Swedish Certification Body for IT Security

002 Evaluation and Certification

Issue: 27.0, 2017-Nov-01

Authorisation: Mats Engquist, Quality 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. It 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 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 Terminology

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 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 PP, resulting in an internationally recognised certificate.

8 The CB 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 has a defined target of evaluation (TOE) on which the evaluation is targeted.

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

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. Procedures for re-evaluation are described in SP-003 *Assurance continuity*.

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

2.2 Principles of Evaluation

12 The evaluation and certification process is designed to achieve appropriateness, impartiality, objectivity, repeatability, reproducibility, generation of sound results, cost-effectiveness, and re-usability.

13 The principles of evaluation are as follows.

- All parties involved in an evaluation SHALL perform their required tasks to a degree of rigour 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 TOE or PP being evaluated. Proper technical oversight coupled with a Scheme that eliminates conflicts of interest SHOULD reduce any residual bias to a nominal level.
- 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 TOE or PP. The evaluation process and results SHOULD be subject to technical oversight to ensure that the requirements of the CC, the Common Methodology (CEM), and the Scheme are met.
- A balance SHOULD continually be maintained between value, and expenditure of time and resources in the evaluation of TOEs and PPs.

- The results of evaluating a TOE or PP, and the interpretations that arise in the course of the evaluation, SHOULD be useful in subsequent evaluations if the same conditions apply.

14 These principles are upheld by:

- using the CC, which provides a well-defined set of security requirements;
- using the CEM when assessing an IT product or a PP against the requirements; and
- implementing the evaluation and certification process defined by the Scheme.

2.3 Requirements for Certification

15 The Requirements for Certification are described in the following documents.

- The CC, and the CEM
- Supporting Documents authorised through the Common Criteria Recognition Arrangement (CCRA) and/or the Senior Officials Group, Information Systems Security - Mutual Recognition Agreement (SOG-IS MRA)
- International Interpretations
- The Scheme documentation

16 Procedures for introducing changes to the Requirements for Certification are described in In SP-007 *Quality Manual*.

2.4 Standard versions

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

18 Final decision about which version is used in a Certification, and thus presented on the certificate and on the CR, is made when the CB makes the decision on certification.

19 Unless otherwise agreed with the Sponsor, the versions used should be the versions valid at the time of the Final Evaluation Report (FER).

20 If the valid versions have been updated during the evaluation and certification; an impact analysis may have to be performed, and parts of the evaluation may have to be updated.

21 If the impact is 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.

2.5 Evaluation and Certification Process

22 The generic evaluation process has three distinct phases as follows, which are explained in detail below.

1. Start-of-evaluation	The four parties involved in the evaluation and certification (Developer, Sponsor, ITSEF, and CB) prepare for evaluation.
2. Conduct of evaluation	The evaluation is performed.
3. Conclusion of evaluation	The evaluation is completed.

2.5.1 Start-of-evaluation

23 The start-of-evaluation phase includes any activities relevant to the upcoming evaluation, including the following.

24 It is recommended that the ITSEF conduct a feasibility study before accepting the evaluation. The sponsor MAY provide the ST or PP, and possibly other evaluation evidence, to the evaluator so that the evaluator may determine the likelihood of a successful evaluation and the possible cost.

25 If the Sponsor decides to seek certification of the PP or IT product, the Sponsor contracts with an ITSEF to perform the evaluation and applies for certification with the CB.

26 The Sponsor submits a signed application for certification to the CB, including several documents, which together demonstrate readiness for the evaluation and certification process, and acceptance of the Sponsor responsibilities described in section 3, *Parties and Responsibilities*. The necessary documents may vary depending on the evaluation type.

27 The CB performs an Application Review, including all attached documents, after which it decides whether to undertake, or decline, the Certification. If the decision is to undertake the certification a Certification Agreement is established according to the procedures described in section 4.3.1, *Certification Agreement*.

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

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

30 For more detail on the Start-of-evaluation phase see section 4, *Start-of-evaluation*.

2.5.2 Conduct of Evaluation

31 After the CB has approved the application, the evaluation may start. The evaluators will carry out the evaluation in accordance with the agreed EWP. Usually the evaluator begins with evaluation of the ST and then performs the evaluator actions as described in the CEM for the targeted evaluation assurance level, i.e., investigating the TOE, the development environment, etc.

32 During the conduct of evaluation phase, the Developer submits evaluation evidence to the evaluator at the ITSEF. The evaluator uses the CEM 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.

33 Thereafter the evaluation approach and results are documented in a single evaluation reports (SERs). The SERs are submitted to the certifier at the CB, together with the Evaluation evidence. The format and required content of the reports is described in Scheme publication SP-002 *Evaluation and Certification*. Copies of the SERs are distributed to the Sponsor and to the Developer.

34 The evaluation work is divided into several parts, resulting in a series of SERs. For each SER, 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 SER, preferably after the evaluation evidence has been updated, and submitting the changed documents to the certifier. The process may be iterated.

35 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.

36 During the whole process, the CB oversees the evaluation, supports the evaluation as requested by the evaluator, and responds to each evaluation report with a TOR.

37 For more detail on the Conduct of Evaluation phase see section 5, *Conduct of Evaluation*.

2.5.3 Conclusion of Evaluation

38 After the evaluators have assessed all necessary topics, all necessary SERs have been produced, and the CB has reviewed and accepted them all, the conclusion of evaluation phase begins. The evaluator produces a FER summarising all the findings and submits it to the CB. The CB assesses the FER, produces and publishes the CR, and issues the certificate to the Sponsor. The CR and the certificate itself will be issued in English, but can be issued in Swedish upon the Sponsor’s request.

39 For an evaluation of a PP a final evaluation report (FER) is not necessary. In this case the CR is based on SER APE.

40 The CB also exercises control over the use of the certificates issued. This is described in section 7.2, *Certificate Misuse.*

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

42 For more detail on the Conclusion of Evaluation phase see section 6, *Conclusion of Evaluation*.

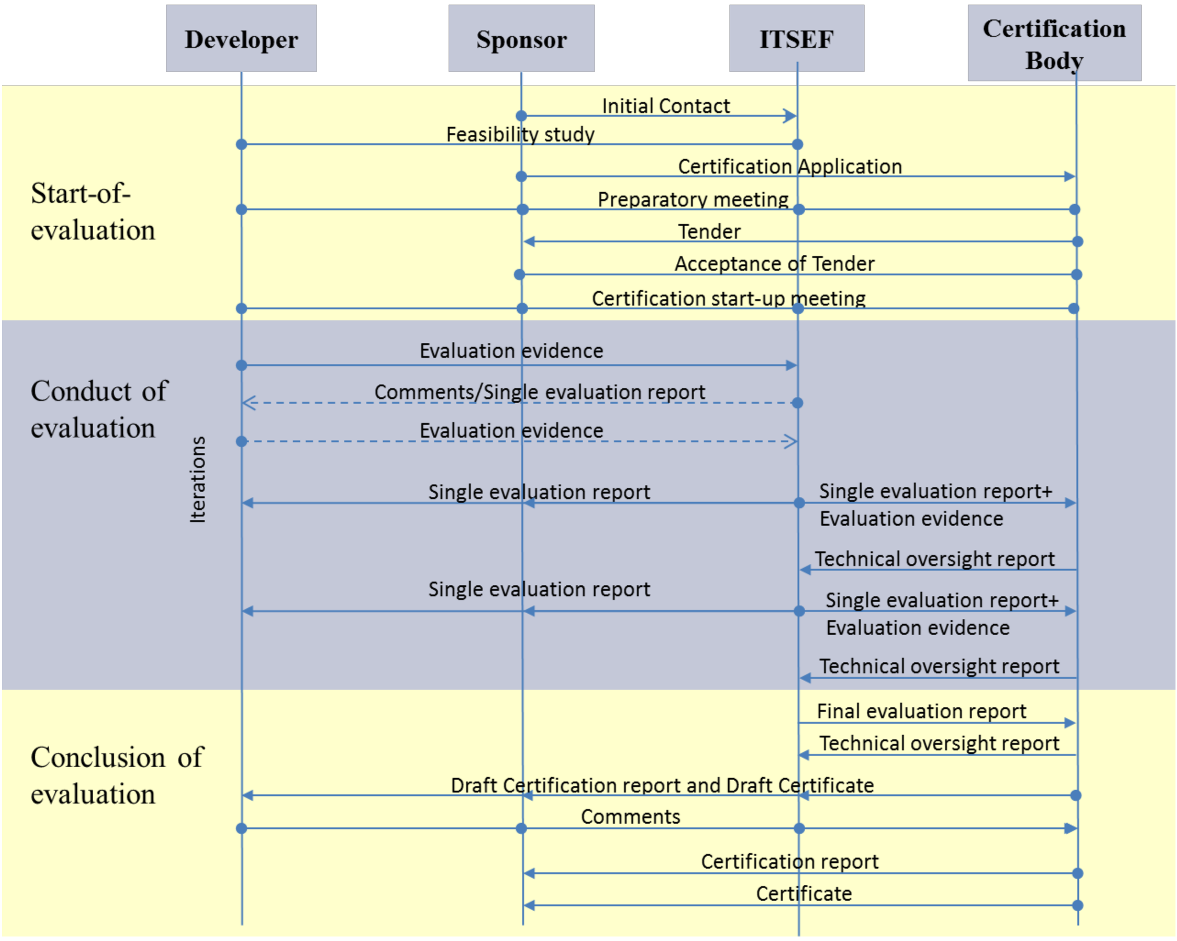

Figure 1 shows the four parties involved in the evaluation and certification process (Sponsor, Developer, ITSEF, and CB), the phases of the process, and a simplified document delivery sequence.

2.6 Cross Frontier Evaluation

43 Evaluations where work is performed in locations situated outside Sweden are subject to the regulations in SP-191 *Cross Frontier Evaluation*. Some Evaluation activities are required to be performed at a Swedish site, designated as a Critical Location, or at the Developer site, whereas other activities may be performed at a Foreign Location covered by the ITSEF license, subject to approval by the Sponsor and the Developer.

2.7 Official Languages of the Scheme

44 Evaluation reports, oversight reports, and CRs may be written in Swedish or English.

45 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 CB.

2.8 Management of Confidential Information

46 Documents received or drawn up by the CB are official documents (“*allmän handling*”) and may be kept secret by the CB 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; and
- the protection of the personal or economic circumstances of private subjects.

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

3 Parties and Responsibilities

48 All parties involved in the evaluation and certification shall fulfil their roles and responsibilities as defined by the CC, the CEM, 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

49 The Sponsor is the organisation that funds the evaluation and certification, applies to the CB for certification, contracts with the ITSEF, and arranges for Developer participation. The Sponsor and the Developer may be the same.

50 The Sponsor SHALL have formal agreements with:

- the ITSEF for the evaluation, and
- the CB for the certification.

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

52 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.

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

54 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, including invoices and the certificate.

55 The Sponsor SHOULD assign a point of contact for external communication related to the evaluation and certification. The Sponsor SHALL ensure that the CB is notified of any changes to the point of contact.

56 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 CB to perform evaluation or certification activities.

57 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.

58 The archived material SHALL be made available to CSEC at request within seven working days.

3.2 Developer

59 The Developer is the organisation that produces the TOE. 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.

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

61 The Developer SHALL:

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

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

3.3 ITSEF

63 The ITSEF is the organisation contracted to perform the evaluation. It is responsible for ensuring that the assessment performed is consistent with the CC, the CEM, and the Scheme.

64 An ITSEF must adhere to the following requirements.

- Observe all rules of the Scheme as laid down in the Scheme documentation and interpreted by the CB
- Be accredited by an authorised accreditation body, in accordance with ISO/IEC 17025 (formerly, ISO Guide 25) or be directly appointed by the government
- Ensure that the status of each of its individual evaluators is recognised by the CB
- Keep the CB informed about the progress of ongoing evaluations and about any changes that might influence its ability to fulfil the requirements of the Scheme

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

66 The ITSEF and the CB must be independent organisations.

67 The evaluator is associated with an ITSEF and performs the assessment of the TOE. The evaluator provides the CB with evaluation reports containing findings and verdicts, such as SERs and FERs.

68 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 CB by achieving the status of Evaluator or Qualified Evaluator. For further information about the procedures for ITSEF licensing and evaluator status achievement, see Scheme publication SP-004 *Licensing of Evaluation Facilities*.

69 The evaluator SHALL:

- comply with the principles of evaluation (see section 2.2, *Principles of Evaluation*) and the Scheme;
- determine which supporting documents (CCRA and SOG-IS MRA) that are applicable to the evaluation and use them accordingly;
- perform the evaluator actions required by the EAL; CC for Information Technology Security Evaluation, Part 3: *Security assurance requirements;* the CEM; and the Scheme;
- request evidence from the Sponsor or Developer and receive and safely store it, e.g., documentation, the Security Target (ST), and the TOE;

- perform the site visits required by the Scheme and the CEM;
- request and receive evaluation support as needed, e.g., TOE 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; and
- document and justify the overall verdict and interim verdicts to the certifier.

70 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.

71 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, and
- assign a Lead Evaluator who SHOULD be technically responsible for the evaluation.

72 If necessary, the ITSEF SHOULD augment the evaluation team with internal or external technical experts.

73 The individual evaluator/evaluation team SHALL be technically competent for the assigned evaluation activities. The Lead Evaluator SHOULD ensure that personnel with the appropriate competencies are assigned for each evaluation activity. Note that an individual evaluator can be both the point of contact and the Lead Evaluator for an evaluation.

74 The Lead Evaluator SHOULD be a Qualified Evaluator. For more information, see Scheme publication SP-004 *Licensing of Evaluation Facilities*.

3.4 Certification Body (CB)

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

76 The certifier oversees an evaluation by reviewing the evaluation reports produced by the evaluator. The result is documented in TORs.

77 Witnessing the evaluator's site visits at the Developer site is added for EAL3 or higher, unless otherwise decided. The certifier may also witness the testing of the product.

78 The certifier also provides support to the evaluator regarding Scheme matters, interpretations of the CC, etc.

79 To ensure uniform application of the CC, the CB 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 CC certificates. The use of publicly available interpretations to document clarifying statements made by the CB is aimed at ensuring consistent and uniform use of the CC and the Scheme rules.

80 The certifier will:

- perform technical oversight of evaluations;
- receive and review evaluation evidence and evaluation reports;
- provide oversight deliverables, e.g., TORs;

- support evaluations by providing Scheme and CC interpretations and guidance;
- disapprove the evaluator's overall verdict and interim verdicts if they are not well-founded or not appropriate;
- document and justify the findings from the oversight; and
- document the certification results in a CR, and issue a certificate.

81 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.

82 The CB shall create conditions that ensure that evaluations conform to:

- the principles of evaluation (see section 2.2, *Principles of Evaluation*),
- the CC,
- the CEM, and
- the Scheme.

83 For each certification, the CB will:

- assign one certifier to be the certification point of contact, and
- assign a Lead Certifier to be technically responsible for the certification.

84 The individual certifier shall be technically competent to perform the assigned certification activities. The Lead Certifier will ensure that personnel with the appropriate competencies are assigned for each certification activity.

4 Start-of-evaluation

4.1 Overview

85 The start-of-evaluation phase begins with the Sponsor contacting an ITSEF to initiate an evaluation of a TOE or PP. 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 CB.

86 A Preparatory Meeting may be held with all parties involved in the evaluation and certification, where the CB describes the evaluation and certification process, and questions are addressed.

87 The CB decides whether to approve the application. If approved, the CB submits a Tender based on the complexity class and the EAL-level of the product to be certified. This Tender must be accepted in writing by the Sponsor, which brings the formal agreement to a conclusion.

88 Prior to the start of the actual evaluation and certification, a Certification Startup Meeting is held with all parties involved. The Certification Startup Meeting follows a formal agenda.

4.2 Feasibility Study

89 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*.

90 After an initial contact between the Sponsor and the ITSEF, the Sponsor MAY provide the ST or the PP, and possibly other evaluation evidence, in draft or completed form to the ITSEF.

91 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.

92 The ITSEF MAY inform the CB 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 CB can formulate appropriate resource plans in preparation for certifier activities during the start-of-evaluation phase.

93 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

94 The Sponsor or the ITSEF on behalf of the Sponsor SHALL submit the following documents to the CB.

- An application for certification using Scheme publication SP-196 *Certification Application with Terms - Form* (Or SP-199 *Certification Application with Terms (FMV) - Form*, for customers within FMV). The Sponsor SHALL sign the application for certification.
- The ST or PP.
- An evaluation work plan (EWP)
- All documents referenced in the ST or PP which are not publically available

95 Other appendices may be added as needed.

96 An evaluator impartiality and independence justification may, if required, be added as an appendix to the Application, or presented at the Certification Start-up meeting.

97 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 CB in a finalised version or in a draft version that meets the requirements of the certification review process.

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

99 An Application for certification is valid one year from the date it is received by the CB.

100 By signing the application the Sponsor commits to the following, which are a part of the formal agreement (see section 4.3.1 *Certification Agreement*):

- to fulfil the requirements for certification, including implementing appropriate changes when they are communicated by the CB;
- to make all necessary arrangements for the conduct of the evaluation and certification, including provision for examining documentation and records, and access to the relevant equipment, location(s), area(s) and personnel;
- in case the Sponsor is not the Developer:
  - to ensure the Developer's co-operation in the fulfilment of these requirements;
- to make claims regarding certification consistent with the scope of certification;
- not to use its product certification in such a manner as to bring the CB into dispute and not to make any statement regarding its product certification which the CB may consider misleading or unauthorized;
- to comply with any requirements that may be prescribed in the product certification scheme that relate to the use of marks of conformity, and on information related to the product;
- to inform the CB, without delay, of changes that may affect its ability to conform with the certification requirements; and
- to archive the evaluated product in its certified configurations and all Developer evidence as outlined in the configuration list which is valid at the end of the certification procedure for a time frame of 5 years.

101 The Sponsor agrees that the CB archives all evidence provided, as well as the CB's internal files, based on the scheme regulation for archiving.

102 The Sponsor agrees to all responsibilities defined in the Scheme.

103 In addition, for evaluations at EAL 2 and above and for which the Sponsor and the Developer are different organisations, the Developer SHOULD agree in writing 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, and
- responsibilities after a completed evaluation and certification.

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

105 The Sponsor-ITSEF evaluation agreement SHOULD cover:

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

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

4.3.1 Certification Agreement

107 According to the rules and regulations for accreditation the CB is required to have a legally enforceable Agreement for the provision of certification activities to its clients.

108 This Agreement is established as follows.

1. The Sponsor signs and submits an Application for Certification to the CB, and thereby accepts compliance with the client's responsibilities, as defined in section 4.3, *Application for Certification*.
2. The CB decides the fees for the certification depending on the complexity of the product to be certified and the EAL, and sends a Tender to the Sponsor.
3. The Sponsor sends a letter of acceptance of the fee and the terms of the Tender, in writing, to the CB.

109 These three documents together form the Certification Agreement.

4.3.2 Security Target (ST) or Protection Profile (PP)

110 The ST or the PP 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 from starting.

111 The quality of the ST or PP is of the utmost importance for the subsequent evaluation and certification.

112 A submitted ST or PP SHOULD fulfil the following requirements.

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

113 The ST must be clear and consistent. Clarifications on requirements on the ST are described in Scheme Note 18, *Highlighted Requirements on the Security Target*. It is recommended that these be taken into account as early as possible in the certification project.

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

4.3.3 Evaluation Work Plan (EWP)

115 The ITSEF SHOULD, together with the Sponsor, produce an EWP based on information gained during the feasibility study. The EWP SHALL describe the schedule for the evaluation and the locations in which each evaluation activity will be carried out.

116 The EWP SHALL meet the requirements stated in Appendix A, Evaluation Work Plan; that is, the EWP shall be reasonable in terms of time, cost, and fulfilment of the CC, the CEM, and the Scheme.

117 At a minimum, the EWP SHALL cover the following.

- Resources
- Competence and training of the resources
- Parallel evaluation activities
- Evaluation evidence deliverances
- Dependencies between evaluation activities

118 The evaluator SHALL present to the CB 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, Evaluation Work Plan. The detailed description can be documented as a part of the EWP, or as a separate document.

119 If the evaluation covers new evaluation areas, like new versions of the CC and the CEM, 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.

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

4.3.4 Evaluator Impartiality and Independence Justification

121 An evaluator impartiality and independence justification SHALL be submitted with the Application or brought to the Certification Start-up 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.

122 When members of the ITSEF have been involved in consulting 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 consulting and those conducting the evaluation.

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

124 If there are no specific circumstances as described above, the evaluator MAY omit an evaluator impartiality and independence justification. This may, for example, be discussed with the CB during the Preparatory Meeting.

4.4 Certification Application Review

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

126 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.

127 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 section and the relevant appendices.

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

129 The certifier shall determine that there are no obvious deficiencies preventing the certification from resulting in a certificate and a CR.

130 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 EWP with fulfilment of the CC, the CEM, and the Scheme. However, the certifier shall not be held responsible for the comprehensiveness of this reporting and of other issues that might be discovered later.

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

4.5 Handling of the Certification Application

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

133 The CB will ensure that the ITSEF and the Developer has signed security agreements, "*säkerhetsskyddsavtal, SUA*", with the appropriate Swedish governmental organisation if information regarding national security or foreign relations is likely to be handled during the certification. The CB will also ensure that the evaluators and developers have security clearance at an appropriate level.

134 For EAL 2 and above, the CB 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.

135 Upon completion of the certification application analysis and resolution of any issues raised, e.g., at the Certification Start-up meeting, the CB will assess whether there are any obstacles to performing the certification.

136 The versions of the CC, the CEM, and interpretations to be used during the evaluation will be defined. The versions and interpretations should be the official versions and all published interpretations listed on the CC project website, www.commoncriteriaportal.org, at the time of the submission of the certification application. The Sponsor SHALL ensure that the ST or PP is consistent with this decision.

137 The CB will assign a Lead Certifier and other certifiers as needed depending on the complexity of the evaluation. The certifiers are responsible for conducting technical oversight of the evaluation activities carried out by the evaluator.

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

4.6 Certification Start-up Meeting

139 A Certification Startup Meeting SHALL take place during the start-of-evaluation phase when the certification application is complete and the certification is to begin.

140 Prior to this a Preparatory Meeting MAY be held.

141 The Certification Startup Meeting MAY be performed at the CB, at the ITSEF, or at the Developer Site.

142 In case the evaluation includes activities performed at Foreign Locations, there are specific instructions for the Start-up meeting in Scheme publication SP-191 *Cross Frontier Evaluation*.

143 The CB, Sponsor, ITSEF, and for EAL 2 and above the Developer, SHOULD be represented at the Certification Start-up 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 Certification Start-up meeting.

144 The Certification Startup Meeting SHOULD provide the CB with some familiarity with the PP or TOE and its evaluation evidence. This should give the CB an understanding of the context and complexity of the evaluation, so that the CB can provide accurate and timely guidance or interpretations.

145 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.

146 Potential problems and all clarification requests related to the evaluation and certification SHOULD be brought up for discussion during the Certification Start-up meeting.

147 The Sponsor or the Developer SHALL, on request by the CB, provide a presentation on the TOE or PP. The Sponsor and the Developer SHALL be prepared to answer questions about the TOE or PP. Note that the questions can cover anything from development procedures to low-level technical details.

148 The ITSEF SHALL be prepared to account for the EWP and SHOULD be prepared for questions regarding time schedule and project risks during the Certification Start-up meeting.

149 The ITSEF SHALL be prepared to justify evaluator assignments in the EWP based on technical skill requirements, the TOE technology, and the methods and techniques needed to test the TOE. This justification is especially important if the evaluators have no previous experience with the specified EAL or with the type of TOE.

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

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

152 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 section 4.3, *Application for Certification*.

153 If the evaluation is a trial evaluation, the CB will inform all parties about 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.

4.7 Certifier Project Planning

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

5 Conduct of Evaluation

5.1 Overview

155 The conduct of evaluation phase can begin when the preparation work in the Start-of-evaluation phase is finished. 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 SERs are completed by the evaluator and accepted by the certifier.

5.2 Sponsor and Developer Activities

156 The Sponsor and/or the Developer SHALL provide the ITSEF and the CB with evaluation evidence.

157 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.

5.3 Evaluator Activities

158 The evaluator SHALL generate evaluation reports; perform CEM work units; conduct site visits and independent testing, etc.; all in accordance with the CC, the CEM, relevant interpretations, and the Scheme.

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

5.3.1 Evaluation Report Generation

160 The evaluator SHALL document, in SERs with supporting justification, the interim verdicts of all CC evaluator actions performed in accordance with the CEM. A SER covers a subset of all assurance packages for the evaluation.

161 The recommendation is to cover no more than one assurance class in each SER. 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 SER, especially for higher EALs.

162 The evaluator SHALL produce SERs using the evaluation evidence provided by the Sponsor and/or Developer. The structure and content requirements of the SERs are detailed in Appendix B, Single Evaluation Report (SER).

163 For a TOE, a separate SER SHALL be written for the ASE assurance class and, in the case of a PP evaluation, an APE assurance class SER SHALL be written. An ASE or APE SER MAY be divided into multiple assurance family SERs if the evaluator finds it suitable.

164 The SERs SHALL be submitted to the CB for the certifier's technical oversight.

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

166 The ASE class SHOULD be the first assurance activity conducted. The ST 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.

167 Due to the importance of the ST the CB has chosen to highlight the importance of some important requirements on this document. These requirements may be found in Scheme Note 18 *Highlighted Requirements on the Security Target*.

168 The ST evaluation SHOULD be reported in a SER before other TOE activities begin. The ST SER remains provisionally complete until the TOE is complete. Findings during the evaluation may necessitate changes to the ST, impacting the previous ST evaluation results and possibly requiring a renewed ST evaluation.

169 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 evaluation require changes to the evaluation evidence. Reassessment results are captured in an updated SER. Note that every dependent work unit SHALL either be reassessed or a sufficient justification SHALL be given as to why reassessment is not necessary.

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

171 If the TOR 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 SER and any evaluation evidence. This SHALL be documented in a separate document submitted with the updated SER, if applicable.

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

- after the SER for ASE and
- after the SER for ADV but before testing.

173 For an evaluation of a PP a final evaluation report (FER) is not necessary and the SER for APE will therefore be used as an input for writing the CR instead of the FER.

5.3.2 Site Visit Assessment

174 The purpose of site visits at the Developer site is to determine whether the procedures described in the Developer documentation are followed. Site visits SHOULD be performed for evaluations at EAL 3 and above, as required by the CC. The CEM identifies the assurance families for which site visits are applicable or required: ALC_CMC.3 (or higher), ALC_DEL and ALC_DVS.

175 The decision not to perform a site visit is subject to certifier approval. The evaluator SHALL produce a separate document detailing a site visit plan for site visits planned in the EWP. The site visit plan SHALL demonstrate how the evaluator plans to conduct the site visit.

176

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

178 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 SERs covering work units related to site visits.

5.3.3 Re-use of Site Visit Assessment Results

179 For new evaluations, where site visits recently have been performed in another evaluation, the following additional rules may apply.

180 If no substantial changes have been done to security relevant parts of the developers procedures, within a time period of 18 months, and if there are no further relevant sites to visit, apart from those already covered, the evaluator MAY provide a rationale explaining why a renewed site visit is not necessary. Based on this rationale, the certifier MAY conclude that a site visit is not necessary.

181 A site visit may be necessary if:

- due to sampling, all relevant sites have not already been visited
- in the new ST, the new TOE has dependencies on the development environment that has not been completely covered in the previous assessment

5.4 Certifier Activities

182 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 (only applicable to EAL 3 or higher, unless otherwise decided.), and
- participating in the evaluator testing activities.

183 The certifier will perform oversight and deliver TORs, according to the EWP and the agreed time plan.

5.4.1 Single Evaluation Report (SER) Technical Oversight

184 The certifier will examine all SERs to determine whether they are technically sound and consistent with the requirements of the CC, the CEM, the relevant interpretations, and the Scheme. The SER content and structure requirements are defined in Appendix B, Single Evaluation Report (SER).

185 The certifier will examine the SERs to verify the evaluation conclusions and the analysis supporting those conclusions. The certifier can use the evaluation evidence to verify the evaluator conclusions.

186 The result of the examination of an evaluation report is documented in a TOR produced by the certifier and sent to the evaluator. The TOR 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.

187 When an issue is resolved in an updated evaluation report the certifier will close it by stating "No further comments" in the TOR.

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

189 The certifier will ensure that TORs are made available to the Sponsor and/or Developer in case Sponsor or Developer actions are required.

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

191 The evaluator SHALL update the SER if work units are reworked and/or respond to the certifier's comments by written statements in the TOR. The certifier will review updated SERs and consider evaluator statements in the returned TOR, and issue a new or updated TOR.

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

- after the SER for ASE and
- after the SER for ADV but before testing.

5.4.2 Site Visit Oversight

193 The certifier may attend site visits performed by the evaluator. Site Visit oversight is performed at EAL 3 and above, unless otherwise decided. The purpose is for the certifier to observe the evaluator actions.

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

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

196 The certifier will document observations accumulated during the site visit assessment in an internal report. 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 SERs covering work units related to site visits. The certifier will report issues, remaining from the site visit, in the TORs corresponding to those SERs.

197 As long as the developer sites, the product type, and the evaluator performing the site visit are familiar to CSEC, the certifier MAY decide that no site visit oversight will be necessary.

5.4.3 Testing Oversight

198 The certifier will observe evaluator actions such as independent testing and penetration testing. Witnessing the evaluator's testing is added for EAL3 and above, unless otherwise decided. Evaluator oversight provides the certifier with an opportunity to verify the evaluator's conformance to the CC and the CEM.

199 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.

200 The certifier will document observations accumulated during the testing oversight in an internal report. The observations will be used to verify the evaluator's reports (SERs), which document the outcome of the tests. The certifier will report issues, remaining from the testing oversight, in the TORs corresponding to those SERs.

6 Conclusion of Evaluation

6.1 Overview

201 The conclusion phase starts when all SERs have been completed and all the certifier's comments on the SERs have been closed.

202 The evaluator will produce the FER, which will be used as an input for writing the CR.

203 For PP evaluations the FER is not necessary, instead the SER for APE will be used as input.

204 This phase will end with the CB issuing, and possibly publishing, the certificate and a CR.

6.2 Final Evaluation Report (FER) Production

205 The FER reports on all evaluation activities in all SERs, covering both the ST evaluation and the TOE evaluation. The objective of the FER is to provide information necessary to produce the CR, which provides practical information about the TOE to the consumer.

206 The evaluator SHALL produce the FER, which SHALL be based on the full set of accepted SERs, by compiling relevant information. For PP evaluations the FER is not necessary if the SER (APE) contains the necessary information instead of the FER.

207 The evaluator's result is documented with an overall verdict in the FER. The overall verdict is defined in the CEM and shall be either PASS or FAIL.

208 The content and structure of the FER SHOULD conform to Appendix C, Final Evaluation Report (FER). The information content requirements are driven by the requirements stated in the CEM, and Scheme-specific requirements.

209 The FER SHALL include detailed information about the evaluation. This may be achieved by referencing the SERs.

210 With the exception of the detailed information, the FER SHALL provide the information necessary to produce the CR and SHOULD be free of any information that is not suited to be copied into the CR. The FER MAY fulfil the information content requirements by reference.

211 The evaluator SHOULD send the FER to the Sponsor and/or Developer for review prior to submission to the certifier. This review is especially important for certifications that will be subject to mutual recognition. The Sponsor and/or Developer review SHOULD ensure that the FER can be used for the generation of the CR.

212 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.

213 The individual SERs, especially the ST SER, are not technically complete until the evaluation is complete; therefore, if needed, SERs SHOULD be updated.

6.3 Final Evaluation Report (FER) Review

214 The certifier will examine the FER to determine that the requirements for information content and structure are satisfied. The correctness and completeness of the FER is important, as this document is the basis for the CR.

215 The certifier will always generate a TOR in answer to the FER.

216 The TOR identifies issues and requests clarifications regarding the FER, and will be sent to the evaluator. The evaluator may have to update one or more SERs to resolve the issues found during the FER examination.

217 Issues reported in the TOR might require evaluator, Sponsor, and/or Developer actions; if necessary, an updated FER and possibly updated SERs and evaluation evidence SHALL be produced and submitted to the CB.

218 If the TOR 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 FER, and possibly SERs, and evaluation evidence. This response SHALL be documented in a separate document submitted with the updated FER, if applicable.

219 If the conclusion is that that there is a need for major changes to a SER, 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 (CR) Preparation

220 When there are no further comments on the FER (see section 6.3 *Final Evaluation Report (FER) Review*), the certifier will produce a CR. The certifier will use the FER as the basis for the CR.

221 For PP certifications the certifier will use the SER for APE as the basis for the CR.

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

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

224 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

225 The final version of the CR will be distributed to the Sponsor.

226 A certificate may be issued when the overall verdict for an evaluation is PASS and when the requirements for certification, as stated in the Scheme, are fulfilled.

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

228 A ST or PP that is certified, and should be internationally recognised, will be registered. The registration is the publication of the ST or PP, and the registration identifier is the certification ID.

6.6 Project Cleanup and Closedown

229 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.

230 The CB will archive the reference material needed to demonstrate the certification results and how the certification was performed.

7 After a Certificate has been Granted

7.1 Duration and Validity of a Certificate

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

232 For as long as the certificate is valid the Sponsor SHALL keep a reference copy of the TOE.

233 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 CB 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

234 The period of validity is agreed between the Sponsor and the CB. During the period of validity, the certificate will be surveiled on a yearly basis to ensure that the Sponsor fulfils its obligations.

7.2 Certificate Misuse

235 The CB exercises control over the use of associated trademarks and issued certificates.

236 The CB 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.

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

238 The CB will withdraw certificates in cases where the conditions for holding a certificate no longer apply.

7.3 Certificate Surveillance

239 After a successful certification the Sponsor and the CB can agree on surveillance of the certificate.

240 The surveillance period is agreed between the Sponsor and the CB. The recommended period is five years.

241 During this period the Sponsor SHALL fulfil the requirements for validity of the certificate described in section 7.1 *Duration and Validity of a Certificate*.

242 The CB will perform surveillance activities to ensure that the conditions for the validity of the certificate are continuously satisfied.

243 The surveillance can be performed in different ways: Planned inspection, Unannounced inspection or Self-declaration by the Sponsor.

Planned inspection

244 The CB performs a planned and announced Site Visit at the Sponsor's premises and conducts the inspection. This is the normal way to perform the surveillance during the first year of the surveillance period.

Unannounced inspection

245 The CB performs an announced Site Visit at the Sponsor's premises and conducts the inspection. Unannounced inspections may also be carried out on suspicion that the Sponsor does not fulfil its obligations.

Self-declaration by the Sponsor

246 The Sponsor makes a self-declaration and sends it to the CB. This will be the yearly procedure after the Site Visit performed during the first year.

8 Supporting Processes

8.1 Observation Report Handling

247 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.

248 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 EWP
- exploitable vulnerabilities, or incomplete or inaccurate evaluation evidence, leading to a potential evaluation failure
- unexpected delays to the evaluation work plan.

249 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 CB.

250 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

251 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.

252 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 marks and one with change marks indicating all changes since the previous version. The version without change marks will have precedence.

Appendix A Evaluation Work Plan

A.1 Overview

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

254 The evaluator SHALL present a detailed evaluation description to the CB. This SHALL be a part of the EWP or a separate document. At the end of this appendix are the requirements for the detailed evaluation description.

255 There are no requirements for the EWP structure. The requirement sections below groups similar requirements together.

A.2 General Requirements

256 The EWP SHALL demonstrate to the CB that the plan is reasonable in terms of time, cost, and fulfilment of the CC, the CEM, and the Scheme. Typical areas of interest are: resources, resources’ competence and training, parallel evaluation activities, evaluation evidence deliverances, and dependencies between evaluation activities.

257 The EWP 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 PP or target of evaluation, Developer, Sponsor, ITSEF, and the PP or TOE version number.

258 The EWP 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

259 The EWP SHALL address all CEM general evaluation tasks, activities, and sub-activities matching the assurance requirements expressed in the ST.

260 The EWP SHALL address the production of the SERs and the FER, 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 EWP with the input section for each CEM sub-activity for the corresponding assurance requirements, to verify that there are no evaluation evidence items missing from the EWP.

261 The EWP 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

262 The EWP 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.

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

264 For an evaluation at EAL 3 and above, the EWP SHALL schedule the evaluator's site-visit(s) at the Developer facility or facilities. For EAL3 and above, the CB will also perform site-visits, i.e., Testing Oversight (a site-visit at the ITSEF or Developer site during independent and penetration testing) and site-visit (witnessing the evaluator's site-visit at the Developer site), unless otherwise decided.

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

266 The evaluator's test plan and vulnerability analysis, together with the Developer's test report SHALL be delivered to the CB at least five working days prior to the evaluator's independent and penetration testing.

267 The EWP SHALL identify planned meetings between the evaluator and the Sponsor, certifier, or Developer.

268 The EWP 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.

269 Note that the SER SHOULD only be sent to the CB when all the verdict in the SER is PASS or when there are unsolved FAIL or INCONCLUSIVE verdicts that require special attention from the certifier.

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

A.5 Evaluation Staffing

271 The EWP SHALL identify the individual evaluators assigned to each evaluation report, so that the certifier can verify the following.

- The CEM 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 Evaluation Locations

272 The EWP shall denote the location where each evaluation activity is performed.

273 Unless otherwise has been agreed with the CB, evaluator testing activities associated with ATE and AVA SHALL be performed at a Critical Location or at the Developer site. (See SP-191 *Cross Frontier Evaluation*.)

274 Unless otherwise has been agreed with the CB, the Certification Startup Meeting SHALL be held at a Critical Location, at the CB, or at the Developer site.

275 Evaluation activities SHOULD be restricted to the Critical Location, the Foreign Location, and the Developer site.

A.7 Detailed Evaluation Description

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

277 The evaluator SHALL demonstrate to the CB 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.

278 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.

279 The evaluator SHALL demonstrate to the CB that the evaluator recognises and has considered the increasing evaluation work complexity as the EAL increases. This applies to all evaluation work including work units that are consistent across all EALs.

Appendix B Single Evaluation Report (SER)

B.1 Overview

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

B.1.1 Protection Profile (PP) Evaluation

281 For PP evaluations the SER is used without a FER and therefore the SER must provide information necessary to produce the CR.

B.2 Structure and Information Content

282 The following requirements apply to a SER 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
- CB name
- Certification ID
- Lead Evaluator name
- Appropriate protective markings

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

- Certification ID
- Appropriate protective markings
- Page number

284 The SER SHOULD be structured by the following section headings.

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

285 The content requirements SHOULD be met in the sections included in the SER. The SER MAY include additional sections, structured as appropriate, complying with the SER purpose.

286 The information content requirements follow.

B.2.1 Evaluation Basis and Documents

287 The evaluation basis SHALL identify the following.

- CC version

- Evaluation methodology
- ST

288 The evaluation basis SHALL also identify the following.

- Relevant Scheme documents
- Interpretations considered for this SER
- Sponsor and/or Developer documents provided for the evaluation aspects addressed in this SER

B.2.2 Objectives and Dependencies

289 The objectives for this assurance class or assurance family SHOULD be identified and described, including the following.

- EAL
- Dependencies taken into account during the evaluation

B.2.3 Evaluation Evidence and Work Units

290 This section SHOULD identify the following.

- Evaluator action elements
- Content and presentation of evaluation evidence elements
- Applicable work units

291 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

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

- the assurance class,
- the assurance components, and
- the evaluator action elements.

293 For each evaluation action element, or for each work unit where applicable, the evaluation result section SHALL provide the following.

- 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

294 The SER 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 SER
- Impact on other documents identified during this evaluation

B.2.5 References

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

296 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 20.0, CSEC, 2013-09-30, FMV ID 13FMV7990-2:1.

B.2.6 Abbreviations and Glossary

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

Appendix C Final Evaluation Report (FER)

C.1 Overview

298 The FER covers all evaluation activities in all SERs. The objective of the FER is to provide the overall verdict with justification, and to provide information necessary to produce the CR.

299 The Evaluation section in the FER contains detailed information about the evaluation. The Results of the Evaluation section contains references to the SERs. A brief summary of the evaluation results is given in the Executive Summary.

300 With the exception of the detailed evaluation information mentioned above, the FER should not contain information not suited to be copied into the CR.

C.2 Structure and Information Content

301 The following requirements apply to the FER in general. At a minimum, the cover page SHOULD contain the following information.

- Document title
- Version number
- File name
- Product name
- Sponsor name
- ITSEF name
- CB name
- Certification ID
- Lead Evaluator name
- Appropriate protective markings

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

- Certification ID
- Appropriate protective markings
- Page number

303 The FER SHOULD be structured by the following section headings.

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

304 The content requirements SHOULD be met in the sections included in the FER. The FER MAY include additional sections, structured as appropriate, providing they comply with the FER purpose.

305 In the case of a PP evaluation, the same structure SHOULD be used; however, non-relevant sections SHOULD be marked “Not applicable” or be omitted.

306 The FER content requirements are described in the following sections.

C.2.1 Executive Summary

307 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 TOE and of the evaluation results. This section SHOULD include all key evaluation findings.

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

309 The executive summary SHOULD contain, but is not limited to, the following items.

- Name of the evaluated TOE
- TOE version identifier
- An enumeration of the components of the TOE 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

310 The executive summary SHOULD also contain a summary of the following.

- Evaluation assurance package
- Conformance claims to PPs
- Security functionality
- Threats and organisational security policies addressed by the evaluated TOE
- Special or unusual configuration requirements
- Special or unusual assumptions about the operating environment

C.2.2 Identification of the TOE

311 The evaluated TOE 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, SHOULD also be uniquely identified.

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

C.2.3 Security Target (ST)

313 The ST, possibly a sanitised version, SHALL be referenced in this section.

C.2.4 Architectural Information

314 This section SHOULD provide a functional decomposition of the TOE 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.

315 If the evaluation assurance requirements include any assurance components from the ADV_TDS family, then the TOE 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.

316 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

317 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.

318 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.

319 The FER SHALL identify all locations where evaluation activities have been performed. (See SP-191 *Cross Frontier Evaluation*.)

C.2.6 Results of the Evaluation

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

321 Also, in this section, a reference to each SER SHOULD be given, where detailed descriptions of the evaluation may be found.

C.2.7 Evaluator Comments, Observations, and Recommendations

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

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

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

C.2.8 References

325 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 the following.

- Applicable versions of the CC and CEM
- Applicable CB documentation

- Technical reference documentation
- A complete listing of evaluation evidence used in the evaluation

326 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 20.0, CSEC, 2013-09-30, FMV ID 13FMV7990-2:1.

C.2.9 Glossary

327 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

328 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.

329