001 Certification and Evaluation Scheme - Scheme Overview

Issue: 19.0, 2013-Sep-26

Authorisation: Dag Ströman, Head of CSEC, CSEC
Table of Contents

1 Preface 3
  1.1 Purpose 3
  1.2 Typography 3

2 Introduction 4
  2.1 Overview 4
  2.2 Goals and Objectives of the Scheme 5
  2.3 Brief Description of the Scheme 6
  2.4 Mutual Recognition 7
  2.5 Relevant Legislation, Standards and Regulations 8
  2.6 Trademarks 9
  2.7 Documentation 9

3 Types of Certifications 11
  3.1 Protection Profile Certification 11
  3.2 Product Certification 11

4 Roles within the Scheme 12
  4.1 Sponsor 12
  4.2 Developer 12
  4.3 ITSEF 12
  4.4 Certification Body 13

5 Processes within the Scheme 14
  5.1 Management of Confidential Information 14
  5.2 Certification Agreement 15
  5.3 Evaluation and Certification Process 15
  5.4 Certificate Maintenance 17
  5.5 Certificate Misuse 17
  5.6 Licensing of Evaluation Facilities 18
  5.7 Mutual Recognition and International Liaison 18
  5.8 CCRA 18
  5.9 SOGIS-MRA 19
  5.10 EA MLA 19
  5.11 Interpretations 19
  5.12 Complaints, Appeals and Disputes 19

Appendix A 21
  A.1 References 21
  A.2 Abbreviations 21
  A.3 Glossary 23
1 Preface

This document is part of the description of the Swedish Common Criteria Evaluation and Certification Scheme ("the Scheme").

This document is part of a series of documents that provide a description of aspects of the Scheme and procedures applied under it. This document is of value to all participants under the Scheme, i.e., to anyone concerned with the development, procurement, or accreditation of IT products for which security is a consideration, as well as those already involved in the Scheme, i.e. employees at the Certification Body, Evaluators, current customers, contractors, and security consultants.

The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security here:

<table>
<thead>
<tr>
<th>Swedish Certification Body for IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMV / CSEC</td>
</tr>
<tr>
<td>Postal address: SE-115 88 Stockholm, Sweden</td>
</tr>
<tr>
<td>Visiting address: Banérgatan 62</td>
</tr>
<tr>
<td>Telephone: +46-8-782 4000</td>
</tr>
<tr>
<td>E-mail: <a href="mailto:csec@fmv.se">csec@fmv.se</a></td>
</tr>
<tr>
<td>Web: <a href="http://www.csec.se">www.csec.se</a></td>
</tr>
</tbody>
</table>

1.1 Purpose

This document provides a general overview of the Scheme for evaluation and certification of IT security products and protection profiles. It is intended for any party interested in the Scheme, including developers, customers, and users of IT security products.

Detailed information on specific aspects of the Scheme is provided in other documents in the series of Scheme publications.

1.2 Typography

The following terms are used to specify requirements:

- **SHALL** Within normative text, “SHALL” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC).
- **SHOULD** Within normative text, “SHOULD” indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.” (ISO/IEC)
  The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.
- **MAY** Within normative text, “MAY” indicates “a course of action permissible within the limits of the document.” (ISO/IEC).
- **CAN** Within normative text, “CAN” indicates “statements of possibility and capability, whether material, physical or causal.” (ISO/IEC).
2 Introduction

2.1 Overview

Advances in information technology (IT), the increasing number of IT systems and networks worldwide, and the increasing dependency of society on IT services have raised concerns about the security of IT.

Concerns about the security of IT products must be taken seriously. Customers of IT products need to feel confident about the security of those products, and they want to be able to compare the security features of various products to understand their capabilities and limitations. Customers also need to be able to judge whether a product is suitable for their environment and whether the product can be used efficiently within their security context. However, customers generally have limited resources available to examine and judge IT products, and might not have sufficient expert knowledge to adequately perform the task. Leaving this responsibility to individual customers also results in considerable duplication of effort if multiple customers with similar requirements separately undertake examination of IT products.

The Common Criteria (CC) establishes an international standard (ISO/IEC 15408) that addresses these needs. The Common Criteria allows the security of IT products or systems to be impartially assessed (evaluated) by an independent body, and then certified by a Certification Body that confirms the validity of the evaluation results.

Common Criteria certification is internationally recognised through multilateral recognition arrangements; a Common Criteria certificate issued by a Certification Body in one country is recognised by government organisations in other participating countries. In order for the evaluation and certification process to be repeatable and reproducible, it must be established and maintained in compliance with Common Criteria community requirements, emphasising the integrity and quality of these processes. The organisation, rules, and processes are specific for each country and are called Evaluation and Certification Schemes. Such Schemes provides the framework for international recognition of certificates issued under the Scheme.

Sweden is a member of the Common Criteria Recognition Arrangement (CCRA) and the Senior Officials Group Information Systems Security - Mutual Recognition Arrangement (SOGIS_MRA) thereby accepting Common Criteria certificates issued, under these agreements, in other countries.

