Swedish Certification Body for IT Security

002 Evaluation and Certification

Issue: 19.0, 2013-jun-17

Authorisation: Martin Bergling, Technical Manager , 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 here:

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 describes the evaluation and certification process performed under the Scheme. The document provides detailed information about the evaluation and certification process and the responsibilities of each party involved in the process.

5 General information about the Scheme is published in Scheme publication SP-001 *Certification and Evaluation Scheme - Scheme Overview*.

1.2 Typography

6 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

7 IT security evaluation is the process whereby an IT product or protection profile (PP) is assessed against a specific set of security requirement claims. IT security certification is the oversight of the evaluation process including the formal approval of the evaluation results by a Certification Body (CB). The objective of the evaluation and certification process is to perform an impartial, objective, and internationally standardised assessment of the IT product or protection profile, resulting in an internationally-recognised verdict of fulfilment on which users can base their trust.

8 The Certification Body will produce a certification report (CR) and issue a certificate after a successful certification.

9 Evaluations may be carried out on an IT product that has already been developed, or in parallel with the development. The latter model is known as concurrent evaluation. The IT product in both cases is known as the target of evaluation (TOE).

10 The Scheme supports both initial evaluations and re-evaluations. An initial evaluation (called simply an *evaluation*) is based on a target of evaluation or a protection profile that has not previously been evaluated, while a *re-evaluation* is based on an already evaluated and certified target of evaluation.

11 A re-evaluation may be applicable to a new version of an IT product with modified functionality, a revised intended environment, or for additional platforms.

12 In the discussion that follows, no distinction is made between a TOE evaluation and a protection profile evaluation, although certain evaluation aspects do not apply to protection profile evaluations as described by the Common Criteria (CC).

2.2 Principles of Evaluation

13 The principles on which the evaluation and certification process is based are: appropriateness, impartiality, objectivity, repeatability, reproducibility, generation of sound results, cost-effectiveness, and re-usability.

14 These are the principles of evaluation:

- All parties involved in an evaluation SHALL perform their required tasks to a degree of rigor consistent with the guidance and requirements of the target evaluation assurance level (EAL).
- No party involved in evaluation SHALL have a bias toward or against any target of evaluation or protection profile being evaluated. Proper technical oversight coupled with a Scheme that eliminates conflicts of interest SHOULD reduce to a nominal level any residual bias.
- Individuals cannot be totally free of opinion or judgements; therefore, proper technical oversight based on well-defined methodology and interpretations SHALL be used to reduce opinions and judgments to an acceptable level.
- The results of each evaluator action element SHOULD yield the same result regardless of who performs the evaluation, and requirements SHOULD be interpreted in a consistent manner across evaluations.
- Outputs of the evaluation process SHALL demonstrate good judgement and an accurate technical assessment of the target of evaluation or protection profile. The evaluation process and results SHOULD be subject to technical oversight to ensure that the requirements of the Common Criteria, the Common Methodology, and the Scheme are met.

- A balance SHOULD continually be maintained between value, and expenditure of time and resources in the evaluation of targets of evaluation and protection profiles.
- The results of evaluating a target of evaluation or protection profile, and the interpretations that arise in the course of the evaluation, SHOULD be useful in subsequent evaluations if the same conditions apply.

15 These principles are upheld by:

- using the Common Criteria, which provides a well-defined set of security requirements.
- using the Common Methodology when assessing an IT product or a protection profile against the requirements.
- implementing the evaluation and certification process defined by the Scheme.

2.3 Standard versions

16 The versions of the Common Criteria and the Common Methodology used in certifications by the Swedish Certification Body for IT Security (CSEC) are those listed on the Common Criteria project website, www.commoncriteriaportal.org.

17 Final decision about which version is used in a Certification, and thus is presented on the certificate and on the certification report, is made when the Certification Body takes the decision on certification.

18 Unless otherwise agreed with the sponsor the versions used should be the versions valid at the time of the Final Evaluation Report.

19 If the valid versions have been updated during the evaluation and certification an impact analysis may have to be performed and some part of the evaluation may have to be updated.

20 Should the impact be too extensive, the certification may also be based on older versions of the standards, as long as this is consistent with the recommendations made by the CCRA.

2.4 Evaluation and Certification Process

21 The generic evaluation process has three distinct phases:

start-of-evaluation	The four parties involved in the evaluation and certification (Developer, Sponsor, ITSEF, and Certification Body) prepare for evaluation.
conduct of evaluation	The evaluation is performed.
conclusion of evaluation	The evaluation is completed.

22 The start-of-evaluation phase includes any activities relevant to the upcoming evaluation. An application for certification includes several documents, which together demonstrate readiness for the evaluation and certification process. The application documentation submitted to the Certification Body is reviewed, and the Certification Body decides whether to accept or reject the application.

23 The conduct of evaluation phase starts after the Certification Body has approved the application, and a certification agreement has been signed between the Sponsor and the Certification Body. The Sponsor also contracts an IT Security Evaluation Facility (ITSEF) to perform the evaluation. Note that the Sponsor can be the same organisation as the Developer.

24 During the conduct of evaluation phase, the Developer submits evaluation evidence to the evaluator at the ITSEF. The evaluator uses the Common Methodology to assess the evidence, and requests necessary updates in the evaluation evidence from the developer, so that remaining issues with status FAIL or INCONCLUSIVE are avoided. Thereafter the evaluation approach and results are documented in a single evaluation reports (SER). The single evaluation reports are submitted to the certifier at the Certification Body, together with the Evaluation evidence. Copies of the single evaluation reports are distributed to the sponsor and to the developer.

25 The evaluation work is divided into several parts, resulting in a series of single evaluation reports.

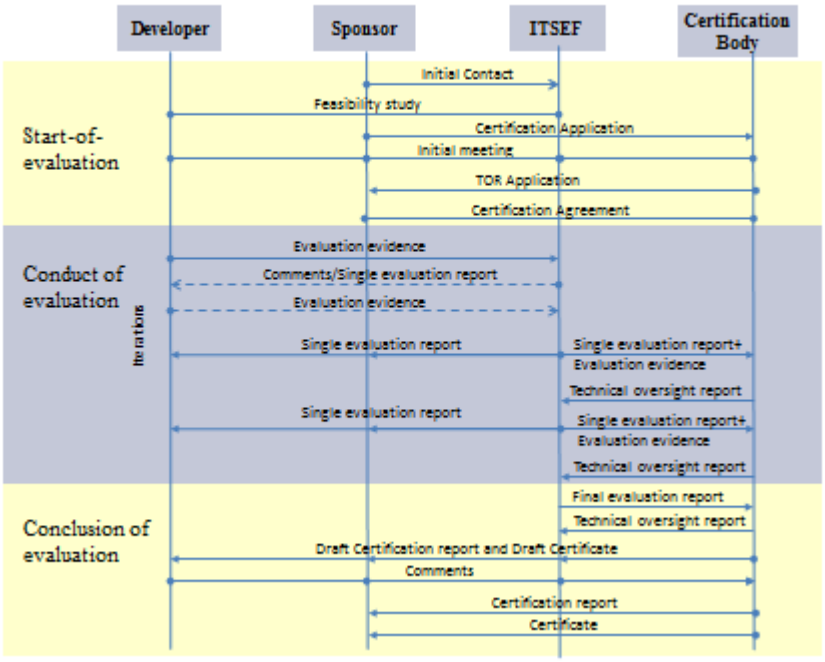
26 For each single evaluation report, the certifier will review the evaluator's approach and results, and document any findings in a technical oversight report (TOR), which is submitted to the ITSEF. The evaluator responds by updating the single evaluation report, preferably after the evaluation evidence has been updated, and submitting the changed documents to the certifier. The process may be iterated.

27 The conduct of evaluation phase also includes site visit activities. The evaluator and the certifier visit the Developer site to assess whether procedures are being followed in a manner consistent with that described in the documentation. The certifier may also be present during the evaluator's independent testing.

28 After all single evaluation reports have been produced by the evaluator and have been accepted by the Certification Body, the conclusion of evaluation phase begins. The evaluator produces a final evaluation report (FER), and the Certification Body produces and publishes a certification report and issues the certificate.

29 Figure 1 shows the four parties involved in the evaluation and certification process (Sponsor, Developer, ITSEF, and Certification Body), the phases of the process, and a simplified document delivery sequence. The parties and phases, as well as the documentation, are described in detail in the sections that follow.

Figure 1 – Visualisation of the Evaluation and Certification Process



30 The Certification Body also exercises control over the use of the certificates issued. This is described in Chapter 7.2, Certificate Misuse.

2.4.1 Official Languages of the Scheme

31 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.

2.5 Management of Confidential Information

32 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

33 For further details on legal protection of confidential information, how to make the Certification Body aware of confidentiality claims and procedures for exchanging confidential information with the Certification Body please contact the Certification Body.

3 Parties and Responsibilities

34 All parties involved in the evaluation and certification shall fulfil their roles and responsibilities as defined by the Common Criteria, the Common Methodology, and the Scheme. It is, therefore, important that all parties are aware of their responsibilities in the Scheme before the evaluation and certification starts.

3.1 Sponsor

35 The Sponsor is the organisation that funds the evaluation and certification, 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.

36 The Sponsor SHALL have formal agreements with:

- the ITSEF for the evaluation
- the Certification Body for the certification

37 The Sponsor SHALL assure that evaluation evidence, training, support, and access to facilities is provided to the evaluator. This MAY require an agreement with the Developer, as well.

38 In some instances, more than one Developer MAY be involved in an evaluation, for example, in cases where subcontractors are involved, 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.

39 The Sponsor SHALL ensure that the certifier is provided with evaluation reports, evaluation evidence, training, support, and access to facilities.

40 The Sponsor SHALL assign a point of contact for the evaluation and certification, which is the contact person to use for the other parties involved. This point of contact SHOULD be the recipient for all communication with the Sponsor within the scope of the evaluation and certification. This communication includes the certification agreement, invoices, and the certificate.

41 The Sponsor SHOULD assign a point of contact for external communication related to the evaluation and certification. The Certification Body will list this point of contact in publications with information about on-going and successful certifications (i.e., *the certified product list*, and the *certified protection profile list*). The Sponsor SHALL ensure that the Certification Body is notified of any changes to the point of contact.

42 Upon successful certification, the Sponsor is responsible for archiving a reference copy of the TOE as well as any and all evidence produced by the Sponsor or the Developer that has been used by the Evaluator or by the Certification Body to perform evaluation or certification activities.

43 The archived material SHALL be complete in order to enable the course of the evaluation and certification to be traced and re-confirmed. It SHALL be securely and accessibly archived for at least five years from the date at which the certificate is issued.

44 The archived material SHALL be made available to the Certification Body CSEC at request within seven working days.

3.2 Developer

45 The Developer is the organisation that produces the target of evaluation. The Developer supports the Sponsor during the evaluation by providing necessary documentation, technical know-how, and evaluation evidence. The Developer and the Sponsor may be the same.

46 All Developer requirements are in legal terms, requirements on the Sponsor with whom the Certification Body has an agreement. In practice, the Developer is the party who will need to take action to fulfil these requirements.

47 The Developer SHALL:

- assign a technical point of contact who the other parties can contact for target of evaluation support and clarifications
- support the evaluation, for example, by educating evaluators and certifiers on the target of evaluation
- develop and deliver evaluation evidence
- respond to evaluator and certifier findings, for example, by updating or producing new evaluation evidence
- support the evaluator during site visits, for example, by ensuring that the evaluator has access to development areas and can interview key personnel

3.3 ITSEF

48 The ITSEF is responsible for ensuring that the assessment performed is consistent with the Common Criteria, the Common Methodology, and the Scheme. The evaluator is associated with an ITSEF and performs the assessment of the target of evaluation. The evaluator provides the certifier with evaluation reports containing findings and verdicts.

49 ITSEFs prove their expertise and ability to conduct evaluations by obtaining a license to operate under the Scheme. The evaluator proves his expertise to the Certification Body by achieving the status of qualified evaluator. For further information about the ITSEF license process and the evaluator training and status program, see Scheme publication SP-004 *Licensing of Evaluation Facilities*.

50 The evaluator SHALL:

- comply with the principles of evaluation (see section 2.2) and the Scheme
- perform the evaluator actions required by the evaluation assurance level; Common Criteria for Information Technology Security Evaluation, Part 3: *Security assurance requirements;* the Common Methodology; and the Scheme
- receive and safely store the evaluation evidence, e.g., documentation, the security target (ST), and the target of evaluation
- perform the site visits required by the Scheme and the Common Methodology
- request and receive evaluation support as needed, e.g., target of evaluation training by the Developer and interpretations by the certifier
- provide and maintain evaluation reports
- provide the certifier with evaluation evidence
- receive and take any necessary actions in response to the oversight deliverables from the certifier
- document and justify the overall verdict and interim verdicts to the certifier

51 Note that this is not a complete list of all evaluator tasks and responsibilities. Also note that the term *evaluator* in this document is gender- and plural non-specific and applies equally to an individual evaluator or an evaluation team.

52 For each evaluation, the ITSEF SHALL:

- determine the competence needed in the evaluation team
- assign evaluators accordingly
- assign one evaluator to be the evaluation point of contact

- assign a lead evaluator who SHOULD be technically responsible for the evaluation

53 If necessary, the ITSEF SHOULD:

- augment the evaluation team with internal or external technical experts.

54 The individual evaluator SHALL be technically competent for the assigned evaluation activities. The lead evaluator SHOULD ensure that the right competence is assigned for each evaluation activity. Note that an individual evaluator can be both the point of contact and the lead evaluator for an evaluation.

55 The lead evaluator SHOULD be a qualified evaluator; for more information, see Scheme publication SP-004 *Licensing of evaluation facilities*.

3.4 Certification Body

56 The Certification Body provides independent confirmation of the evaluation results by overseeing the evaluation process. This oversight is performed by certifiers working for the Certification Body. The Certification Body will carry out surveillance of the ITSEF operation through its day-to-day involvement in the evaluations performed by the ITSEF.

57 The certifier oversees an evaluation by reviewing the evaluation reports produced by the evaluator and by witnessing the evaluator's site visits at the Developer site. The results are documented as technical oversight reports. The certifier also provides support to the evaluator regarding Scheme matters, interpretations of the Common Criteria, etc.

58 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 publicly available 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.

59 The certifier will:

- perform technical oversight of evaluations
- receive and review evaluation evidence and evaluation reports
- provide oversight deliverables, e.g., technical oversight reports
- support evaluations by providing Scheme and Common Criteria interpretations and guidance
- approve or disapprove the evaluator's overall verdict and interim verdicts
- document and justify the oversight verdict and oversight interim verdicts
- document the certification results in a certification report and issue a certificate
- report insufficiencies regarding the evaluation to Licenser

60 Note that the list above is not a complete list of all certifier tasks and responsibilities. Also note that the term *certifier* in this document is gender- and plural non-specific and applies equally to individual certifiers and a certification team.

61 The Certification Body shall create conditions that ensure that evaluations conform to:

- the principles of evaluation (see section 2.2)
- the Common Criteria
- the Common Methodology
- the Scheme

62 For each certification, the Certification Body will:

- assign one certifier to be the certification point of contact
- assign a lead certifier to be technically responsible for the certification

63 The individual certifier shall be technically competent to perform the assigned certification activities. The lead certifier will ensure that the right competence is assigned for each certification activity.

4 Start-of-evaluation

4.1 Overview

64 The start-of-evaluation phase begins with the Sponsor contacting an ITSEF to initiate an evaluation of a target of evaluation or protection profile. Before and during this phase, the Sponsor will prepare for the evaluation and certification process, possibly with the help of the ITSEF. After the Sponsor and the ITSEF have completed the necessary preparation, the Sponsor will submit a certification application to the Certification Body for review. An initial meeting is held with all parties involved in the evaluation and certification. At the meeting, the Certification Body describes the evaluation and certification process, and all questions are addressed. The Certification Body decides whether to accept or reject the certification application. The conduct of evaluation phase can begin after both an evaluation agreement and a certification agreement are signed.

4.2 Feasibility Study

65 It is recommended that the ITSEF conduct a feasibility study before accepting the evaluation. It is also recommended that the Sponsor and the Developer prepare for the evaluation and certification. More guidance for the start-of-evaluation phase is available in Scheme publication SP-084 *Sponsor's and Developer's Guide - Evaluation and Certification.*

66 After an initial contact between the Sponsor and the ITSEF, the Sponsor MAY provide the security target or the protection profile, and possibly other evaluation evidence, in draft or completed form to the ITSEF.

67 The ITSEF MAY conduct a feasibility study on the provided evidence to determine the likelihood of a successful evaluation, as well as to scope out the evaluation and to estimate the cost.

68 The ITSEF MAY inform the Certification Body that initial contact has been made with a potential Sponsor and the expected completion date of the feasibility study. With the knowledge of initial contact between the Sponsor and the ITSEF, the Certification Body can formulate appropriate resource plans in preparation for certifier activities during the start-of-evaluation phase.

69 The feasibility study will result in one of the following conclusions:

- The evaluation is not feasible and therefore will not be initiated.
- The evaluation is feasible, but only after additional preparation.
- The evaluation is feasible and may proceed without the need for any additional preparation.

4.3 Application for Certification

70 The Sponsor or the ITSEF on behalf of the Sponsor SHALL submit to the Certification Body:

- an application for certification using Scheme publication SP-010 *Certification Application - Form* The Sponsor SHALL sign the application for certification.
- The following appendices are mandatory:the security target or protection profile
- all documents referenced in the security target or protection profile which are not publically available
- an evaluation work plan (EWP)

71 Other appendices may be added as needed,

72 An evaluator impartiality and independence justification, if required, may be added as an appendix to the Application, or presented at the Initial meeting.

73 An Application fee will be invoiced according to SP-008 *Charges and Fees.*

74 An Application for certification is valid one year from the date it is received by the certification body. Applications that has not resulted in a Certification Agreement within that period SHOULD be renewed by the sponsor.

75 In the case of a re-evaluation the Sponsor SHALL also provide:

- a re-evaluation impact analysis report
- the certified security target
- the corresponding certification report

76 All the documents identified above are referred to as the certification application deliverables and SHALL be delivered with the application for certification. The certification application is considered complete when all the documents identified above have been delivered to the Certification Body in a finalised version or in a draft version that meets the requirements of the certification review process (see section 4.3 *Application for Certification - 4.3.4 Re-evaluation Impact Analysis Report*. The application review may start and the initial meeting may take place as soon as the certification application is complete. This is mandated by the CSEC queue policy (see Köpolicy -CC-Certifiering).

77 For evaluations at EAL 2 and above and for which the Sponsor and the Developer are different organisations, the Developer SHOULD in writing agree to provide necessary support to the Sponsor throughout the evaluation. The agreement SHOULD also cover:

- confidentiality between the Sponsor and the Developer
- intellectual property rights
- responsibilities after a completed evaluation and certification

78 Upon request by the Certification Body, the Sponsor-Developer agreement SHOULD be made available to the Certification Body during the review of the certification application.

79 The Sponsor-ITSEF evaluation agreement SHOULD cover:

- confidentiality between the Sponsor and the ITSEF
- intellectual property rights
- terms of payment
- how evaluation-related documentation, software, hardware, etc. shall be handled after the evaluation

80 Upon request by the Certification Body, the Sponsor-ITSEF agreement SHOULD be made available to the Certification Body during the review of the certification application.

4.3.1 Security Target or Protection Profile

81 The security target or the protection profile SHALL comprise all major content items stated in CC Part 1 *Introduction and general model* and SHALL enable the evaluator to determine that there are no obvious deficiencies preventing the certification to start.

82 The quality of the security target or protection profile is of outmost importance for the subsequent evaluation and certification.

83 A submitted security target or protection profile SHOULD fulfil the following requirements:

- The scope and physical and logical boundaries of the target of evaluation SHALL be clearly identified and meaningful for an evaluation and for a potential customer of the target of evaluation.
- The security functional requirements provided by the target of evaluation SHALL provide a meaningful set of security requirements for the intended use.

84 Before submitting the Security target to the Certification Body the Sponsor, or the ITSEF on behalf of the Sponsor, SHALL ensure that the following issues are handled.:

- The physical (what TOE is) and the logical (what TOE and TSF does) scopes of the TOE are clearly defined.
- The subjects (the active parts of the TOE) , the objects (passive parts of the TOE), any protected information (data flowing to/from objects, subjects and external entities), any protected resources (typically access to services or interfaces), the operations (what the TOE does), the security attributes (properties of subjects and objects used by the security mechanisms), etc. are well defined in the ST, and that these are used to describe the TOE throughout the ST, in particular in the SFRs.
- The security problem stated in the ST is well-defined, non-trivial, and not misleading considering the TOE type and the TOE description.
- The security objectives are written in the form of security requirements, not functional requirements.
- The mappings are presented on the same level of detail as the items being mapped.
- The rationales are presented in a logically coherent manner, and on the same level of detail as the items whose relation are being justified.
- The statement of SFRs is complete. For example, the proper FCS_COP and FCS_CKM requirements shall be present when cryptographic mechanisms are used to meet the security objectives of the TOE.
- CSEC's policies and Scheme Notes are being followed.
- General quality management is applied, including e.g. correct and specific references.

85 If the evaluation and certification will be subject to mutual recognition, the security target or protection profile in its final version will be public and, therefore, SHOULD not contain any information that is not suited for publication. In cases where the security target in its final version contains information that should not be made publicly available, a sanitised security target, called an ST-lite, can be published instead. The ST-lite must be a real representation of the complete security target. This means that the ST-lite cannot omit information that is necessary to understand the security properties of the target of evaluation and the scope of evaluation. The Sponsor SHOULD notify the Certification Body in writing if an ST- lite will be developed.

4.3.2 Evaluation Work Plan

86 The ITSEF SHOULD together with the Sponsor produce an evaluation work plan based on information gained during the feasibility study. The evaluation work plan SHALL describe the schedule for the evaluation.

87 The evaluation work plan SHALL meet the requirements stated in Appendix A; that is, the evaluation work plan shall be reasonable in terms of time, cost, and fulfilment of the Common Criteria, the Common Methodology, and the Scheme.

88 At a minimum, the evaluation work plan SHALL cover the following:

- resources
- competence and training of the resources

- parallel evaluation activities
- evaluation evidence deliverances
- dependencies between evaluation activities

89 The evaluator SHALL present to the Certification Body a detailed description of the evaluator's approach to performing the evaluation work including a detailed evaluation time schedule; see the detailed evaluation description requirements in Appendix A. The detailed description can be documented as a part of the evaluation work plan, or as a separate document.

90 If the evaluation covers new evaluation areas, like new versions of Common Criteria and Common Methodology, assurance levels EAL5 or higher, or technical areas new to the ITSEF (e.g. hardware, smart cards), the evaluation facility SHOULD in writing declare the evaluator's competence with respect to the new areas and how the evaluator has achieved this knowledge.

91 If new evaluation areas are covered this may result in additional interviews with the evaluator and new assessment of the ITSEF site and equipment.

4.3.3 Evaluator Impartiality and Independence Justification

92 An evaluator and impartiality justification SHALL be submitted with the Application or brought to the Initial Meeting, if there are specific circumstances that may affect the evaluators ability to act free from any undue internal and external commercial, financial and other pressure and influence that may adversely affect the quality of their work.

93 When members of the ITSEF have been involved in advice activities or assisting the Sponsor with the development of evaluation evidence, the evaluator impartiality and independence justification SHALL explain how the objectivity of the evaluation will be upheld. The justification SHALL demonstrate sufficient organisational separation between those individuals providing advice and those conducting the evaluation.

94 An evaluator impartiality and independence declaration MAY be stated e.g. within the evaluation work plan or any other document and may not have to be documented in a separate document.

95 If there are no specific circumstances as described above, the evaluator MAY omit submission of an evaluator impartiality and independence justification. This may, for example be discussed with the CB during the certification initial meeting.

4.3.4 Re-evaluation Impact Analysis Report

96 A re-evaluation impact analysis report SHALL be submitted in case of a re-evaluation. The re-evaluation impact analysis report SHALL show the security-relevant impact of any changes made to the target of evaluation since the previous certification. Relevant changes are not necessarily limited to the product itself; for example, changes in development tools, development physical security, and delivery processes are potentially security-relevant. In particular, the necessary changes that has to be done to the evaluation evidence, and which evaluation activities that have to be redone, SHALL be described.

4.4 Certification Application Review

97 The Certification Body will acknowledge the receipt of the certification application and provide an estimate to the Sponsor specifying how long the Certification Body will need to review and approve the application. When the certification application is complete, one or more certifiers will be assigned the task of analysing the contents of the application.

98 The certification application review will consider all submitted certification application deliverables and, if applicable the evaluation agreement and the , agreements between the Sponsor and Developer.

99 The certifier will examine all certification application deliverables to determine whether the deliverables, the ITSEF, and the assigned evaluators meet the requirements stated in this chapter and the relevant appendices.

100 The certifier will determine the competence needed in the evaluation team and assess the assignments made by the ITSEF.

101 The certifier will report the assessment results, and may request justification from the ITSEF for the assignment decisions, with regard to the overall technical competence of the evaluation team.

102 The certifier shall determine that there are no obvious deficiencies preventing the certification to result in a certificate and a certification report.

103 The certifier shall present to the Sponsor and evaluator any and all reasonable doubts found during the examination of the application that may hinder execution of the evaluation work plan with fulfilment of the Common Criteria, the Common Methodology, and the Scheme. However, the certifier shall not be held responsible for the comprehensiveness of this reporting and other issues that might be discovered later.

104 If the certifier finds evidence (or evidence incompleteness) that shows beyond a reasonable doubt that the evaluation cannot be executed with fulfilment of the Common Criteria, the Common Methodology, and the Scheme, the certifier will reject the certification application.

4.5 Initial Meeting

105 An initial meeting SHALL take place during the start-of-evaluation phase when the certification application is complete. The Certification Body uses the certification application deliverables and the initial meeting to decide whether to accept or reject the certification. The Certification Body will request the initial meeting.

106 The Certification Body, Sponsor, ITSEF, and for EAL 2 and above the Developer, SHOULD be represented at the initial meeting. The lead certifier, the lead evaluator, the certification point of contact, the evaluator point of contact, and the Developer's technical point of contact SHOULD attend the initial meeting.

107 The initial meeting SHOULD provide the Certification Body with some familiarity with the protection profile or target of evaluation and its evaluation evidence. This should give the Certification Body an understanding of the context and complexity of the evaluation, so that the Certification Body can provide accurate and timely guidance or interpretations.

108 The certifier will inform the parties of their responsibilities and provide process guidance if any party is new to the Scheme or if any party requests such information. It is critical that all parties agree on the terms of confidentiality, post-certification documentation and material (e.g., software and hardware) storage, and the rights of each party with regard to evaluation evidence and evaluation results.

109 Potential problems and all clarification requests related to the evaluation and certification SHOULD be brought up for discussion during the initial meeting.

110 The Sponsor or the Developer SHALL, on request by the Certification Body, provide a presentation on the target of evaluation or protection profile. The Sponsor and the Developer SHALL be prepared to answer questions about the target of evaluation or protection profile. Note that the questions can cover anything from development procedures to low-level technical details.

111 The ITSEF SHALL be prepared to justify the evaluation work plan and SHOULD be prepared for time schedule and project risk questions during the initial meeting.

112 The ITSEF SHALL be prepared to justify evaluator assignments in the evaluation work plan based on technical skill requirements, the target of evaluation technology, and the methods and techniques needed to test the target of evaluation. This justification is especially important if the evaluators have no previous experience with the specified evaluation assurance level or with the type of target of evaluation.

113 The ITSEF SHALL be prepared to give further details about the competence needed and how these competence needs are met.

114 The ITSEF SHALL be prepared to answer questions about the evaluator impartiality and independence justification.

115 The Sponsor, ITSEF and Developer SHALL be prepared to answer questions about the status and content of agreements between the three parties relevant for the evaluation, as described in previous section, "Certification Application".

116 If the evaluation is a trial evaluation, the Certification Body will inform all parties on the effects this will have on the process. See Scheme publication SP-004 *Licensing of evaluation facilities* for more information on trial evaluations and ITSEF licensing.

4.6 Certifier Project Planning

117 Based on the evaluation work plan delivered as a certification application deliverable, the Certification Body will plan its own corresponding activities and inform the ITSEF in writing which meetings and evaluation work items the certifier intends to observe, as well as when the Certification Body plans to perform technical oversight at the ITSEF and Developer facilities.

4.7 Certification Application Approval

118 The Certification Body will review the agreement between the Sponsor and the ITSEF to ensure that the agreement does not contain any conditions that impact impartiality.

119 The Certification Body will assure that the ITSEF and the Developer has signed security agreements, "säkerhetsskyddsavtal, SUA", with the appropriate Swedish governmental organisation if information regarding national security or the relation to other state is likely to be handled during the certification. The Certification Body will also assure that the evaluators and developers have security clearance to a level appropriate for the work foreseen.

120 For EAL 2 and above, the Certification Body will review the agreement between the Sponsor and the Developer (if these are separate organisations) to ensure that the Developer will support the evaluation and certification.

121 Upon completion of the certification application analysis and resolution of any issues raised, e.g., at the initial meeting, the Certification Body will inform the Sponsor and ITSEF whether the certification application is accepted or rejected.

122 If accepted, the Certification Body will assign a certification ID that SHALL be quoted on all future evaluation and certification documents, such as cover letters for evaluation evidence, single evaluation reports, and correspondence relevant to the evaluation and certification. This identifier shall be unique for evaluations conducted under the Scheme.

123 The Certification Body will submit the certification agreement to the Sponsor.

124 Both the Sponsor and the Certification Body SHALL sign the certification agreement.

125 The versions of the Common Criteria, the Common Methodology, and interpretations to be used during the evaluation will be listed as part of the approval in the certification agreement. The versions and interpretations should be the official versions and all published interpretations listed on the Common Criteria project website, www.commoncriteriaportal.org, at the time of the submission of the certification application. The Sponsor SHALL ensure that the security target or protection profile is consistent with this decision.

126 The certification agreement SHALL also cover:

- confidentiality
- intellectual property rights
- archiving evaluation material

127 The Certification Body will assign a lead certifier to the evaluation and depending on the complexity of the evaluation, will assign more certifiers as needed. The certifiers are responsible for conducting technical oversight of the evaluation activities carried out by the evaluator.

128 The Certification Body may use external experts on technical issues during the technical oversight process. The rules and procedures for Certification Body use of external experts are described in Scheme publication SP-007 *Quality Manual*.

5 Conduct of Evaluation

5.1 Overview

129 The conduct of evaluation phase can begin after the certification agreement is signed by the Sponsor and the Certification Body. The Sponsor and/or Developer will provide evaluation evidence, the evaluator will perform evaluation activities, and the certifier will perform technical oversight activities. The conduct of evaluation phase ends when all single evaluation reports are completed by the evaluator and accepted by the certifier.

5.2 Sponsor and Developer Activities

130 The Sponsor and/or the Developer SHALL provide the ITSEF and the Certification Body with evaluation evidence.

131 The Sponsor and/or Developer SHALL also be prepared to act on findings made by the evaluator or the certifier. The evaluator or the certifier MAY require the Sponsor and/or Developer to update the evaluation evidence or produce records to demonstrate use of processes relevant to the evaluation.

132 The Sponsor SHALL request in writing to enter the next phase, conclusion of evaluation, when all work units are assigned PASS interim verdicts and "No further comments" oversight interim verdicts, and there are no more changes to the target of evaluation or protection profile. Note that the certifier might still find issues that require changes to the evaluation evidence or the evaluation reports during the conclusion of evaluation phase.

5.3 Evaluator Activities

133 The evaluator SHALL generate evaluation reports, perform Common Methodology work units, conduct site visits and independent testing, etc., all in accordance with the Common Criteria, the Common Methodology, relevant interpretations, and the Scheme.

134 The evaluator's verdicts for work units, evaluator action elements, assurance components, and assurance classes are called interim verdicts and are documented in single evaluation reports. The interim verdict follows the evaluator verdict assignment rules defined in the Common Methodology. An interim verdict SHALL be one of the following: PASS, INCONCLUSIVE, or FAIL.

5.3.1 Evaluation Report Generation

135 The evaluator SHALL document in single evaluation reports with supporting justification the interim verdicts of all Common Criteria evaluator actions performed in accordance with the Common Methodology. A single evaluation report covers a subset of all assurance packages for the evaluation. The recommendation is to cover no more than one assurance class in each single evaluation report. For larger assurance classes such as ADV, each assurance family within the assurance class (e.g., ADV_TDS, TOE Design) can be covered in a separate single evaluation report, especially for higher evaluation assurance levels.

136 The evaluator SHALL produce single evaluation reports using the evaluation evidence provided by the Sponsor and/or Developer. The structure and content requirements of the single evaluation reports are detailed in Appendix B.

137 For a target of evaluation, a separate single evaluation report SHALL be written for the ASE assurance class and in the case of a protection profile evaluation, an APE assurance class single evaluation report SHALL be written. An ASE or APE single evaluation report MAY be divided into multiple assurance family single evaluation reports if the evaluator finds it suitable.

138 The single evaluation reports SHALL be submitted to the Certification Body for the certifier's technical oversight.

139 The individual single evaluation reports SHALL be considered provisionally complete until no certifier findings or requests for clarification remain in any single evaluation reports or in the final evaluation report.

140 The ASE class SHOULD be the first assurance activity conducted. The security target is the basis for the whole evaluation, and it must be clear and consistent before successful assurance work can be performed on other evaluation evidence. The security target evaluation SHOULD be reported in a single evaluation report before other target of evaluation evaluation activities begin. The security target single evaluation report remains provisionally complete until the target of evaluation evaluation is complete. Findings during the target of evaluation evaluation may necessitate changes to the security target, impacting the previous security target evaluation results and possibly requiring a renewed security target evaluation.

141 During an evaluation, it may be necessary to evaluate some work units and entire assurance families several times. The need to repeat evaluation work arises when new or updated evaluation evidence becomes available, or when findings during the target of evaluation require changes to the evaluation evidence. Reassessment results are captured in an updated single evaluation report. Note that every dependent work unit SHALL either be reassessed or a sufficient justification SHALL be given as to why reassessment is not necessary.

142 If the certifier identifies faults or requests clarifications in the technical oversight report, the evaluator SHALL respond or correct, update, and resubmit the single evaluation report. The evaluator's actions SHOULD be performed without delaying overall progress on the evaluation and certification.

143 If the technical oversight report identifies faults or requests clarifications, for each issue identified, the evaluator SHALL produce an answer containing the requested clarification or a description of and references to the changes made to the single evaluation report and any evaluation evidence. This SHALL be documented in a separate document submitted with the updated single evaluation report, if applicable.

144 The evaluator and certifier MAY meet to discuss the Evaluation Report and the content of the Technical Oversight Report. It is particularly recommended to do so on two occasions:

- after the Single Evaluation Report for ASE
- after the Single Evaluation Report for ADV but before testing

5.3.2 Site Visit Assessment

145 The purpose of site visits at the Developer site is to determine whether the procedures described in the Developer documentation are followed. Site visits SHALL be performed for evaluations at EAL 3 and above, as required by the Common Criteria. The Common Methodology identifies the assurance families for which site visits are applicable or required: ALC_CMC.n (n>=3), ALC_DEL and ALC_DVS.

146 For re-evaluations at EAL 3 and above, site visits SHOULD be performed. The decision not to perform a site visit is subject to certifier approval.

147 The evaluator SHALL produce a separate document detailing a site visit plan for site visits planned in the evaluation work plan. The site visit plan SHALL demonstrate how the evaluator plans to conduct the site visit.

148 The certifier SHALL review the site visit plan and, if necessary, request an update.

149 The evaluator SHALL invite the certifier to attend the site visit well in advance of the scheduled date.

150 The evaluator SHALL produce a site visit report documenting the outcome after conducting the site visit. The site visit report SHOULD be considered input for the single evaluation reports covering work units related to site visits.

5.4 Certifier Activities

151 During the conduct of evaluation phase, the certifier oversees the evaluation. This oversight is based on three certifier activities:

- examination of evaluation reports and evaluation evidence as documented in the various evaluator reports
- participating in the evaluator site visit at the Developer site
- particpating in the evaluator testing activities

152 The certifier will perform oversight and deliver technical oversight reports, according to the EWP and the agreed time plan.

5.4.1 Single Evaluation Report Technical Oversight

153 The certifier will examine all single evaluation reports to verify that they are technically sound and consistent with the requirements of the Common Criteria, the Common Methodology, the relevant interpretations, and the Scheme. The single evaluation report content and structure requirements are defined in Appendix B.

154 The certifier will examine the single evaluation reports to verify the evaluation conclusions and the analysis supporting those conclusions. The certifier can use the evaluation evidence to verify the evaluator conclusions.

155 The result of the examination of an evaluation report is documented in a technical oversight report produced by the certifier and sent to the evaluator. The technical oversight report shall provide the evaluator with identified evaluation issues, comments, and requests for clarifications. Each issue and request will be uniquely identified. The issues reported might require evaluator, Sponsor, and/or Developer actions.

156 The certifier uses two oversight interim verdicts in the technical oversight report: "Not OK" and "No further comments". The certifier shall state “Not OK” for each examined work unit with identified issues or for which the certifier requests clarification. “No further comments” shall be stated if no findings are found. The "No further comments" verdict will be stated at the appropriate level: on an assurance class as a whole, an assurance family, an evaluation sub-activity, an evaluation action, or an individual work unit, in such way that all work units identified in the examined single evaluation report are covered by the verdicts reported in the technical oversight report. The oversight interim verdict for an assurance family and assurance class shall be "Not OK" if any underlying work unit is judged "Not OK".

157 If the certifier has no further comments, the single evaluation report is provisionally accepted. However, new or updated evaluation evidence and findings during the target of evaluation evaluation that require changes to the evaluation evidence sometimes impact previous evaluation results, requiring work units to be reworked.

158 The certifier will ensure that technical oversight reports are made available to the Sponsor and/or Developer in case Sponsor or Developer actions are required.

159 The appropriate party (Sponsor, Developer, or ITSEF) SHOULD resolve reported issues in a timely manner, not delaying overall progress on the evaluation and certification.

160 The evaluator SHALL update the single evaluation report if work units are redone and/or respond to the certifiers comments by written statements in the technical oversight report. The certifier will review updated single evaluation reports and consider evaluator statements in the returned technical oversight report, and issue a new or updated technical oversight report.

161 The evaluator and certifier MAY meet to discuss the Evaluation Report and the content of the Technical Oversight Report. It is particularly recommended to do so on two occasions:

- after the Single Evaluation Report for ASE
- after the Single Evaluation Report for ADV but before testing

5.4.2 Sight Visit Oversight

162 The certifier reserves the right to attend site visits performed by the evaluator. Site visits are required at EAL 3 and above. The purpose is for the certifier to observe the evaluator actions.

163 The certifier shall review the evaluator's site visit plan and, if necessary, request an update.

164 The certifier will focus on observing the evaluator's compliance with the principles of evaluation (see section 2.2). For example, the certifier shall verify that the evaluator only collects evidence, and does not generate new evidence.

165 The certifier will document observations accumulated during the site visit assessment. The observations will be used to verify the evaluator's site visit report, which documents the outcome of the site visit. The evaluator's site visit report SHOULD be considered input for the single evaluation reports covering work units related to site visits.

5.4.3 Testing Oversight

166 The certifier will observe evaluator actions such as independent testing and penetration testing. Evaluator oversight provides the certifier with an opportunity to verify the evaluator's conformance to the Common Criteria and the Common Methodology.

167 Although oversight is primarily an observation activity, the certifier sometimes has an opportunity to provide guidance in response to a request from the evaluator, Developer, or Sponsor. In such cases, the certifier will carefully consider the nature of the guidance requested, giving due consideration to its application as a Scheme-wide interpretation and to its formal distribution in accordance with interpretation procedures.

6 Conclusion of Evaluation

6.1 Overview

168 The conclusion of evaluation phase can be entered when all single evaluation reports have been completed and accepted by the certifier; i.e., all work units have a "No further comments" oversight interim verdict.

169 The evaluator will produce the final evaluation report, which will be used as an input for writing the certification report. This phase will end with the Certification Body issuing and possibly publishing the certificate and a certification report.

6.2 Final Evaluation Report Production

170 The final evaluation report reports on all evaluation activities in all single evaluation reports, covering both the security target evaluation and the TOE evaluation. The objective of the final evaluation report is to provide information necessary to produce the certification report, which provides practical information about the target of evaluation to the consumer.

