheme instruction "Demonstrable Application of Assessment Guidelines"

The tasks, the mutual responsibilities, and the way of working between TÜV Rheinland Nederland and the Evaluation Supervisor is formalised by contract.

Demonstrable competence is required for performing this role. To make sure that CC certifications are being performed by qualified personnel, the scheme instruction "Qualification of NSCIB personnel performing technical oversight" is applicable.

The reliability and the integrity of the representative of the BZK/NLNCSSA is warranted by either the national security screening that this representative has passed successfully or a written and signed pledge of confidentiality.

2.4. Scheme Supervisor

This role shall be performed by the Advisory Board of TÜV Rheinland Nederland. A representative of the BZK/NLNCISA shall be a member of the Advisory Board and he supplies his expert knowledge in the field of the Assessment Guidelines. This role operates independently of other roles.

The objective of this role is to assess and monitor the NSCIB. This includes:

- validating updates of the scheme documentation;
- ensuring that the scheme continues to share the objectives mentioned in the International recognition agreements;
- reviewing the results of the scheme audits.

Part 2 of this Scheme Documentation describes in which cases the Advisory Board shall come into action.

2.5. Certificate Issuer

This role shall be performed by TÜV Rheinland Nederland.

The objective of this role is to issue Common Criteria certificates to Sponsors with a PP, IT product or System, when

- The PP, IT product or System has been successfully evaluated by a licensed ITSEF, and
- The Supervisor of Evaluations has accepted the ETR.

The Issuer of Certificates has the following tasks:

- Taking a formal Certification Decision (see also Section 2.3, *Evaluation Supervisor*);
- The Issuance of Common Criteria Certificates;
- Monitoring correct use of the TÜV Rheinland Nederland Logo and the International Certification Marks;
- Monitoring correct use of Common Criteria Certificates;
- Publication and filing of running Evaluations;
- Publication and filing of certified PPs, IT Products and Systems (inclusive of the relevant documents ST, CR, ETR).
- Ensuring that the content of Common Criteria certificates complies with the [CCRA] and [SOGIS-MRA] requirements.

2.6. License Issuer

This role shall be performed by TÜV Rheinland Nederland.

The objective of this role is to issue licenses to ITSEFs that conform to the requirements described in Part 3 of this Scheme Documentation.

The Issuer of Licenses has the following tasks:

- Taking a formal Licensing Decision;
- Monitoring correct use of NSCIB licenses;
- Publication of the ITSEFs associated with the NSCIB.

3. Internal Quality Processes

The Internal Quality Processes required for the CB are defined by the Baseline Document 'Kwaliteitsmanagementsysteem' [TÜV-KMS]. These shall be used for the NSCIB as much as possible. The NSCIB documentation is binding for CC Evaluations and shall prevail in case of contradictions.

4. International Recognition of Certificates

One of the objectives of the NSCIB is the recognition of Common Criteria Certificates issued by the TÜV Rheinland Nederland on the basis of the [CCRA] and the [SOGIS-MRA]. Both TÜV Rheinland Nederland and BZK/NLNCSA have the responsibility to ensure that all obligations defined by the [CCRA] and [SOG-IS] are performed in the NSCIB. In addition shall BZK/NLNCSA for this purpose facilitate the following:

- Taking part in the Management Committee of each respective Recognition Agreement;
- Taking part in the relevant sub-committees;
- Taking part in any other relevant meetings or conferences;
- Arrange that Certification Marks may be used in The Netherlands and that the Certification Marks are protected by law.

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

Part 5 – Appendices



1. Application Form to Initiate a Certification Process

The current application form to initiate a Certification Process can be found on the NSCIB website.

2. Certification Agreement Template

CONFORMITY CERTIFICATION AGREEMENT {CERTIFICATIE-ID}

COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

Parties

TÜV Rheinland Nederland B.V., The Netherlands, Chamber of Commerce number 27288788, Postal address: P.O. Box 2220, 6802 CE Arnhem, The Netherlands, hereinafter referred to as "TÜV Rheinland",

and

{SPONSOR NAME}, {SPONSOR ADDRESS} hereinafter referred to as "Sponsor"

Considering

- A. Sponsor is the manufacturer of {TOE NAME}, hereinafter referred to as "the Product";
- B. Following the application form dated {APPLICATION DATE}, Sponsor wishes to have the above mentioned Product examined by TÜV Rheinland according to the Netherlands Scheme for Certification in the area of IT Security (NSCIB), hereinafter referred to as "Guideline".
- C. The work will be done according to the final work plan, which is delivered by {NAME ITSEF} and approved by TÜV Rheinland and Sponsor.

Agree the following:

1. The Regulations for the delivery conditions as mentioned in the Guideline are applicable with the exclusion of the Purchase Conditions of Sponsor. The Guideline is published on the Website: www.tuv-nederland.nl.
2. TÜV Rheinland will ascertain whether the Product meets the Guideline. TÜV Rheinland will then issue Sponsor with a Certificate.
3. The cost for the certification, including one certificate, will be EUR #,-- excluding VAT. {OPTIONAL: Additionally the cost of a certifier will be EUR #,-- excluding VAT.}
4. Unless agreed otherwise, all prices mentioned in this Agreement are net prices; banking charges are for the account of Sponsor.
5. An invoice of {SELECT 50% OR 100%} of the costs is payable before the start of the certification.
6. The Certificate will be made out in the English language and is valid for 5 years under the condition of a yearly declaration that the product or production process is not altered and the sponsor is not aware of relevant vulnerabilities that have been found after the date of certification.
7. After a positive decision the Certificate including the Security Target will {SELECT NOT} be published on the website of TÜV Rheinland.
8. Termination of the certificate by Sponsor has to be done in writing, at least 1 month before the desired end date.
9. The mentioned costs are based on the tariffs of 20.. and subject to changes
10. This agreement is drawn up under Netherlands Law and any disputes arising hereunder shall be resolved in accordance with the laws of the Netherlands.