Sweden is also a member of the European co-operation for Accreditation (EA). This agreement means that a test or inspection report or a certificate issued by an accredited body in one country is recognised as equivalent to a report or a certificate issued by an accredited body in any of the countries signatories to the EA MLA.

With the establishment of the Swedish Common Criteria Evaluation and Certification Scheme, the organisational and procedural context for the conduct of IT security evaluations and the issuance of Common Criteria certificates is established in Sweden (see Figure 1). FMV, the Swedish Defence Material Administration, has been appointed to define this Scheme and to operate a Certification Body. This document provides a high level description of the Scheme and the procedures applied under it.

---

1 Ordinance with instructions for the Swedish Defence Materiel Administration (SFS 2007:854); see also section 2.5 Relevant Legislation, Standards and Regulations
2.2 Goals and Objectives of the Scheme

The main purpose of the Scheme is to ensure that a high and consistent quality is maintained in evaluations under the Scheme. This is enforced by the systematic organisation and management of the evaluation and certification functions.

The Scheme provides a basis for conducting evaluations and certifications by describing and implementing the necessary legal framework and processes, thereby upholding the following principles in all evaluation activities:

- **Appropriateness**
  The evaluation activities employed in achieving an intended level of assurance shall be appropriate.

- **Impartiality**
  All evaluations shall be free from any commercial, financial, or other pressures that might influence the outcome of the evaluation.

- **Objectivity**
  Evaluation results shall be obtained with a minimum of subjective judgment or opinion.

- **Repeatability and reproducibility**
  Repeated evaluation of the same IT product or system to the same requirements with the same evaluation evidence shall yield the same results.

- **Soundness of results**
  The results of evaluation shall be complete and technically correct.

- **Cost-effectiveness**
  The value of an evaluation shall offset the time, resources, and money spent by all interested parties.

- **International recognition**
  The Scheme shall allow for the international recognition of certificates issued under it.

- **Re-usability**
  Evaluations shall make effective use of previous evaluation results.
Methodology evolution
The impact of changing environmental and technical factors on evaluations should be integrated into the evaluation methodology in a well-considered and consistent manner.

Common terminology
A common nomenclature shall be introduced for use by all parties involved in evaluation and certification activities.

In implementing these principles, the Scheme will achieve its major objectives, which are:

- to ensure that evaluations and certifications are performed to high and consistent standards and will promote confidence in the security of IT products certified under this Scheme
- to improve the availability of evaluated, security-enhanced IT products and protection profiles
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles

2.3 Brief Description of the Scheme
The cornerstone of the Scheme is the process of evaluation and certification, whereby security evaluations are carried out by licensed IT Security Evaluation Facilities (ITSEF) and certifications are carried out by the Certification Body.

Evaluation is the assessment of an IT product or a protection profile against the Common Criteria using the Common Methodology for Information Technology Evaluation (called the Common Methodology or CEM) to determine whether or not the security claims on the product or protection profile are justified.

Certification is the formal approval of an IT product or protection profile based on the result of the evaluation, and is performed by the Certification Body. The certification will result in a certification report (CR), and for successful certifications, a certificate will be issued for the IT product or protection profile.

The process of evaluation and certification involves different parties with specific responsibilities, which are detailed in Chapter 4:

- Sponsor
- Developer
- ITSEF
- Certification Body

This leads to the structure depicted in Figure 2 of the different organisations currently involved in the Scheme.
For the evaluation and certification process to work, the framework provided by the Scheme must define additional processes, which are necessary to set up the organisational context and to achieve recognition of the certificates issued.

Additional processes and procedures are:

- Assurance continuity
- Certificate surveillance
- Licensing of evaluation facilities
- Mutual recognition and international liaison
- Interpretations
- Complaints, appeals, and disputes

These processes are explained in Chapter 5 and detailed in additional documents (see section 2.7, Documentation).

### 2.4 Mutual Recognition

Certificates issued under the Scheme may be subject for mutual recognition according to the following arrangements:

- **Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security (CCRA).**
  Certification bodies accepted by the participants of CCRA as compliant may issue certificates that is recognised, under the conditions of the arrangement, by all participants of CCRA.

- **The European cooperation for accreditation MLA (EA-MLA)**
  Certification bodies accredited by an approved accreditation body within the EA may issue certificates that is recognised, under the conditions of the stipulated by EA regulations, by all signatories of the EA-MLA for the scope of product certification.

- **Senior Officials Group Information Systems Security - Mutual Recognition Arrangement - (SOGIS-MRA)**
  Certification bodies accepted by the participants of SOGIS-MRA as compliant may issue certificates that are recognised, under the conditions of the agreement, by all participants of SOGIS-MRA.
A certification performed by CSEC may be covered by all these arrangements. It is possible to engage in a certification where only one of the arrangements will be referenced. Which mutual recognition agreement that is applicable to a specific certification will be documented in the certification agreement.

It is possible to get two, or more, different certificates, one for each mutual recognition agreement, in the same certification. In this case only the certificates will differ. Only one certification report will be issued.

2.5 Relevant Legislation, Standards and Regulations

2.5.1 Government Ordinance

In the Ordinance with instructions for the Swedish Defence Materiel Administration (SFS 2007:854) the Swedish government has stated that at the Defence Material Administration (FMV) there is a Certification Body that should establish and operate a Certification Scheme for security in IT-products and systems. FMV should act to obtain and maintain international recognition for issued certificates.

2.5.2 Appropriation Directions

In the Appropriation Directions for the Swedish Defence Materiel Administration, the Swedish Department of Defence has stated that FMV shall act as national Certification Body within the area of IT-security. The Certification Body shall co-operate internationally in order to make the methodology for evaluation and certification more effective. The Certification Body shall give support and guidance in using Common Criteria for requirements specification.

FMV shall, as a result of the Government’s ambition to coordinate functions within IT-security, be Sweden’s signatory within the international agreement on mutual recognition of certification of IT-security products, the Common Criteria Recognition Arrangement (CCRA).

2.5.3 Standards

The Scheme relies on a set of international standards to support the objectives set forth in this document.

Common Criteria
First and foremost, the Common Criteria is the standard that defines IT security evaluation, with the related Common Methodology defining the methodology for evaluators to perform their work. Where questions have arisen about the intent of specific clauses of the Common Criteria or the Common Methodology, interpretations have been issued by the Common Criteria Maintenance Board (CCMB).

ISO/IEC 15408
The ISO/IEC-versions of the Common Criteria standards.

ISO/IEC 18045
The ISO/IEC-version of the Common Evaluation Methodology.

ISO/IEC 17065
For a Certification Body, ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services applies according to the regulations of the CCRA, SOGIS, and SWEDAC, to ensure the quality of certifications.
ISO/IEC 17025
For an ITSEF, ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* (earlier known as ISO/IEC Guide 25) apply according to the regulations of the CCRA, SOGIS and SWEDAC, to ensure the quality of evaluations.

2.5.4 National Regulations - STAFS
The Swedish Board for Accreditation and Conformity Assessment (SWEDAC) has issued regulations for accreditation in the field of IT Security. These regulations are complements to the general regulations for accreditation.

*SWEDAC STAFS 2010:10*
Regulations and guidelines for accreditation.

*SWEDAC STAFS 2013:15*
Regulations and guidelines for accreditation of bodies certifying products.

*SWEDAC STAFS 2007:20*
Regulations and guidelines for accreditation of bodies evaluating IT-security.

*SWEDAC STAFS 2007:21*
Regulations and guidelines for accreditation of bodies certifying IT-security.

2.6 Trademarks
Conditions for the use of trademarks applicable to the certification and licensing processes are listed in SP-070 *Conditions for Use of Trademarks*.

2.7 Documentation
This document provides an overview of the Scheme. Other documents described below give detailed information about other processes of the Scheme. All public Scheme publications are available from the CSEC website, www.csec.se.

*SP-001 Scheme Overview*
Introduces the Swedish Common Criteria Evaluation and Certification Scheme, providing an overview and a guide to the goals and objectives, roles, responsibilities, and procedures of the Scheme.

*SP-002 Evaluation and Certification*
Defines the processes and requirements for Common Criteria evaluation and certification, which are the central processes of the Scheme. IT security evaluations are carried out by licensed evaluation facilities, and certificates are awarded for successfully evaluated products and protection profiles.

*SP-003 Certificate Maintenance*
Defines how to extend the validity of a Common Criteria certificate to apply to a changed version of the Target of Evaluation, without having to repeat the evaluation and certification process.
SP-004 Licensing of Evaluation Facilities
Defines the processes and requirements for licensing an Evaluation Facility and evaluators, to ensure that evaluations will be carried out in an impartial, objective, repeatable, and reproducible manner.

SP-007 Quality Manual
Describes the standard operating procedures of the Certification Body, satisfying the requirement, from ISO/IEC 17065, that the Certification Body must have a Quality Manual.

This set of documents may be supplemented by documents addressing specific topics. For example, if evaluation of products at evaluation assurance levels higher than EAL 4 is sought, or if evaluation of systems rather than products will be carried out, additional documents may be necessary. The goal of supplemental documents is to guide sponsors, developers, evaluators, and certifiers, so that requirements for the impartiality, objectivity, repeatability, reproducibility, and appropriateness of such evaluations can be guaranteed.
3 Types of Certifications

3.1 Protection Profile Certification

A protection profile is an implementation-independent set of security requirements for a category of IT products that meet specific customer needs. A protection profile may be created by an organisation to define its security needs. Sponsors then may claim compliance to the protection profile in their security targets (ST).

A protection profile is evaluated in accordance with the requirements for protection profile evaluation contained in the Common Criteria. The goal of such an evaluation is to demonstrate that the protection profile is complete, consistent, technically sound, and suitable for use as a statement of requirements for a category of IT products. A successful evaluation following the rules of the Scheme may result in certification of the protection profile.

3.2 Product Certification

The target of evaluation (TOE) consists of an entire IT product or parts of an IT product selected for Common Criteria evaluation, along with its associated administrator and user guidance documentation. An IT product is a package of software, firmware, and/or hardware providing certain functionality.

The target of evaluation is defined in the context of a specific configuration or set of configurations, which is called the evaluated configuration of the target of evaluation. The target of evaluation is evaluated in accordance with requirements contained in the Common Criteria. A security target, a set of security requirements and specifications, is used as the basis for evaluating the target of evaluation. Investing substantial effort in creating the security target reduces the risk of running into problems later in the evaluation process. The goal of a TOE evaluation is to demonstrate that the target of evaluation meets the security requirements contained in the evaluated security target. Successful evaluation following the rules of the Scheme may result in certification of the product.
Roles within the Scheme

The parties involved in certifications under the Scheme fall into four categories: Sponsors, Developers, ITSEFs, and the Certification Body, each with its own specific role and responsibilities.

4.1 Sponsor

The Sponsor is the organisation that pays for the evaluation, applies to the Certification Body for certification, contracts with the ITSEF, and arranges for Developer participation. The Sponsor and the Developer may be the same.

The Sponsor has a formal agreement with the ITSEF for the evaluation and with the Certification Body for the certification.

The Sponsor ensures that the evaluator and the certifier are provided with evaluation evidence, training, and access to facilities in a timely manner and in accordance to the Scheme. This may require an agreement with the Developer, as well.

In some instances, more than one Developer may be involved in an evaluation, for example, in cases where subcontractors are involved in the development of an IT product, or where different organisations are responsible for developing different components of the product. Under such circumstances, it is essential for the Sponsor to ensure the cooperation of all parties.

The obligations of the Sponsor in an evaluation are detailed in Scheme publication SP-002 Evaluation and Certification.

4.2 Developer

The Developer is the organisation that produces the product to be certified. The Developer, which may be the same as the Sponsor, is responsible for supporting the evaluation by making evaluation evidence available.

If the Developer is distinct from the Sponsor, it may be necessary that the Developer and the Sponsor agree how to support the evaluation. At higher evaluation levels, extensive Developer documentation is required; if this documentation evidence is not delivered as scheduled, the entire evaluation could come to a stop.

The obligations of the Developer in an evaluation are detailed in Scheme publication SP-002 Evaluation and Certification.

4.3 ITSEF

An Evaluation Facility licensed by the Certification Body to operate under the Scheme is called an ITSEF. The ITSEF is responsible for the assessment of the protection profile or the target of evaluation by performing the evaluator actions required by the Common Methodology and the Scheme.

An evaluator working for an ITSEF requests all necessary evaluation evidence from the Sponsor or the Developer. The evaluator also may request other support, such as training by the Developer, or clarifications or advice from the certifier assigned to the evaluation by the Certification Body.

The evaluator produces the evaluation reports that are submitted to the Certification Body, such as single evaluation reports (SER) and final evaluation report (FER).

An ITSEF must:

- observe all rules of the Scheme as laid down in the Scheme documentation and interpreted by the Certification Body
Swedish Certification Body for IT Security
001 Certification and Evaluation Scheme - Scheme Overview

- be accredited by an authorised accreditation body, in accordance with ISO/IEC 17025 (formerly, ISO Guide 25) or be directly appointed by the government
- ensure that the status of each of its individual evaluators is recognised by the Certification Body
- keep the Certification Body informed about the progress of ongoing evaluations and about any changes that might influence its ability to fulfil the requirements of the Scheme

The ITSEF is subject to supervision by both the Certification Body and the accreditation body as appropriate to ensure that it meets its obligations.

The Certification Body provides independent confirmation of the validity of evaluation results by overseeing the evaluation process. This oversight is performed by certifiers working for the Certification Body.

The certifier oversees an evaluation by reviewing the single evaluation reports and the final evaluation reports produced by the evaluator, by witnessing the evaluator's site visits, and by witnessing the testing of the product. The results are documented as technical oversight reports (TOR). The certifier also may provide support to the evaluator regarding Scheme matters, interpretations of the Common Criteria, etc.

To ensure uniform application of the Common Criteria, the Certification Body itself is being reviewed and audited according to the rules and regulations for accreditation as well as according to the regulations for applicable arrangements on mutual recognition of Common Criteria certificates. The use of interpretations to document clarifying statements made by the Certification Body is aimed at ensuring consistent and uniform use of the Common Criteria and the Scheme rules.

A more extensive presentation of the responsibilities of the Certification Body is found in the following Scheme publications:

- SP-002 Evaluation and Certification
- SP-003 Certificate Maintenance
- SP-004 Licensing of Evaluation Facilities
- SP-007 Quality Manual.
5 Processes within the Scheme

5.1 Management of Confidential Information

5.1.1 Legal Protection of Confidential Information

Documents received or drawn up by the Certification Body are official documents ("allmän handling") and may be kept secret by the Certification Body only when it is required to protect the interests covered by articles in The Swedish Law on Publicity and Secrecy regarding:

- the security of the realm or its relationships with another state or international organisation
- inspection, control, or other supervisory activities of a public authority
- the prevention or prosecution of crime
- the economic interests of the public institutions
- the protection of the personal or economic circumstances of private subjects

When a request is made by a third party for access to an official document, the Certification Body judges whether the information is confidential given the conditions at that time.

Information deemed confidential according to the act SHALL be kept secret, while information not covered SHALL be disclosed to the requesting party in accordance with The Freedom of Press act.

Before exchanging confidential information with the Certification Body, the information owner MAY seek advice from the Certification Body on the applicability of Swedish Law on the information.

If the identity of a party (sponsor, developer etc) are to be treated as confidential this SHALL be noted to the Certification Body prior any post are being sent.

More information on legal protection of confidential information is described in SP-007 Quality Manual.

5.1.2 Protective Marking of Confidential Information

Originators of information SHALL make the Certification Body aware of any confidentiality claims regarding information that is shared with the Certification Body:

- Documents with confidentiality claims regarding the entire document or parts thereof SHALL bear protective marks indicating that the information should be regarded as confidential.
- The originator is to clarify their claims on confidentiality to the Certification Body by presenting a justification describing the parts of the document covered by the security claims. A brief statement outlining the nature of the damage, which would result from disclosure, can be added.
- The applicable articles in The Swedish Law on Publicity and Secrecy MAY be added to the statement to help the Certification Body in forming its judgement when applying a security classification.

If the identity of a party (sponsor, developer etc) is to be treated as confidential this SHALL be clarified with the Certification Body before any correspondence commence.
5.1.3 Sending Confidential Information by Mail

Documents containing confidential information sent via standard post ("A-post") SHOULD be sent using two enclosed envelopes:

- The outer envelope SHOULD carry the address of the Certification Body and MAY have the name of the addressee (Certification Body Point-of-Contact) on top of the address.
- The inner envelope SHOULD bear a protective mark indicating that the information should be regarded as confidential, carry the address of the Certification Body and have the name of the addressee on top of the address.

```
<Name of the addressee>
Swedish Certification Body for IT Security
FMV/CSEC
SE-115 88 Stockholm, Sweden
```

5.1.4 Electronic Transmission of Confidential Information

Any use of electronic transmission of confidential information SHALL be agreed with the Certification Body before any correspondence commence.

5.2 Certification Agreement

According to the rules and regulations for accreditation the Certification Body SHALL have a legally enforceable Agreement for the provision of certification activities to its clients.

This Agreement is established in the following way:

1. The Sponsor signs and submits an Application for Certification to the Certification Body, and thereby accepts to comply with the clients responsibilities, as defined in SP-002 Evaluation and Certification.
2. The Certification Body decides, depending on complexity of the product to be certified and the Evaluation Assurance Level, the fees for the certification and sends a Tender to the Sponsor.
3. The Sponsor sends an acceptance of the fee and the terms of the Tender, in writing, to the Certification Body.

These three documents together form the Certification Agreement.

5.3 Evaluation and Certification Process

The IT security evaluation is the process of assessing a protection profile or target of evaluation against defined criteria.

Within the Scheme, the criteria used for evaluations are those of the Common Criteria and the Common Methodology, supplemented by additional requirements and specialisations in the Scheme's procedures for evaluation and certification.

Certification is the formal approval of a protection profile or target of evaluation based on the result of the evaluation and the oversight carried out by the Certification Body.

Every completed certification will result in a certification report; for successful certifications, a certificate will be issued for the IT product or protection profile.

The evaluation and certification process consists of three phases explained below:

1. Start-of-evaluation
2. Conduct of evaluation
3. Conclusion of evaluation

There are several types of evaluations: An evaluation is for products or protection profiles that have not been evaluated before. A re-evaluation may be conducted when another version of an already-certified product shall be evaluated. This may be the case for a new version of an IT product with modified functionality, a revised intended environment, or for additional platforms.

Evaluations may be carried out on a target of evaluation that has already been finished, or in parallel with target of evaluation development (i.e., concurrent evaluation).

The detailed evaluation and certification process is described in Scheme publication SP-002 Evaluation and Certification.

5.3.1 Start-of-evaluation

Start-of-evaluation begins with the Sponsor approaching an ITSEF to initiate the evaluation of a protection profile or IT product. The Sponsor provides the evaluator with the protection profile or security target, and possibly other evaluation evidence, so that the evaluator may conduct a feasibility study on this evidence to determine the likelihood of a successful evaluation, as well as to scope out and cost the evaluation.

If the Sponsor decides to seek certification of the protection profile or IT product, the Sponsor contracts with an ITSEF to perform the evaluation and applies for certification with the Certification Body.

The Sponsor submits a signed application to the Certification Body.

Together with the application the Sponsor submits the protection profile or security target, and the proposed evaluation work plan (EWP) containing the schedule and milestones of the evaluation to the Certification Body.

In the case of a re-evaluation, the Sponsor must also provide a re-evaluation impact analysis (RIA) detailing the changes in the target of evaluation since the previous evaluation and identifying the impact of these changes on the evaluation process.

The Certification Body performs an Application review after which it decides whether to undertake, or decline, the Certification.

During start-of-evaluation, the Developer/Sponsor carries out a number of activities to prepare for evaluation. The certification application and other necessary documents must be created. Start-of-evaluation tasks may be handled by the Sponsor/Developer alone, or may include independent pre-evaluation consultancy.

Pre-evaluation consultancy may be provided by the ITSEF performing the evaluation only if a possible conflict of interest is prevented by proper separation of evaluation and consultancy work.

5.3.2 Conduct of Evaluation

After the Certification Body has approved the application, the evaluation may start. The evaluators will carry out the evaluation in accordance with the agreed evaluation work plan. Usually the evaluator begins with evaluation of the security target and then performs the evaluator actions as described in the Common Methodology for the targeted evaluation assurance level, i.e., investigating the target of evaluation, the development environment, etc. The findings are reported in single evaluation reports submitted to the Certification Body for review. The format and required content of the reports is described in Scheme publication SP-002 Evaluation and Certification.

During the whole process, the Certification Body oversees the evaluation, supports the evaluation as requested by the evaluator, and responds to each evaluation report with a technical oversight report.
5.3.3 Conclusion of Evaluation

After the evaluators have assessed all necessary topics and the Certification Body has reviewed all single evaluation reports, a final evaluation report summarising all the findings is submitted to the Certification Body. The Certification Body assesses the final evaluation report, writes the certification report, and issues the certificate to the Sponsor. The certification report and the certificate itself will be issued in English, but can be issued in Swedish upon the Sponsor’s request.

This phase also involves publishing the evaluation results as agreed with the Sponsor and, in accordance with the requirements for mutual recognition.

5.3.4 Cost of Evaluation and Certification

The total cost of evaluation and certification includes:

- The Developer's and Sponsor's internal costs for the preparation and conduct of the evaluation, including document updates, bug fixes, additional testing, etc.
- The evaluation cost, covering the ITSEF's work.
- The certification cost, covering the Certification Body’s work.

The internal costs to the Sponsor and the Developer may be substantial and should be taken into account; however, discussion of those costs is outside the scope of this document. The cost for the ITSEF’s work will be agreed between the Sponsor and the ITSEF, but should be free from undue conditions that may impact the ITSEF's impartiality.

The Certification Body's charges and fees for certification, including Application Fee and Certification Fee, are described in Scheme publication SP-008 Charges and Fees.

5.3.5 Official Languages of the Scheme

Evaluation reports, oversight reports, and certification reports may be written in Swedish or English. Other languages may be used in evaluation evidence and other documentation related to the certification, but must be made available in either Swedish or English if required by the Certification Body.

5.4 Certificate Maintenance

If a certified product or its intended environment is changed, without affecting the assurance in the product, the validity of the certificate may be extended to incorporate the changed version of the product. To do this, a maintenance impact analysis report and a maintenance application has to be submitted to the Certification Body. If the Certification Body accepts to extend the certificate validity, a maintenance addendum, including a maintenance report will be published in the certified products list on the CSEC website. If the certificate cannot be extended, a re-evaluation re-using previous evaluation results or a new full certification may be performed. The procedures for certificate maintenance are described in detail in SP-003 Certificate Maintenance.

5.5 Certificate Misuse

The Certification Body will perform surveillance to ensure that the use of certificates, trademarks, and claims is compliant with the Scheme and does not bring the Scheme or its symbols into disrepute.
5.6 Licensing of Evaluation Facilities

Licensing of evaluation facilities is the formal process whereby the Certification Body grants an Evaluation Facility the right to conduct Common Criteria evaluations under the Scheme, thus becoming a licensed ITSEF. Before the Certification Body issues a license, the ITSEF must be accredited by a recognised accreditation body as a test laboratory according to ISO/IEC 17025. This whole process guarantees that the evaluators of an ITSEF will carry out impartial, objective, repeatable, and reproducible evaluations. Developers and Sponsors will then be able to trust the ITSEF to provide professional work and effective results.

Within the scope of mutual recognition according to CCRA, an ITSEF may conduct evaluations at every evaluation assurance level accepted for mutual recognition by CCRA and on every topic.

Within the scope of the SOGIS-MRA, CSEC will adapt to regulations issued within this MRA.

Within the scope of the EA MLA, CSEC will adapt to regulations issued by SWEDAC.

The Scheme leaves differentiation of ITSEF skills to market forces and assumes that Sponsors will select appropriate ITSEFs to perform evaluations. A list of ITSEFs will be available from the Certification Body.

Prior to each evaluation, the ITSEF must demonstrate to the Certification Body that the resources assigned to the project have appropriate skills and background to complete the evaluation.

Thus, before the evaluation starts, the Certification Body will assess the combined skills of the evaluation team in relation to the evaluation and may require that the staffing is justified by the ITSEF.

The details of the ITSEF licensing process are described in Scheme publication SP-004 Licensing of Evaluation Facilities.

5.7 Mutual Recognition and International Liaison

Mutual recognition and international liaison refers to the international framework for acceptance of IT security certificates among nations, the requirements to meet in this context, and the international efforts to develop the standard and methodology for IT security evaluation.

CSEC has been assigned by the Swedish government to operate the Swedish Common Criteria Evaluation and Certification Scheme in compliance with the CCRA, and to participate in the international cooperation in the field.

CSEC also represent Sweden in the in the European SOGIS-MRA collaboration and the Scheme is operated in accordance with the SOGIS-MRA.

5.8 CCRA

The mutual recognition, according to CCRA, of certificates issued within the Scheme is subject to certain requirements upon the Scheme itself, such as undergoing periodic assessment by other participants in the CCRA and complying with special restrictions for handling protected information shared between participants. Because there are requirements to make certificate reports, certificates, and other information publicly available for each recognised certificate, it must be agreed between the Sponsor, evaluator and certifier at the start of the certification whether mutual recognition is an objective of the certification.
The framework for mutual recognition within the CCRA, the procedures for voluntary periodic assessment (VPA), sharing of protected information, documenting interpretations, and for international liaison is further described in Scheme publication SP-007 Quality Manual.

5.9 SOGIS-MRA
CSEC is accepted as a Certification Body, up to EAL4, by the participants in the SOGIS-MRA. Mutual recognition is subject to regulations, as agreed by the nations collaborating within the SOGIS-MRA, similar to the CCRA.

5.10 EA MLA
CSEC is accredited by SWEDAC as a certification body for security in IT-products and is thus also able to perform certifications that may be recognised under the EA MLA.

The rules and regulations for accreditation and for mutual recognition according to the EA MLA are issued by SWEDAC. (See section 2.5.4 National Regulations)

5.11 Interpretations
An interpretation is a non-trivial clarification of the contents of the Common Criteria, the Common Methodology, or the Scheme procedures. Interpretations must be documented and taken into consideration when a similar clarification is made, to ensure consistency over time in the application of the evaluation criteria.

Interpretations related to the Common Criteria or the Common Methodology will be documented as national interpretations and may be forwarded to CC Maintainence Board to achieve international recognition through the CCRA.

Interpretations related to Scheme-specific procedures will result in Scheme Notes.

All interpretation matters will be presented to the Change Control Board for comment, before national interpretations or Scheme Notes are published. National interpretations will also be presented to the CCMB, which must accept the interpretations to be valid under mutual recognition. National interpretations are used by the CCMB as a source for future improvements of the Common Criteria and the Common Methodology.

Scheme Notes will be considered valid parts of the Scheme procedures until the corresponding changes have been made in the Scheme documents.

Interpretation issues will normally be raised by the Certification Body staff and have their origin in on-going evaluations, but all relevant issues brought to the attention of the Certification Body will be considered.

5.12 Complaints, Appeals and Disputes
The purpose of the procedures for management of complaints, appeals, and disputes is to provide means for resolving differences between the parties involved in the Scheme, and to provide a source of correction and improvement for the Scheme.

Disputes
Disputes between parties in the Scheme other than the Certification Body, e.g., disputes regarding contractual issues, are expected to be resolved among the parties themselves. However, if the dispute relates to compliance with Scheme regulations or to interpretations of the evaluation standard or methodology, the relevant Scheme procedures will be applied.

Disputes involving the Certification Body will be handled as complaints.
Complaints
The Certification Body will document and investigate any complaint directed towards it. The Certification Body is responsible for investigating all complaints in order to identify possible nonconformities to Scheme regulations. Any nonconformity found will be subject to the procedures for handling of nonconformities.

Appeals
A decision made by the Certification Body may be appealed within thirty days of the original decision. The appeal shall be sent to the Certification Body, where the matter will be reconsidered.

An appeal shall be made in writing and shall contain the name, address, and telephone number of the appellant. It shall identify and describe the requested changes to the decision that is being appealed.

Contact information for the Certification Body and forms for complaints and appeals will be found on the CSEC web site, www.csec.se. Use of these forms is recommended, but not mandatory.
Appendix A

A.1 References

These references are common to all public Scheme documents.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC</td>
<td>Common Criteria for Information Technology Security Evaluation</td>
</tr>
<tr>
<td>CCRA</td>
<td>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000</td>
</tr>
<tr>
<td>CEM</td>
<td>Common Methodology for Information Technology Security Evaluation</td>
</tr>
<tr>
<td>ISO/IEC 17065</td>
<td>Conformity assessment — Requirements for bodies certifying products, processes and services. The most recent version is ISO/IEC 17065:2012.</td>
</tr>
<tr>
<td>SP-001</td>
<td>Scheme Overview</td>
</tr>
<tr>
<td>SP-002</td>
<td>Evaluation and Certification</td>
</tr>
<tr>
<td>SP-003</td>
<td>Certificate Maintenance</td>
</tr>
<tr>
<td>SP-004</td>
<td>Licensing of Evaluation Facilities</td>
</tr>
<tr>
<td>SP-007</td>
<td>Quality Manual</td>
</tr>
<tr>
<td>SP-008</td>
<td>Charges and Fees</td>
</tr>
<tr>
<td>SP-070</td>
<td>Conditions for the Use of Trademarks</td>
</tr>
<tr>
<td>SP-084</td>
<td>Sponsor's and Developer's Guide to the Evaluation and Certification Process</td>
</tr>
<tr>
<td>ISO/IEC 17025</td>
<td>General requirements for the competence of testing and calibration laboratories. The most recent version is ISO/IEC 17025:2005</td>
</tr>
<tr>
<td>STAFS 2010:10</td>
<td>Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om ackreditering</td>
</tr>
<tr>
<td>STAFS 2013:15</td>
<td>Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om ackreditering av organ som certifierar produkter</td>
</tr>
<tr>
<td>STAFS 2007:20</td>
<td>Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om evalueringsorganisationer som utvärderar IT-säkerhet</td>
</tr>
<tr>
<td>STAFS 2007:21</td>
<td>Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om organ som certifierar IT-säkerhet;</td>
</tr>
</tbody>
</table>

A.2 Abbreviations

The following abbreviations are used in this document and other CSEC documents.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CB</td>
<td>Certification Body</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria (CC Part 1-3 refers to the Common Criteria standard documentation)</td>
</tr>
<tr>
<td>CCMB</td>
<td>Common Criteria Maintenance Board</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CCRA</td>
<td>Common Criteria Recognition Arrangement</td>
</tr>
<tr>
<td>CEM</td>
<td>Common Methodology for Information Technology Security Evaluation</td>
</tr>
<tr>
<td>CM</td>
<td>configuration management</td>
</tr>
<tr>
<td>COTS</td>
<td>commercial off-the-shelf</td>
</tr>
<tr>
<td>CR</td>
<td>certification report</td>
</tr>
<tr>
<td>EAL</td>
<td>evaluation assurance level</td>
</tr>
<tr>
<td>EN</td>
<td>European Norm</td>
</tr>
<tr>
<td>EWP</td>
<td>evaluation work plan</td>
</tr>
<tr>
<td>FER</td>
<td>final evaluation report</td>
</tr>
<tr>
<td>FMV</td>
<td>Försvarets Materielverk - The Swedish Defence Material Administration</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>MIA</td>
<td>maintenance impact analysis</td>
</tr>
<tr>
<td>RIA</td>
<td>re-evaluation impact analysis</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardisation</td>
</tr>
<tr>
<td>IT</td>
<td>information technology</td>
</tr>
<tr>
<td>ITSEF</td>
<td>IT Security Evaluation Facility</td>
</tr>
<tr>
<td>OR</td>
<td>observation report</td>
</tr>
<tr>
<td>PP</td>
<td>protection profile</td>
</tr>
<tr>
<td>SAC</td>
<td>Scheme Advisory Committee</td>
</tr>
<tr>
<td>SER</td>
<td>single evaluation report</td>
</tr>
<tr>
<td>SOGIS-MRA</td>
<td>Senior Officials Group Information Systems Security - Mutual Recognition Agreement</td>
</tr>
<tr>
<td>ST</td>
<td>security target</td>
</tr>
<tr>
<td>TOE</td>
<td>target of evaluation</td>
</tr>
<tr>
<td>TOR</td>
<td>technical oversight report</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Functions</td>
</tr>
<tr>
<td>TSFI</td>
<td>TOE Security Functional Interface</td>
</tr>
<tr>
<td>TSP</td>
<td>TOE Security Policy</td>
</tr>
</tbody>
</table>
## A.3 Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concurrent evaluation</td>
<td>An evaluation of a TOE that is in development.</td>
</tr>
<tr>
<td>Protection profile</td>
<td>An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs. [CC]</td>
</tr>
<tr>
<td>Security target</td>
<td>A set of security requirements and specifications to be used as the basis for evaluation of an identified target of evaluation. [CC]</td>
</tr>
<tr>
<td>Target of evaluation</td>
<td>A set of software, firmware and/or hardware possibly accompanied by guidance. [CC]</td>
</tr>
</tbody>
</table>