CSEC

Swedish Certification Body for IT Security

001 Certification and Evaluation Scheme - Scheme Overview

Issue: 28.0, 2019-Sep-24

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Preface

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

2 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.

3 The Scheme documents and further information can be obtained from the Swedish Certification Body for IT Security. Complete contact information is provided in the following box.

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: SE-115 88 Stockholm, Sweden
Visiting address: Banérgatan 62

Telephone: +46-8-782 4000 E-mail: csec@fmv.se
Web: www.csec.se

1.1 Purpose

4 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.

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

1.2 Terminology

6 Abbreviations commonly used by the Swedish Certification Body for IT Security (CSEC) in Scheme Publications (SP) are for all SP-documents described in Appendix 2 in this document, SP-001 *Certification and Evaluation - Scheme Overview.*

7 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

8 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.

9 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.

10 The Common Criteria (CC) establishes an international standard (ISO/IEC 15408) that addresses these needs. The CC 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.

11 CC certification is internationally recognised through multilateral recognition arrangements; a CC 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 CC 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.

12 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 CC certificates issued, under these agreements, in other countries.

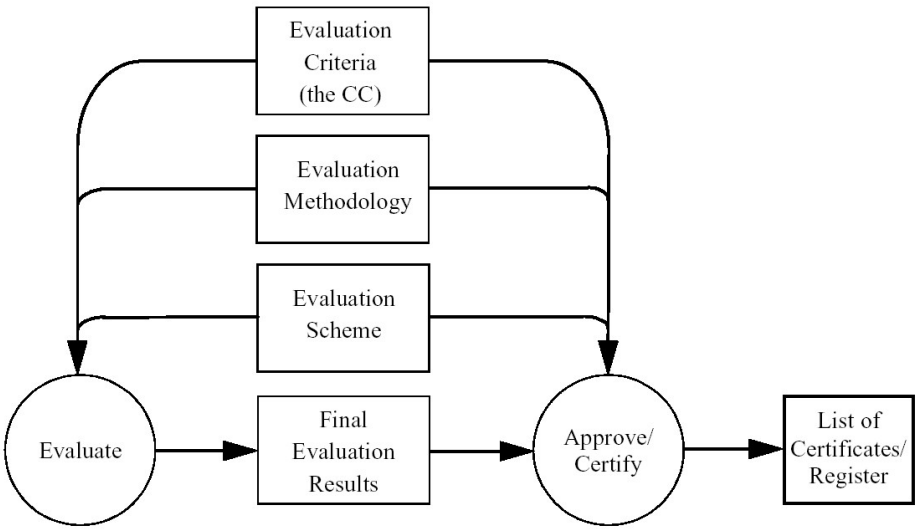
13 Sweden is also a member of the European co-operation for Accreditation (EA). This agreement means that a test or inspection report or a certificate issued by an accredited body in one country is recognised as equivalent to a report or a certificate issued by an accredited body in any of the countries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

14 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 CC certificates is established in Sweden (see Figure 1). The Swedish Defence Materiel Administration (FMV), has been appointed[1] 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.

15 CSEC is the owner (Scheme Owner) of the Swedish Common Criteria Evaluation and Certification Scheme.

[1] Ordinance with instructions for the Swedish Defence Materiel Administration (SFS 2007:854); see also section 2.5 Relevant Legislation, Standards and Regulations

Figure 1 – Evaluation Context



2.2 Objectives of the Scheme

16 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.

17 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 evaluations 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.
- High and consistent standard
  Evaluations performed to high and consistent standard will promote confidence in the security of IT products certified under this Scheme

2.3 Brief Description of the Scheme

18 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.

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

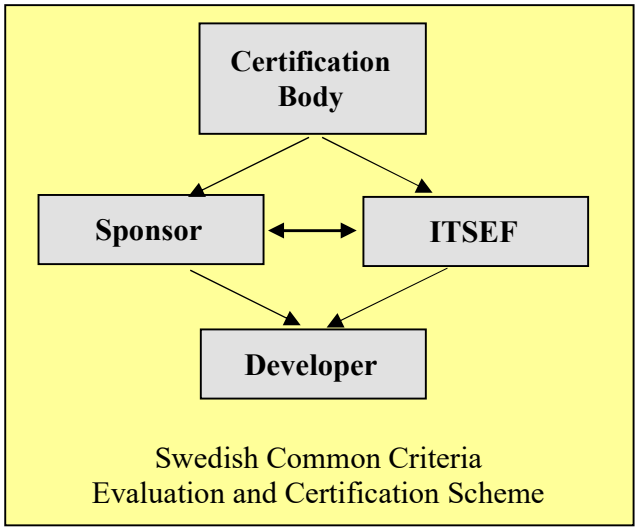
20 Certification is the process carried out by the Certification Body leading to the issuing of a CC certificate. The certificate is a public document issued by the Certification Body which confirms that a specific IT product or protection profile has successfully completed evaluation by an ITSEF. A CC certificate always has a certification report (CR) associated with it.

21 The process of evaluation and certification involves the following parties with specific responsibilities, which are detailed in section 4, *Roles within the Scheme*.

- Sponsor
- Developer
- ITSEF
- Certification Body

22 This leads to the structure depicted in Figure 2 of the different organisations currently involved in the Scheme.

Figure 2 – Organisational Structure of the Scheme



23 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.

24 Additional processes and procedures are:

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

25 These processes are explained in section 5, *Processes within the Scheme*, and detailed in additional documents (see section 2.7, *Documentation*).

2.4 Mutual Recognition

26 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 are recognised, under the conditions of the arrangement, by all participants of CCRA.
- The European cooperation for accreditation multilateral agreement (EA MLA)
  Certification bodies accredited by an approved accreditation body within the EA may issue certificates that are 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.

27 A certification performed by the Swedish Certification Body for IT Security (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.

28 A customer who applies for certification will be able to choose which mutual recognition agreements the certification should be covered by.

2.4.1 Certificates issued by CSEC

CSEC can issue the following certificates:

- EA MLA: Certificates with claims of compliance against any of the Common Criteria Evaluation Assurance Level 1 through 7[2] and assurance life-cycle support flaw remediation (ALC_FLR).

[2] Certifications above EAL4 is conditioned that there exist evaluation methodology for the concerned product type which has been approved by CSEC and that the ITSEF in question demonstrate their competence and procedures for such evaluations.

- CCRA: Certificates with claims of compliance against Common Criteria assurance components of either:
  - a collaborative protection profile (cPP), developed and maintained in accordance with CCRA Annex K, with assurance activities selected from Evaluation Assurance Levels up to and including level 4 and ALC_FLR, developed through an International Technical Community endorsed by the CCRA Management Committee; or
  - Evaluation Assurance Levels 1 through 2 and ALC_FLR.2.
- SOGIS-MRA: Certificates with claims of compliance against any of the Common Criteria Evaluation Assurance Level 1 through 4.
- National Certificate: Certificates not subject for any of above mutual recognition arrangements and with claims of compliance against any of the Common Criteria Evaluation Assurance Level 1 through 7[3] and ALC_FLR.

29 All certificates are issued separately.

2.5 Relevant Legislation, Standards and Regulations

2.5.1 Government Ordinance

30 In the *Ordinance with instructions for the Swedish Defence Materiel Administration* (SFS 2007:854) the Swedish government has stated that at the 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.

31 In the *Ordinance with instructions for the Swedish Defence Materiel Administration* CSEC has been appointed by the Swedish government to issue regulations for certification and to certify electronic identification and trust services for electronic transactions in the EU internal market, referred to as eIDAS (Swedish: "utländska e-legitimationer i svenska digitala tjänster"). In the complementary law (SFS 2016:561) to the EU regulation (No 910/2014 of 23 July 2014) on electronic identification and trust services for electronic transactions in the internal market the Swedish government or an authority appointed by the Swedish government may issue the regulations above.

2.5.2 Appropriation Directions

32 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 for 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 CC for requirements specification.

33 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

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

[3] Certifications above EAL4 is conditioned that there exist evaluation methodology for the concerned product type which has been approved by CSEC and that the ITSEF in question demonstrate their competence and procedures for such evaluations.

Common Criteria (CC)

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

ISO/IEC 15408

36 ISO/IEC-versions of the CC standards

ISO/IEC 18045

37 ISO/IEC-version of the Common Evaluation Methodology

ISO/IEC 17065

38 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-MRA, and the Swedish Board for Accreditation and Conformity Assessment (Swedac), to ensure the quality of certifications.

ISO/IEC 17025

39 For an ITSEF, ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* (earlier known as ISO/IEC Guide 25) applies according to the regulations of the CCRA, SOGIS-MRA and Swedac, to ensure the quality of evaluations.

2.5.4 National Regulations - STAFS

40 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 2015:8

Regulations and guidelines for accreditation

Swedac STAFS 2013:5

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

41 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

42 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

43 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

44 Defines the processes and requirements for CC 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 Assurance Continuity

45 Defines the concept of Assurance Continuity within the Scheme, referring to detailed process descriptions in other documents.

SP-004 Licensing of Evaluation Facilities

46 This document 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

47 This document 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.

48 This set of documents may be supplemented by documents addressing specific topics. For example, if evaluation of products at evaluation assurance levels (EAL) above 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

49 A protection profile is an implementation-independent set of security requirements for a category of IT products that meet specific customer needs.

50 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).

51 A protection profile is evaluated in accordance with the requirements for protection profile evaluation contained in the CC. 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

52 The target of evaluation (TOE) consists of an entire IT product or parts of an IT product selected for CC 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.

53 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.

54 The target of evaluation is evaluated in accordance with requirements contained in the CC. 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 target of evaluation 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.

4 Roles within the Scheme

55 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

56 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.

57 The obligations of the Sponsor in an evaluation are detailed in Scheme publication SP-002 *Evaluation and Certification*, section 3, *Parties and Responsibilities*.

4.2 Developer

58 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.

59 The obligations of the Developer in an evaluation are detailed in Scheme publication SP-002 *Evaluation and Certification*, section 3, *Parties and Responsibilities*.

4.3 IT Security Evaluation Facility (ITSEF)

60 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 CEM and the Scheme.

61 Further details of the obligations for ITSEFs and evaluators are found in Scheme publication SP-004 *Licensing of Evaluation Facilities*, section 3, *Parties and Responsibilities*.

4.4 Certification Body

62 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.

63 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 *Assurance Continuity*
- 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

64 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 following.

- 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

65 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.

66 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*.

67 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.

68 If the identity of a party (sponsor, developer etc) is to be treated as confidential this SHALL be noted to the Certification Body prior to any correspondence commencing.

69 The confidentiality requirements between the ITSEF, Sponsors, and Developers SHOULD be defined in detail in agreements between the parties.

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

5.1.2 Protective Marking of Confidential Information

71 Originators of information SHALL make the Certification Body aware of any confidentiality claims regarding information that is shared with the Certification Body as follows.

- 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.

72 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 commences.

5.1.3 Sending Confidential Information by Mail

73 Documents containing confidential information sent via standard post ("A-post") SHOULD be sent using two enclosed envelopes as follows.

- 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 as follows.

<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

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

5.2 Certification Agreement

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

76 This Agreement is established as follows.

1. The Sponsor signs and submits an Application for Certification to the Certification Body, and thereby accepts compliance 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 EAL, 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.

77 These three documents together form the Certification Agreement.

5.3 Evaluation and Certification Process

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

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

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

81 The evaluation and certification process consists of three phases as follows.

1. Start-of-evaluation The four parties involved in the evaluation and certi-

	fication (Developer, Sponsor, ITSEF, and Certification Body) prepare for evaluation.
2. Conduct of evaluation	The evaluation is performed.
3. Conclusion of evaluation	The evaluation is completed.

82 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.

83 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).

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

5.3.1 Cost of Evaluation and Certification

85 The total cost of evaluation and certification includes the following.

- 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

86 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.

87 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*.

5.3.2 Official Languages of the Scheme

88 Evaluation reports, oversight reports, and certification reports may be written in Swedish or English.

89 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 Validity within the CCRA and SOGIS-MRA

90 Effective 1 June 2019, the validity of Common Criteria Certificates mutually recognised within the CCRA and SOGIS-MRA will be limited over time.

91 The details of this policy may be found in the *Procedure for Certificate Validity* that may be obtained from the CCRA portal (www.commoncriteriaportal.org).

5.4.1 Valid certificates

92 Valid certificates will be published on the Certified Products List (CPL) on the CCRA portal and on the list of valid certificates at the CSEC website.

5.4.2 Expired certificates

93 Certificates with an expired validity period will be moved to an Archive list on the CCRA portal and on the list of Archived certificates at the CSEC website.

5.4.3 Surveillance/reassessment

94 The process of surveillance/reassessment allows for extending the administrative validity of a certificate.

5.5 Certificate Maintenance

95 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 have to be submitted to the Certification Body. If the Certification Body accepts extension of 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-002 *Evaluation and Certification*.

5.6 Certificate Misuse

96 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.

5.7 Licensing of Evaluation Facilities

97 Licensing of evaluation facilities is the formal process whereby the Certification Body grants an Evaluation Facility the right to conduct CC 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.

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

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

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

101 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.

102 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.

103 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.

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

5.8 Mutual Recognition and International Liaison

105 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.

106 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.

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

5.9 CCRA

108 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.

109 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.*

5.10 SOGIS-MRA

110 CSEC is accepted as a Certification Body, up to EAL 4, 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.

5.11 EA MLA

111 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.

112 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*).

5.12 Interpretations

113 An interpretation is a non-trivial clarification of the contents of the CC, the CEM, 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.

114 Interpretations related to the CC or the CEM will be documented as national interpretations and may be forwarded to CCIMB to achieve international recognition through the CCRA.

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

116 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 CCIMB, which must accept the interpretations to be valid under mutual recognition. National interpretations are used by the CCIMB as a source for future improvements of the CC and the CEM. Scheme Notes will be considered valid parts of the Scheme procedures until the corresponding changes have been made in the Scheme documents.

117 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.

5.13 Complaints and Appeals

118 The purpose of the procedures for management of complaints and appeals is to ensure that:

- the Certification Body has suitable policies and procedures for the resolution of complaints and appeals,
- details of the procedures for handling complaints and appeals are documented and published according to applicable standards,
- the Certification Body has procedures to correct decisions that are not made according to the rules of the Scheme, and
- the Certification Body has procedures to learn from any complaints or appeals and to update the Scheme accordingly.

Complaints

119 The Certification Body will document and investigate any complaint directed towards it that applies to the certification activities for which it is responsible.

120 The Certification Body is responsible for investigating all such complaints in order to identify possible nonconformities to Scheme regulations. Any nonconformity found will be subject to the procedures for handling of nonconformities.

121 The procedures for handling Complaints are described in SP-007 *Quality Manual*.

Appeals

122 A complainant that is not satisfied with a decision, or with the outcome of a complaint, that applies to the certification activities for which the Certification Body is responsible, may file an appeal.

123 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.

124 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.

125 The procedures for handling Appeals are described in SP-007 *Quality Manual*.

Appendix A

A.1 References

These references are common to all public Scheme documents.

Reference	Description
CC	Common Criteria for Information Technology Security Evaluation
CC Part 1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
CC Part 2	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements
CC Part 3	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014
CEM	Common Methodology for Information Technology Security Evaluation
ISO/IEC 17065	Conformity assessment — Requirements for bodies certifying products, processes and services. The most recent version is ISO/IEC 17065:2012.
SP-001	Scheme Overview
SP-002	Evaluation and Certification
SP-003	Assurance Continuity
SP-004	Licensing of Evaluation Facilities
SP-007	Quality Manual
SP-008	Charges and Fees
SP-070	Conditions for the Use of Trademarks
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories. The most recent version is ISO/IEC 17025:2005
STAFS 2015:8	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om ackreditering
STAFS 2013:15	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om ackreditering av organ som certifierar produkter
STAFS 2007:20	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om evalueringsorganisationer som utvärderar IT-säkerhet
STAFS 2007:21	Styrelsens för ackreditering och teknisk kontroll (Swedac) föreskrifter och allmänna råd om organ som certifierar IT-säkerhet;

A.2 Abbreviations

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

Abbreviation	Description
CC	Common Criteria (CC Part 1-3 refers to the Common Criteria standard documentation)
CCIMB	Common Criteria Interpretations Maintenance Board
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for Information Technology Security Evaluation
CSEC	Swedish Certification Body for IT Security
CV	Curriculum Vitae
EAL	evaluation assurance level
EWP	evaluation work plan
FER	final evaluation report
FMV	Försvarets Materielverk - The Swedish Defence Materiel Administration
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	information technology
ITSEF	IT Security Evaluation Facility
OR	observation report
cPP	collaborative protection profile
PP	protection profile
SAC	Scheme Advisory Committee
SER	single evaluation report
SN	Scheme Note
SOGIS	Senior Officials Group Information Systems Security
SOGIS-MRA	Senior Officials Group Information Systems Security - Mutual Recognition Agreement
SP	Scheme Publication
ST	security target
Swedac	Swedish Board for Accreditation and Conformity Assessment
TOE	target of evaluation
TOR	technical oversight report
TSF	TOE Security Functions
TSFI	TOE Security Functional Interface
TSP	TOE Security Policy

A.3 Glossary

Glossary

Concurrent evaluation	An evaluation of a target of evaluation (TOE) that is in development.
Cross frontier evaluation	An evaluation where work is performed in locations situated outside Sweden.
Initial evaluation	An evaluation of a target of evaluation or a protection profile (PP) that has not previously been evaluated.
Protection profile	An implementation-independent set of security requirements for a category of targets of evaluation that meet specific consumer needs. [CC]
Re-evaluation	An evaluation of a new version of an already evaluated target of evaluation.
Security target	A set of security requirements and specifications to be used as the basis for evaluation of an identified target of evaluation. [CC]
Target of evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC]

A.4 Assurance Classes and Assurance Families used in CC

Assurance Class	Assurance Family	Description
Development	ADV_ARC	ADV_security architecture
	ADV_FSP	ADV_functional specification
	ADV_IMP	ADV_implementation representation
	ADV_INT	ADV_TSF internals
	ADV_SPM	ADV_security policy modelling
	ADV_TDS	ADV_TOE design
Guidance documents	AGD_OPE	AGD_operational user guidance
	AGD_PRE	AGD_preperative procedures
Life-cycle support	ALC_CMC	ALC_CM capabilities
	ALC_CMS	ALC_CM scope
	ALC_DEL	ALC_delivery
	ALC_DVS	ALC_development security
	ALC_FLR	ALC_flaw remidation
	ALC_LCD	ALC_life-cycle definition
	ALC_TAT	ALC_tools and techniques
Security Target evaluation	ASE_CCL	ASE_conformance claims
	ASE_ECD	ASE_extended components definition

Assurance Class	Assurance Family	Description
	ASE_INT	ASE_ST introduction
	ASE_OBJ	ASE_security objectives
	ASE_REQ	ASE_security requirements
	ASE_SPD	ASE_security problem definition
	ASE_TSS	ASE_TOE summary specification
Tests	ATE_COV	ATE_coverage
	ATE_DPT	ATE_depth
	ATE_FUN	ATE_functional tests
	ATE_IND	ATE_independent testing
Vulnerability assessment	AVA_VAN	AVA_vulnerability analysis
Composition	ACO_COR	ACO_composition rationale
	ACO_DEV	ACO_development evidence
	ACO_REL	ACO_reliance of dependent component
	ACO_CTT	ACO_composed testing
	ACO_VUL	ACO_composition vulnerability analysis

A.5 Security Functional Requirements (SFRs) Classes and Families

SFR Class	SFR Family	Description
Security audit	FAU_ARP	ARP_security audit automatic response
	FAU_GEN	GEN_security audit data generation
	FAU_SAA	SAA_security audit analysis
	FAU_SAR	SAR_security audit review
	FAU_SEL	SEL_security audit event selection
	FAU_STG	STG_Security audit event storage
Communication	FCO_NRO	NRO_non-repudiation of origin
	FCO_NRR	NRR_non-repudiation of receipt
Cryptographic support	FCS_CKM	CKM_cryptographic key management
	FCS_COP	COP_cryptographic operation
User data protection	FDP_ACC	ACC_access control policy
	FDP_ACF	ACF_access control functions
	FDP_DAU	DAU_data authentication
	FDP_ETC	ETC_export to outside TSF control
	FDP_IFC	IFC_information flow control policy

SFR Class	SFR Family	Description
	FDP_IFF	IFF_information flow control functions
	FDP_ITC	ITC_import from outside TSF control
	FDP_ITT	ITT_internal TOE transfer
	FDP_RIP	RIP_residual information protection
	FDP_ROL	ROL_rollback
	FDP_SDI	SDI_stored data integrity
	FDP_UCT	UCT_inter-TSF user data confidentiality transfer protection
	FDP_UIT	UIT_Inter-TSF user data integrity transfer protection
	FTP_TRP	TRP_trusted path
Identification and authentication	FIA_AFL	AFL_authentication failures
	FIA_ATD	ATD_user attribute definition
	FIA_SOS	SOS_specification of secrets
	FIA_UAU	UAU_user authentication
	FIA_UID	UID_user identification
	FIA_USB	USB_user-subject binding
Security management	FMT_MOF	MOF_management of functions in TSF
	FMT_MSA	MSA_management of security attributes
	FMT_MTD	MTD_management of TSF data
	FMT_REV	REV_revocation
	FMT_SAE	SAE_security attribute expiration
	FMT_SMR	SMR_security management role
Privacy	FPR_ANO	ANO_anonymity
	FPR_PSE	PSE_pseudonymity
	FPR_UNL	UNL_unlinkability
	FPR_UNO	UNO-unobservability
Protection of the TSF	FPT_AMT	AMT_underlying abstract machine test
	FPT_FLS	FLS_fail secure
	FPT_ITA	ITA_availability of exported TSF data
	FPT_ITC	ITC_confidentiality of exported TSF data
	FPT_ITI	ITI_integrity of exported TSF data
	FPT_ITT	ITT_internal TOE TSF data transfer
	FPT_PHP	PHP_TSF physical protection
	FPT_RCV	RCV_trusted recovery

SFR Class	SFR Family	Description
	FPT_RPL	RPL_replay detection
	FPT_RVM	RVM_reference mediation
	FPT_SEP	SEP_domain separation
	FPT_SSP	SSP_state synchrony protocol
	FPT_STM	STM_time stamps
	FPT_TDC	TDC_inter-TSF TSF data consistency
	FPT_TRC	TRC_internal TOE TSF data replication consistency
	FPT_TST	TST_TSF self test
Resource utilisation	FRU_FLT	FLT_fault tolerance
	FRU_PRS	PRS_priority of service
	FRU_RSA	RSA_resource allocation
TOE access	FTA_LSA	LSA_limitation on scope of selectable attributes
	FTA_MCS	MCS_limitation on multiple concurrent sessions
	FTA_SSL	SSL_session locking
	FTA_TAB	TAB_TOE access banners
	FTA_TAH	TAH_TOE access history
	FTA_TSE	TSE_TOE session establishment
Trusted path/channels	FTP_ITC	ITC_inter-TSF trusted channel