171 The evaluator SHALL produce the final evaluation report, which SHALL be based on the full set of accepted single evaluation reports, by compiling relevant information.

172 The evaluator's result is documented with an overall verdict in the final evaluation report. The overall verdict is defined in the Common Methodology and can be one of the following: PASS or FAIL.

173 The content and structure of the final evaluation report SHOULD follow Appendix C. The information content requirements are driven by the requirements stated in the Common Methodology, and Scheme-specific requirements.

174 The final evaluation report SHALL include detailed information about the evaluation. This may be done by referencing the single evaluation reports.

175 With the exception of the detailed information, the final evaluation report SHALL provide the information necessary to produce the certification report and SHOULD be free of any information that is not suited to be copied into the certification report. The final evaluation report MAY fulfil the information content requirements by reference.

176 The evaluator SHOULD send the final evaluation report to the Sponsor and/or Developer for review prior to submission to the certifier. This review is especially important for certification that will be subject to mutual recognition. The Sponsor and/or Developer review SHOULD ensure that the final evaluation report can be used for the generation of the certification report.

177 In addition, the evaluator MAY assume that the certifier is familiar with general principles of IT and IT security and need not elaborate on them unless it is appropriate to do so to provide a clear presentation.

178 The individual single evaluation reports, especially the security target single evaluation report, are not technically complete until the evaluation is complete; therefore, if needed, single evaluation reports SHOULD be updated.

6.3 Final Evaluation Report Review

179 The certifier will examine the final evaluation report to determine that the requirements for information content and structure are satisfied. The correctness and completeness of the final evaluation report is important, as this document is the basis for the certification report.

180 The certifier's certification result verdict is called an oversight verdict, and is documented in the final evaluation report, technical oversight report, and in the certification report. The oversight verdict is defined in the Common Methodology and shall be either PASS or FAIL.

181 The certifier will always generate a technical oversight report in answer to the final evaluation report.

182 The technical oversight report identifies issues and requests clarifications regarding the final evaluation report, and will be sent to the evaluator. The evaluator may have to update one or more single evaluation reports to resolve the issues found during the final evaluation report examination.

183 Issues reported in the technical oversight report might require evaluator, Sponsor, and/or Developer actions; if necessary, an updated final evaluation report and possibly updated single evaluation reports and evaluation evidence SHALL be produced and submitted to the Certification Body.

184 If the technical oversight report identifies faults or requests clarifications, for each issue identified, the evaluator SHALL produce an answer containing the requested clarification or a description of and references to changes made to the final evaluation report and possibly single evaluation reports and evaluation evidence. This response SHALL be documented in a separate document submitted with the updated final evaluation report, if applicable.

185 If the overall verdict is FAIL and there is a need for major changes to a single evaluation report or if the evaluation evidence needs to be updated, the certifier will send the evaluation and certification back to the previous phase, conduct of evaluation.

6.4 Certification Report Preparation and Approval

186 After the certifier has approved the final evaluation report (see section 6.3), the certifier will produce a certification report. The certifier will use the final evaluation report as the basis for the certification report.

187 The certifier will deliver a draft certification report to the Sponsor and the evaluator for comment, indicating a due date for comments. The Sponsor SHALL assist the certifier by reviewing the certification report.

188 If the certificate is intended to achieve mutual recognition, the certification report shall only contain information that can be made public. The Sponsor SHALL inform the certifier of any information in the certification report considered inappropriate for public release.

189 The certifier will inform the Sponsor if suggested changes might have an impact on the Scheme compliance or mutual recognition. The certifier shall also inform the Sponsor about the possibility of developing an ST-lite.

6.5 Certificate Report and Certificate Issuing and Publishing

190 The final version of the certification report will be distributed to the Sponsor.

191 A certificate may be issued for an evaluation and certification with a PASS overall verdict and a PASS oversight verdict.

192 If a certificate has been issued, the certifier will update the certified products list in accordance with the scope of recognition.

193 A security target or protection profile that is certified, and should be internationally recognised, will be registered. The registration is the publication of the security target or protection profile, and the registration identifier is the certification ID.

6.6 Project Cleanup and Closedown

194 After the evaluation has been finished, the evaluator SHALL handle all material used during the evaluation according to the terms in the evaluation agreement; material will be archived, returned, or destroyed, as agreed.

195 In the case of a TOE evaluation, the Sponsor SHALL ensure that the Certification Body has access to a reference copy of the certified target of evaluation as long as the certificate is valid, i.e., not withdrawn. This arrangement SHOULD be regulated in the certification agreement between the two parties.

196 The Certification Body will archive the reference material needed to demonstrate traceability, reproducibility, and repeatability of evaluation and certification result.

7 After a Certificate has been Granted

7.1 Duration and Validity of Certificate

197 A certificate is valid only for the specific product and version that has been evaluated according to the Certificate Report.

198 For as long as the certificate is valid the sponsor SHALL keep a reference copy of the Target of Evaluation.

199 For as long as the certificate is valid the sponsor SHALL also:

- keep a record of all complaints made known to the sponsor relating to a product's compliance with requirements for certification and make these records available to the certification body when requested;
- take appropriate action with respect to such complaints and any deficiencies found in products or services that affect compliance with the requirements for certification;
- document the actions taken.

200 The period of validity is agreed between the Sponsor and the Certification Body. During the period of validity, the certificate will be surveilled on a yearly basis to ensure that the Sponsor fulfils its obligations under the terms of the agreement.

7.2 Certificate Misuse

201 The Certification Body exercises control over the use of associated trademarks and issued certificates.

202 The Certification Body will take appropriate administrative, procedural, or legal steps to prevent or counter misuse of certificates or associated trademarks and to correct false, misleading, or improper statements about certificates or about the Scheme.

203 Conditions for the use of trademarks applicable to the certification process are listed in Scheme publication SP-070 *Conditions for Use of Trademarks*

204 The Certification Body will withdraw certificates in cases where the conditions for holding a certificate no longer apply.

8 Supporting Processes

8.1 Observation Report Handling

205 The observation report (OR) is a mechanism whereby actions required of an evaluation or certification party are documented and under control, to be resolved in a timely manner.

206 Observation reports may be used when a party experiences difficulties related to the evaluation, or with evaluation findings, such as:

- difficulties in obtaining necessary documentation from the Sponsor, Developer, or the ITSEF as scheduled in the evaluation work plan
- exploitable vulnerabilities, or incomplete or inaccurate evaluation evidence, leading to a potential evaluation failure
- unexpected delays to the evaluation work plan

207 For example, if during the course of the evaluation, the evaluator requires support from the certifier that cannot be provided using other means, e.g., evaluation reports, the evaluator may submit an observation report to the Certification Body.

208 The party responsible for resolution of an observation report SHALL resolve the matter in a timely manner, in accordance with the timeframe that SHALL be specified in the observation report. In cases where the specified timeframe cannot be met, the responsible party SHALL communicate this information and SHALL provide a revised timeframe for resolution.

8.2 Document Management

209 If a specific statement is identified in the Scheme procedures regarding the format of a certain document, this statement SHALL be followed. If no specific format statements apply, the documents SHOULD be in the Portable Document Format (PDF) and in digital form, preferably on CD or DVD. If a document is delivered to CSEC in multiple formats, one of these will be selected as the original. If one of these formats is consistent with the above format rules, that format will have precedence over the other.

210 All evaluation reports and other evaluator-generated documentation submitted to the certifier in the certification process SHOULD be made available in two versions: one without change markings and one with change markings indicating all changes since the previous version. The version without change markings will have precedence.

Appendix A Evaluation Work Plan

A.1 Overview

211 The evaluation work plan is a project plan that describes the evaluation work items, the work schedule, and the resources assigned to perform the evaluation work items. The evaluation work plan SHOULD be produced jointly between the Sponsor and the evaluator, and SHALL be delivered as a part of the certification application deliverables to the Certification Body.

212 The evaluator SHALL present a detailed evaluation description to the Certification Body. This SHALL be a part of the evaluation work plan or a separate document. At the end of this appendix are the requirements for the detailed evaluation description.

213 There are no requirements for the evaluation work plan structure. The requirement sections below groups similar requirements together.

A.2 General Requirements

214 The evaluation work plan SHALL demonstrate to the Certification Body that the plan is reasonable in terms of time, cost, and fulfilment of the Common Criteria, the Common Methodology, and the Scheme. Typical areas of interest are: resources, resources' competence and training, parallel evaluation activities, evaluation evidence deliverances, and dependencies between evaluation activities.

215 The evaluation work plan SHALL, as in all other deliverables, contain appropriate protective markings and SHALL identify all appropriate evaluation identification information including, but not necessarily limited to: identification of the protection profile or target of evaluation, Developer, Sponsor, ITSEF, and the protection profile or target of evaluation version number.

216 The evaluation work plan SHALL describe, when applicable, how access is given to equipment (test systems, hardware, software, etc.) not owned by the ITSEF that is required for certain evaluation work. The evaluator's independent tests may, for example, be performed in a lab at the Developer site.

A.3 Evaluation Activities

217 The evaluation work plan SHALL address all Common Methodology general evaluation tasks, activities, and sub-activities matching the assurance requirements expressed in the security target.

218 The evaluation work plan SHALL address the production of the single evaluation reports and the final evaluation report, and SHALL also identify the evaluation evidence that is necessary to produce each of these reports. This can be checked by comparing each evaluation work item comprising the evaluation work plan with the input section for each Common Methodology sub-activity for the corresponding assurance requirements, to verify that there are no evaluation evidence items missing from the evaluation work plan.

219 The evaluation work plan SHALL take proper account of all dependencies between work units. As an example, work units corresponding to vulnerability analysis MAY generally be the last ones scheduled, because vulnerability analysis relies upon evaluator knowledge and experience gained as a result of performing the other evaluation work units.

A.4 Schedule and Delivery Dates

220 The evaluation work plan SHALL include an evaluation schedule that identifies the start date and completion date for each work item. The schedule MAY be represented as a Gantt chart and a delivery timetable.

221 The Sponsor and the evaluator SHALL specify their deliveries and delivery dates in the evaluation work plan, and for EAL 2 and above the evaluation work plan SHALL include the Developer's delivery dates for the evaluation evidence.

222 For an evaluation at EAL 3 and above, the evaluation work plan SHALL schedule the evaluator's site-visit(s) at the Developer facility or facilities. The Certification Body will also perform site visits, for example, a site visit at the ITSEF during independent and penetration testing.

223 A site visit plan SHALL be delivered to the Certification Body at least five working days prior to the evaluator's site-visit.

224 The evaluators test plan and vulnerability analysis, together with the developers test report SHALL be delivered to the Certification Body at least five working days prior to the evaluator's independent and penetration testing.

225 The evaluation work plan SHALL identify planned meetings between the evaluator and the Sponsor, certifier, or Developer.

226 The evaluation work plan SHALL reserve time for updates of evaluation reports and evaluation evidence. The initial delivery of an evaluation report is usually not the only delivered version, because the certifier might find issues with the report, or the evaluation evidence on which the report is based might change during evaluation and certification. Sometimes significant changes to the evaluation report, as well as to the related evaluation evidence, will be required.

227 Note that the Single Evaluation Report SHOULD only be sent to the Certification Body when all the verdict in the Single Evaluation Report is PASS or when there are unsolved FAIL or INCONCLUSIVE verdicts that require special attention from the certifier.

228 For a TOE evaluation, the ASE class SHOULD be the first assurance activity planned.

A.5 Evaluation Staffing

229 The evaluation work plan SHALL identify the individual evaluators assigned to each evaluation report, such that the certifier can verify that:

- the Common Methodology principle of impartiality is upheld in cases where an evaluation is preceded by advice activities or other consultancy activities by the ITSEF.
- evaluators are qualified to perform the assigned evaluation work.

A.6 Detailed Evaluation Description

230 The evaluator SHALL present an evaluation schedule that identifies the total amount of planned effort required to perform the work for each work item.

231 The evaluator SHALL demonstrate to the Certification Body that the plan is achievable with the allocated resources. For example, concurrently assigning the same evaluators to two or more different work items may indicate a risk to completing the evaluation work as planned.

232 The evaluator SHALL present details regarding the evaluator's approach to independent testing, as well as the evaluator's approach to vulnerability analysis (assuming this is part of the evaluation). The level of detail expected shall be sufficient to provide the certifier with confidence that the evaluator has performed enough preliminary investigation to determine the scope and magnitude of the independent testing and vulnerability analysis.

233 The evaluator SHALL demonstrate to the Certification Body that the evaluator recognises and has considered the increasing evaluation work complexity as the evaluation assurance level increases. This applies to all evaluation work including work units that are consistent across all evaluation assurance levels.

Appendix B Single Evaluation Report

B.1 Overview

234 The evaluator documents the interim verdicts and justifications in accordance with the Common Methodology in a single evaluation report. A single evaluation report covers a subset of all assurance packages for the evaluation. For larger assurance classes, each assurance family can be covered in a separate single evaluation report.

B.2 Structure and Information Content

235 The following requirements apply to a single evaluation report in general. At a minimum, the cover page SHOULD contain the following information:

- document name
- version number
- file name
- product name
- Sponsor name
- ITSEF name
- Certification Body name
- certification ID
- lead evaluator name
- appropriate protective markings

236 At a minimum, the headers or footers of all pages following the cover page SHOULD identify:

- certification ID
- appropriate protective markings
- page number

237 The single evaluation report SHOULD be structured following the section headings below:

1. Evaluation Basis and Documents
2. Objectives and Dependencies
3. Evaluation Evidence and Work Units
4. Evaluation Result
5. References
6. Abbreviations and Glossary

238 The content requirements SHOULD be met in the sections included in the single evaluation report. The single evaluation report MAY include additional sections, structured as appropriate, complying with the single evaluation report purpose.

239 The information content requirements follow.

B.2.1 Evaluation Basis and Documents

240 The evaluation basis SHALL identify:

- the Common Criteria version
- the evaluation methodology
- the security target

241 The evaluation basis SHALL also identify:

- relevant Scheme documents
- interpretations considered for this single evaluation report
- Sponsor and/or Developer documents provided for the evaluation aspects addressed in this single evaluation report

B.2.2 Objectives and Dependencies

242 The objectives for this assurance class or assurance family SHOULD be identified and described, including:

- evaluation assurance level
- dependencies taken into account during the evaluation .

B.2.3 Evaluation Evidence and Work Units

243 This section SHOULD identify:

- evaluator action elements
- content and presentation of evaluation evidence elements
- applicable work units

244 When several evaluators have been working on the report and the result will be used for collecting merits for Qualified evaluator status this section SHOULD clearly identify which work units or parts of work units each involved evaluator conducted.

B.2.4 Evaluation Result

245 The evaluation result section is the major part of the single evaluation report. This section SHALL contain, preferably presented in a table, the interim verdicts for:

- the assurance class
- the assurance components
- the evaluator action elements

246 For each evaluation action element, or for each work unit where applicable, the evaluation result section SHALL provide:

- unique identification of the work unit
- identification of the evaluation input and a brief description of the information provided by the Sponsor and/or Developer relevant to this evaluation action element or work unit
- description of the evaluation work that was performed, detailed enough for the certifier's examination and to ensure general repeatability and reproducibility; preferably divided into separate sections for strategies, methods, techniques, tools, and standards used, as applicable
- description of how the evaluation evidence does or does not meet each aspect of the evaluation action element or work unit, together with a rationale linking this description to the purpose of the assurance component, the evaluation action element or work unit, the method or strategy used, and to the evaluator's interim verdict
- evaluator's interim verdict for this evaluation action element or work unit.

247 The single evaluation report SHOULD also identify the following for each work unit, evaluation action element, assurance family, or assurance class, where applicable:

- Consideration of vulnerabilities, in which the evaluator describes all potential vulnerabilities found during the evaluation covered by the single evaluation report.

- Impact on other documents identified during this evaluation.

B.2.5 References

248 The list of references SHALL contain a complete listing of all documents used during the evaluation and referred to in the single evaluation report.

249 Documents should be referenced using the following format:
Title (incl. product name & version if applicable), Document version x.x, Issuing organisation, Date, Document id (optional).

Example:
SP-002 *Evaluation and Certification*, document version 12.0, CSEC, 2009-01-16, FMV ID 25550:73 298/2005.

B.2.6 Abbreviations and Glossary

250 This section SHOULD expand on acronyms or abbreviations and define any specialised terms used in the single evaluation report that are not considered common knowledge. The acronyms and abbreviations list and glossary may be a part of the single evaluation report or may be maintained as a separate document referenced by the single evaluation report.

Appendix C Final Evaluation Report

C.1 Overview

251 The final evaluation report covers all evaluation activities in all single evaluation reports. The objective of the final evaluation report is to provide the overall verdict with justification, and to provide information necessary to produce the certification report.

252 The Evaluation section in the final evaluation report contains detailed information about the evaluation. The Results of the Evaluation section contains references to the single evaluation reports. A brief summary of the evaluation results is given in the Executive Summary.

253 With the exception of the detailed evaluation information mentioned above, the final evaluation report should not contain information not suited to be copied into the certification report.

C.2 Structure and Information Content

254 The following requirements apply to the final evaluation report in general. At a minimum, the cover page SHOULD contain the following information:

- document name
- version number
- file name
- product name
- Sponsor name
- ITSEF name
- Certification Body name
- certification ID
- lead evaluator name
- appropriate protective markings

255 At a minimum, the headers or footers of all pages following the cover page SHOULD identify:

- certification ID
- appropriate protective markings
- page number

256 The final evaluation report SHOULD be structured following the section headings below:

257

1 Introduction
  1.1 Executive Summary
  1.2 Identification of the TOE
  1.3 Security Target
2 Architectural Description of the TOE
3 Evaluation
4 Results of the Evaluation

5 Evaluator Comments, Observations and Recommendations

6 References

7 Glossary

A Annexes

258 The content requirements SHOULD be met in the sections included in the final evaluation report. The final evaluation report MAY include additional sections, structured as appropriate, complying with the final evaluation report purpose.

259 In the case of a protection profile evaluation, the same structure SHOULD be used; however, non-relevant chapters SHOULD be marked "Not applicable" or be omitted.

260 The final evaluation report content requirements are described in the following sections.

C.2.1 Executive Summary

261 The executive summary SHOULD be a brief summary of the entire report. The information contained within this section SHOULD provide the audience with a clear and concise overview of the target of evaluation and of the evaluation results. This section SHOULD include all key evaluation findings.

262 The reader of this section SHOULD gain a basic understanding of the evaluated product's functionality, as well as the results of the evaluation.

263 The executive summary SHOULD contain, but is not limited to, the following items:

- name of the evaluated target of evaluation
- target of evaluation version identifier
- an enumeration of the components of the target of evaluation that are part of the evaluation
- the name of the Scheme: "Swedish Common Criteria Evaluation and Certification Scheme"
- Developer name
- Sponsor name
- ITSEF name
- completion date of the evaluation
- brief description of the report results

264 The executive summary SHOULD also contain a summary of:

- evaluation assurance package
- conformance claims to Protection Profiles
- security functionality
- threats and organisational security policies addressed by the evaluated target of evaluation
- special or unusual configuration requirements
- special or unusual assumptions about the operating environment

C.2.2 Identification of the TOE

265 The evaluated target of evaluation SHALL be clearly identified. The version number of all separate software modules in the TOE, applicable software patches, hardware, and peripheral devices SHOULD be identified. All documentation, included when the TOE is delivered to a customer, also SHOULD be uniquely identified.

266 All labelling and descriptive information necessary to completely identify the target of evaluation SHALL be given here. Complete identification of the target of evaluation will ensure that a whole and accurate representation of the target of evaluation can be recreated for use or for future evaluation efforts.

C.2.3 Security Target

267 The security target, possibly a sanitised version, SHALL be referenced in this section.

C.2.4 Architectural Information

268 This section SHOULD provide a functional decomposition of the target of evaluation in terms of its major hardware and software structures. Significant data flows between these structures SHOULD also be identified and described as necessary to understand how the data is used in the context of the security policy.

269 If the evaluation assurance requirements include any assurance components from the ADV_TDS family, then the target of evaluation architectural description SHOULD be based on the evaluator's understanding of the high-level design; but this section SHOULD contain neither a complete reproduction of, nor simply a reference to, the high-level design.

270 If a high-level design is not available because no ADV_TDS component is included in the evaluation assurance package, then the architectural description SHOULD be based on the evaluator's understanding of other evaluation evidence available to the evaluator, particularly the functional specification.

C.2.5 Evaluation

271 This section SHOULD define the evaluation in terms of evaluation methods, techniques, tools and standards used. In particular, it SHOULD be made clear which version of the evaluation criteria and evaluation methodology has been used, as well as which interpretations have been taken into account. Also, devices used to perform the tests SHOULD be mentioned.

272 If any constraints apply to the evaluation, such as special circumstances or assumptions made during the evaluation that have an impact on the evaluation results, it SHOULD be reported here. Other relevant information, related to legal aspects, confidentiality requirements MAY also be presented in this section.

C.2.6 Results of the Evaluation

273 This section SHALL provide the overall verdict for the evaluation as defined in Common Criteria Part 1 *Introduction and general model*, Chapter 7, evaluator's interim verdict for each evaluator action element, each assurance component, and each assurance class.

274 Also, in this section, a reference to each single evaluation report SHOULD be given, where detailed descriptions of the evaluation will be found.

C.2.7 Evaluator Comments, Observations, and Recommendations

275 Additional information of possible interest to potential users acquired by the evaluator during the course of the evaluation SHOULD be documented in this section.

276 This section may include information on shortcomings of the target of evaluation that did not have an impact on the evaluation results, or information helpful in using the product more securely.

277 This section SHOULD include a complete list of all observation reports submitted during the evaluation and their status.

C.2.8 References

278 This section SHALL list all referenced documentation used as source material in the compilation of the report. This information SHOULD include, but not be limited to:

- applicable versions of the Common Criteria and Common Methodology
- applicable Certification Body documentation
- technical reference documentation
- complete listing of evaluation evidence used in the evaluation

279 Documents should be referenced using the following format:
Title (incl. product name & version if applicable), Document version x.x, Issuing organisation, Date, Document id (optional).

Example:
SP-002 *Evaluation and Certification*, document version 12.0, CSEC, 2009-01-16, FMV ID 25550:73 298/2005.

C.2.9 Glossary

280 The glossary SHOULD be used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

C.2.10 Annexes

281 The annexes MAY be used to outline any additional information that may be useful to the reader but does not logically fit within the prescribed headings of the report.

Appendix D Re-evaluation Impact analysis report

D.1 Introduction

282 The developer SHALL report the Re-evaluation Impact analysis report (RIAR) unique reference. It SHALL contain information that identifies the RIAR (e.g. name, date and version number).

283 The developer SHALL report the current TOE configuration control identifiers.

284 The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.

285 The developer shall report the configuration control identifiers for the ETR, CR, and certified TOE.

286 These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.

287 The developer SHALL report the configuration control identifiers for the version of the ST related to the certified TOE.

288 The developer SHALL report the identity of the developer.

289 The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.

290 The developer may include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

D.2 Description of the change(s)

291 The developer SHALL report the changes to the TOE in the RIAR.

292 The reported changes SHALL be relative to the certified TOE.

293 The developer SHALL report the changes to the development environment.

294 The identified changes are with regard to the development environment of the certified TOE.

D.3 Affected evaluation evidence found by developer

295 For each change, the developer SHALL report the list of affected items of the evaluation evidence.

296 For each change to the certified TOE or to the development or operational environment of the certified TOE, any item of the evaluation evidence that need to be modified in order to address the developer action elements SHALL be identified.

D.4 Description of the evaluation evidence modifications

297 The developer SHALL briefly describe the required modifications to the affected items of the evaluation evidence.

298 For each affected item of the evaluation evidence, the modifications required to address the corresponding content and presentation of evidence elements SHALL be briefly described.

D.5 Conclusions

299 For each change the developer SHALL report if the impact on assurance is considered minor or major.

300 For each change the developer should provide a supporting rationale for the reported impact.

301 The developer should include a supporting rationale, taking the culmination of changes into consideration.

D.6 Annex: Updated evaluation evidence

302 The developer SHALL report for each updated item of evaluation evidence the following information:

- -the title;
- -the unique reference (e.g. issue date and version number).

303 Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the TOE, then it does not need to be included.