Thus agreed and signed in twofold,

3. Work Plan Template

- 1 Introduction
 - 1.1 Status
 - 1.2 Purpose of the document
 - 1.3 Identifiers
 - 1.4 Points of contact
 - 1.5 Structure of the document
 - 2 Evaluation criteria and documentation
 - 2.1 Criteria and methodology
 - 2.2 International interpretations and guidelines
 - 2.3 Scheme Instructions
 - 2.4 Guidelines
 - 3 TOE evaluation
 - 3.1 Background information
 - 3.2 Personnel assignment
 - 3.3 Start meeting
 - 3.4 Evaluation approach
 - 4 Miscellaneous
 - 4.1 Formats and languages
 - 4.2 Management information exchange
 - 4.3 Document updates
 - 4.4 Confidential exchange of information
- A Appendix Overall planning

4. Intermediate Report Template

- 1 Introduction
 - 1.1 Status
 - 1.2 Identifiers
 - 1.3 Structure of the document
- 2 Basis of the evaluation and documentation used
- 3 Evaluation objective / dependencies
- 4 Evaluation summary
 - 4.1 Verdict
 - 4.2 Actions
 - 4.3 (Possible) vulnerabilities found
- 5 Evaluation results
 - 5.x Evaluation action elements
 - 5.x.y Work units
- 6 Annex
 - 6.1 Glossary of terms and abbreviations
 - 6.2 References

5. Review Report Template

- 1 Document information
- 2 Subject of review
- 3 General comments
- 4 Detailed comments
- 5 Verdict / requested actions

6. Evaluation Technical Report Template (TOE)

- 1 Document information
 - 1.1 Status
 - 1.2 Identifiers
 - 1.3 Structure of the report
- 2 Introduction to evaluation
 - 2.1 Target of Evaluation
 - 2.2 Persons involved
 - 2.3 Evaluation schedule
 - 2.4 Foundations of the evaluation
 - 2.4.1 Criteria
 - 2.4.2 Conformity claims
 - 2.4.3 Type of evaluation
- 3 TOE scope of delivery
 - 3.1 Overview of delivery items
 - 3.2 Identification of the TOE by customers
- 4 Architectural description
 - 4.1 TOE definition
 - 4.2 Logical architecture
 - 4.3 Security Functions (or Features)
 - 4.4 Life-cycle
- 5 Results of the evaluation
 - 5.1 Other evaluation reports
 - 5.2 Locations audited
 - 5.3 TOE configuration description
 - 5.5 Developer testing
 - 5.6 Independent testing
 - 5.6.1 Approach
 - 5.6.2 Test configuration description
 - 5.6.3 Summary of testing performed
 - 5.7 Penetration testing results
 - 5.7.1 Approach
 - 5.7.2 Summary of vulnerability analysis results
 - 5.7.3 Test configuration description
 - 5.7.4 Summary of testing performed
 - 5.7.5 Verdict
 - 5.8 Results of other configurations
 - 5.9 Specific limitations and exceptions
- 6 Vulnerabilities
 - 6.1 Exploitable vulnerabilities

- 6.2 Residual vulnerabilities
 - 7 Obligation and recommendations
 - 7.1 Obligations and recommendations for the use of the TOE
 - 7.2 Obligations and recommendations for the manufacturer
 - 8 Evaluation conclusions and Votum
-
- A Appendix: Glossary of terms and abbreviations
 - B Appendix: References
 - C Appendix: Developer evidence

7. Certification Report Requirements

Foreword

- 1 Executive Summary
- 2 Certification Results
 - 2.1 Identification of Target of Evaluation
 - 2.2 Security Policy
 - 2.3 Assumptions and Clarification of Scope
 - 2.4 Architectural Information
 - 2.5 Documentation
 - 2.6 IT Product Testing
 - 2.7 Evaluated Configuration
 - 2.8 Results of the Evaluation
 - 2.9 Evaluator Comments/Recommendations
- 3 Security Target
- 4 Definitions
- 5 Bibliography

8. Certificate Template

Certificate

Standard Common Criteria for Information Technology Security Evaluation (CC),
Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number **CC-YY-xxxxxx**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder **Sponsor Name**

and developer

Located in Full address, Country

Product and assurance level **TOE name, Unique Identifier,**

Assurance Package:

§ EAL#4#augmented with X and Y

Protection Profile Conformance (if appropriate):

§ PP Certification ID: PP Title, PP Configuration (if appropriate),
PP Version, Issue Date

Project number **NSCIB-CC-xxxxxx**

Evaluation facility **BrightSight/Riscure BV located in Delft, the Netherlands**



Common Criteria Recognition
Arrangement for components
up to EAL2



SOGIS Mutual Recognition
Agreement for components up
to EAL4 or 7

Applying the Common Methodology for Information Technology Security
Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity Date of issue : ##-##-20##

Certificate expiry : ##-##-20##



Accredited by the Dutch
Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands