Swedish Certification Body for IT Security

084 Sponsors and Developers Guide to the Evaluation and Certification

Issue: 14.0, 2017-nov-01

Authorisation: Mats Engquist, Quality Manager , CSEC

Template: CSEC_mall_doc, 7.0

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 The Scheme is established and maintained by the Swedish Certification Body for IT Security (CSEC) to evaluate and certify the trustworthiness of security features in IT products and the suitability of protection profiles (PP) to define implementation-independent sets of IT security requirements.

3 The objectives of the Scheme are to ensure that all evaluations are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and protection profiles; to improve the availability of evaluated IT products and protection profiles; and to continuously improve the efficiency and cost-effectiveness of the evaluation and certification process for IT products and protection profiles.

4 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., anyone concerned with the development, procurement, or accreditation of IT systems for which security is a consideration, as well as those already involved in the Scheme, i.e., Scheme employees, evaluators, current customers, contractors, and security consultants.

5 The Scheme documents and further information can be obtained from CSEC here:

Swedish Certification Body for IT Security
FMV / CSEC
Postal address: S-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

6 This document is an introduction for Sponsors of Common Criteria certifications and Developers of IT products[1] subject to initial certification. The document describes the certification process and the obligations of Sponsors and Developers in this process. The document is intended to reduce project risks by enabling Sponsors and Developers to understand and plan for the tasks they will be responsible for during the certification process.

7 Information in this document is provided as a guide to Sponsors and Developers. Adhering to the advice in this document will not necessary result in successful certification.

8 The scope of this document is for evaluations up to evaluation assurance level 4 (EAL 4). For evaluations at higher assurance levels, additional guidance may be necessary. The Certifier or the Evaluator should be able to provide advice and assistance.

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

[1] In certification of protection profiles, the Developer or Sponsor role is limited to the production of the protection profile.

1.2 Typography

10 All paragraphs are indexed to enable convenient referencing. Paragraph numbering is unique to the version of the document.

11 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).

1.3 Document Maintenance

12 CSEC maintains this document and other documents describing the Scheme. Any changes, addenda, or updated versions will be posted to the CSEC website, www.csec.se.

1.4 References

13 For a list of references, see Scheme publication SP-001 *Certification and Evaluation Scheme - Scheme Overview.*

2 Introduction

14 A Common Criteria certification is an independent assessment of an IT product according to internationally-recognised criteria. A product that has been successfully evaluated and certified is awarded a certificate by the overseeing Certification Body.

15 The success of the certification depends to great extent on the ability of the Sponsor and Developer to understand and manage their responsibilities during the certification process.

16 A number of factors, such as software engineering praxis, previous design and evaluation experience of the Developer, and the chosen assurance level determine the effort required of the Sponsor and Developer in the certification process. This effort may exceed the Evaluator effort by a factor of two, three, or more, especially if the Sponsor and Developer are not properly prepared. Identifying core issues that are significant for the Sponsor and Developer is important for a successful outcome.

17 This document is provided by the Certification Body to help Sponsors and Developers prepare for their roles in the certification process. Readers with interest in specific topics, such as how to write a security target (ST), should consult the list of references in Appendix A.

3 Common Criteria Summary

18 The objective of a certification is to confirm the claims made in the security target for a specific IT product configuration. Assessment of this claim is done by the Certification Body (the Certifier) and a licensed IT Security Evaluation Facility (the Evaluator). This dual verification ensures that the independence and quality of the certificate is unquestionable.

19 Only certificates issued by Certification Bodies approved by the CCRA group of nations can become internationally recognised.

20 International recognition also requires that the security claims made in the security target are compliant with the Common Criteria, the Common Methodology for Information Technology Security Evaluation (the Common Methodology, or CEM), and the certification Scheme, and that the result of the certification is published.

21 The security claims made in the security target state that the product is able to counter specified threats and comply with organisational security policies defined in the security target, provided that stated assumptions about the operational environment are fulfilled. In order to counter the threats and meet the organisational security policies, the product must meet certain security functional requirements (SFR) and security assurance requirements (SAR), also defined in the security target.

22 The security assurance requirements represent different depth of assessment levels. There are seven hierarchically-ordered evaluation assurance levels, EAL 1 to EAL 7; each level represents more assurance than all lower levels. Each level also may be "augmented", which means that one or more additional assurance components are added to the evaluation assurance level. With increased capacity of an assumed attacker, the assurance level used should increase to ensure that the product is able to withstand such an attacker.

23 The business decision to certify a product may be motivated by the desire to gain a competitive advantage, by a customer requirement, or by a need to show legal compliance.

24 The Certification Body handle all incoming applications or reports in the order they have arrived and are complete. The Certification Body cannot make any statements when the project will be finished since it is mostly depending on the Developer, Sponsor and Evaluator. Please note that the Certification Body is impartial and is not allowed to prioritize due to any Developer/Sponsor commercial requests or any other request to prioritize.

25 There are usually three different (hierarchical) levels of detail for expressing these requirements on a product:

- having a recognised Common Criteria certificate
- being certified at a certain evaluation assurance level
- being compliant with a certain protection profile

26 The Sponsor should anticipate which (if any) of the above scenarios is the case for the product that is a candidate for certification, as it has a significant impact on how accurately the Sponsor may determine the scope of the security target and the evaluation.

4 Roles, Responsibilities, and the Certification Process

27 The evaluation and certification process identifies four different roles:

- The *Sponsor* requests the evaluation of the product, applies for the certification, and interacts with the Evaluator, the Certification Body, and the Developer of the product. The Sponsor may be a person or an organisation. The Sponsor may be the same as the Developer of the product. The Sponsor makes sure that the required evaluation evidence is available, access is given to the development environment, and the product and testing tools are available to the Evaluator.
- The *Developer* is the organisation that develops the product. The Developer supports the Sponsor during the evaluation by providing necessary documentation, technical know-how, and evaluation evidence. With the exception of the lowest assurance level (EAL 1), the Sponsor must rely on Developer support to successfully complete a certification.
- The *Evaluator* is responsible for the assessment of the product by performing the Evaluator actions required by the Common Methodology and the Scheme. Evaluators provide their findings and verdicts in reports to the Certifier. An Evaluator is associated with an Evaluation Facility. To obtain a license to operate under the Scheme, both the Evaluator and the Evaluation Facility must prove their expertise and ability to conduct evaluations to the Certifier. An Evaluation Facility that is licensed by the Certification Body to operate under the Scheme is called an IT Security Evaluation Facility (ITSEF).
- The *Certifier* provides independent confirmation of the validity of evaluation results by overseeing the evaluation process. A Certifier belongs to a Certification Body. If the certification is successful, the Certification Body issues a certificate for the IT product.

28 As the name of the role implies, the Sponsor pays for most of the costs associated with the certification. The Sponsor finances the work of the Evaluator. In many cases, the Sponsor also finances the work of the Developer, who produces the evaluation evidence. If external experts are needed (e.g., to write the security target), this is also often paid for by the Sponsor. In some Schemes, the Sponsor also pays for the work of the Certification Body.

29 The Sponsor is the applicant for the certification and has a formal agreement with the Evaluation Facility for the evaluation and with the Certifier for the certification. The Sponsor also ensures that the Evaluator is provided with evaluation deliverables, training, and access to facilities in a timely manner and in accordance with the Scheme.

30 The Sponsor and the Developer are often the same organisation, but sometimes the Sponsor is different than the Developer, e.g., when a sales organisation or integrator is sponsoring a certification. In cases where the Sponsor and Developer are not the same, there is an increased need for clearly identified responsibilities. In such cases, there is usually a need for the Sponsor to establish agreements for Developer cooperation.

31 The evaluation and certification process may be described in terms of three distinct phases:

- During *pre-evaluation*, the Sponsor, Developer, Evaluator, and Certifier prepare for evaluation. The Account Manager will suggest a First Meeting with the Developer, the Sponsor and the Evaluator to explain how CSEC works in general, roles and responsibilities between CSEC and ITSEF, Swedish laws that apply and information regarding classified material. During the planning phase, it is important that the Sponsor, with the support of the Developer, identifies which required documentation is missing or is insufficient as evaluation evidence. Any missing documentation may be produced in this phase or in parallel with the conduct of the evaluation. One important goal of this phase is to schedule the work of the Developer (i.e., to provide Developer evidence) and the Evaluator (i.e., to evaluate the product) in an e*valuation work plan (EWP)*.
- During the *conduct of evaluation* phase, the evaluation is performed. This means that the Evaluator assesses the evaluation evidence and independently tests the product. This phase may also include site visits to the Developer site. The Sponsor and Developer should expect changes to be made iteratively to the security target, the evidence, and the product as a result of the evaluation process. During this phase we recommend that the ITSEF send updates on the EWP to CSEC once a month to ensure that the Certifier has a time-slot available when the report arrives.
- During the *conclusion of evaluation* phase, the evaluation is completed. The certification report and the certificate are produced. Most work in this phase is done by the Certifier, not the Sponsor or Developer.

32 The steps and the interaction between the parties are illustrated in Figure 1 below. The arrows show the direction of contacts and information provided. Please note that the process illustrated below is specific to the Scheme managed by CSEC.

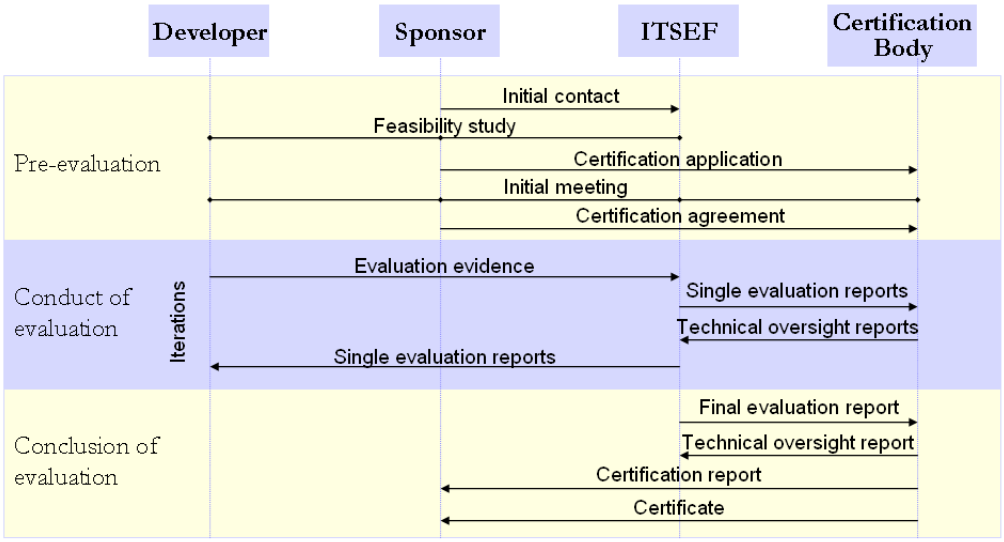


Figure 1 – Interaction between the parties in an evaluation and certification

33 The more information that is available during the pre-evaluation stage and the better the quality of this documentation, the fewer surprises that will come during the conduct of evaluation phase.

34 The Sponsor may decide to have the certification performed in parallel with development, in order to make the certificate available at the time of the product release. In this case, we recommend strong coordination between the development team and the team producing the Developer evidence for the certification.

5 Selecting the Scheme and the Evaluation Facility

35 For certifications performed under mutual recognition, evaluations and certifications are recognised internationally among the CCRA member nations. Certifications up to EAL 4 performed under one national Scheme recognised by the CCRA have the same recognition as any other evaluation.

36 The Sponsor chooses to have the certification performed under a certain Scheme and/or with a certain Evaluation Facility based on previous experience, geographic location, languages used, special skills, or costs involved. The cost and effort may be different under different Schemes and with different Evaluation Facilities, and may be subject to negotiation.

37 In order to obtain a certificate, the Sponsor and Developer must go through an evaluation and certification process. This may take a couple of months, or a year or more, depending on a number of issues, such as the state of development, the complexity of the product, experience with the chosen Scheme, the evaluation assurance level, and the availability of the participating parties.

38 The costs for the Sponsor may include the cost of producing the security target, the cost of the Developer to provide evidence, the assessment work of the Evaluation Facility, and (depending on the national Scheme selected) the oversight work of the Certifier.

39 Evaluation Facilities may make claims on the intellectual property assigned to evaluation reports. This may have implications for re-evaluation, restricting the Sponsor's ability to reuse evaluation reports in a re-evaluation if the Evaluation Facility is different from the original one.

40 There are differences between the Schemes that might have an impact on the certification. The issues that are most likely to be relevant to a Sponsor or Developer are listed below:

- the course of action to be taken if a problem is encountered during the evaluation (i.e., whether the evaluation continues after the problem is remedied, or ends immediately requiring later resubmission of the remedied product)
- (natural) language in which documentation must be provided
- requirements for provision of Evaluator evidence to support re-evaluation and reuse of evidence
- specific handling of Scheme identifiers, logos, trademarks, etc.
- specific guidance in dealing with cryptography
- handling and application of Scheme, national, and international interpretations
- guidelines of suitable alternative approaches to testing where testing is infeasible
- preferred test approach (if any): at internal interface or at external interface

41 Handling of these issues may differ between the Schemes, and the differences may have some impact on the Sponsor. The handling of these issues should be known to the Certification Body and any Evaluation Facility licensed under its Scheme. The Sponsor should seek advice on the issues listed above or other identified issues whenever appropriate.

6 Making the Security Claims

42 A certification is made against the security claims stated in the security target. These claims are specific for a certain version of the product, with a certain scope, and in a specific configuration. The content of the security target largely determines the effort involved in the certification. The version, configuration, and scope of the subject of evaluation are referred to as the target of evaluation (TOE).

43 Many factors determine the effort of the evaluation work, such as the complexity and overall quality of the product and the development environment. However, there are four main factors that the Sponsor may be able to influence, that will have an impact on the effort of the evaluation work. The factors are listed in descending order, starting with the most determining factor:

- *The evaluation assurance level*. The evaluation assurance level stipulates the required Developer evidence and the assessment effort, and is the most important factor in determining the total effort of an evaluation. Note that the evaluation assurance level cannot always be selected by the Sponsor; the decision might be based on the expected effort or the available budget for the evaluation. To make an evaluation meaningful, the selected evaluation assurance level must be appropriate for the environment in which the product is intended to be used. This means that Sponsors may have greater freedom to decide on the appropriate evaluation assurance level for general purpose products than for products with a specific target environment.
- *The scope of the evaluation*. By limiting the scope of the evaluation, for example by including only the core functionality (e.g., by excluding administrative tools), the size of the TOE can be kept smaller, which will reduce the effort both for the Developer to develop design documentation and for the Evaluator to assess these parts not included in the evaluation. The parts excluded from the scope of evaluation may still be considered part of the environment, which means that they can still be part of the installed environment and even have certain security functions, but they will not be evaluated in the evaluation.
- *The security functional requirements.* Each security functional requirement must be implemented by one or more security functions, which must be documented in the design documentation and tested to the level of detail required by the selected assurance level. By reducing the number of security functional requirements, this effort will be reduced. Simply removing security functional requirements usually means that certain threats cannot be countered. This means that these threats either must be removed from the environment (cannot be assumed in the environment) or that they must be addressed by the environment and not by the product. However, this may reduce the usefulness of the product, and may even make the certified claims and configuration of the product useless in the intended end user environment.
- *The evaluated configurations and platforms*. Claiming evaluation on a number of different configurations and platforms must be verified by testing. This means that the effort for testing will increase with the number of different configurations and platforms described in the security target.

44 How these factors impact efforts to produce Developer evidence is shown in the next chapter.

7 Creating Developer Evidence and Records

7.1 Format of the Evidence

45 The security criteria stipulate that certain documentation is needed for the evaluation of the product. However, apart from the security target, there are no requirements about the formal structure of Developer documentation. The requirements are simply that the documentation must address certain aspects of the product and its development environment and must be stable and formally issued versions, not just verbal explanations.

46 The responsibility for providing the required evaluation evidence lies with the Sponsor. However, most of the evaluation evidence is likely to be produced by the Developer or by an external consultant on behalf of the Sponsor or Developer.

47 The required documentation and how much detail it should contain depends on the security assurance requirements identified in the security target, usually expressed as an evaluation assurance level (EAL 1 to EAL 7). The type of product and its intended use also help determine which type of documentation must be provided.

48 The assurance levels are hierarchical; an increasing level of assurance results from the application of greater evaluation effort. The goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon [CC Part 3, section 6.3]:

- *scope* – i.e., the effort is greater because a larger portion of the IT product is included
- *depth* – i.e., the effort is greater because evaluation is deployed to a finer level of design and implementation detail
- *rigour* – i.e., the effort is greater because it is applied in a more structured, formal manner

49 For a description of the different assurance levels see the Common Criteria [Part 3, section 8.1]. The following table from the Common Criteria Part 3 section 8.1 provides some guidance. For example, the table shows that for an EAL 3 evaluation, within the ADV class, three development families are required: ADV_FSP.3, ADV_ARC.1, and ADV_TDS.2. ADV_FSP.3 is the assurance requirement for the functional specification for EAL 3, which requires more detail than the ADV_FSP.2 requirement for EAL 2. In the table, numerals that are highlighted by bolding show where assurance requirements increase at the higher evaluation assurance level.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Figure 2, Assurance Components by Evaluation Assurance Level

50 As previously noted, apart from the security target, the Common Criteria does not require creating any specific documentation. Existing documentation can and should be used as evidence, provided that it is correct and sufficiently complete. In most cases, existing documentation must be extended, and new information specific to the Common Criteria must be added.

7.2 The Developer's Role

51 The Developer must to produce evidence that makes sense to the Evaluator and fulfils the requirements of the Common Criteria, the Common Methodology, and the Scheme. In order to meet the Evaluator's expectations, the Developer should read and understand the Common Criteria and the Common Methodology sections that are relevant for the evaluation, and request advice from the Evaluator or the Certifier.

52 It may not be necessary to develop entirely new documentation in order to satisfy the requirements. Re-using existing documentation created during the regular development of the product is both possible and preferable. Often the Developer can simply add a rationale about how the existing documentation satisfies the requirements. This solution prevents higher long term costs for the Sponsor, because documents created for evaluation must be updated each time the product is developed further and needs to be re-certified.

53 Please note that if evidence is changed in any way, the Developer shall notify the Evaluator.

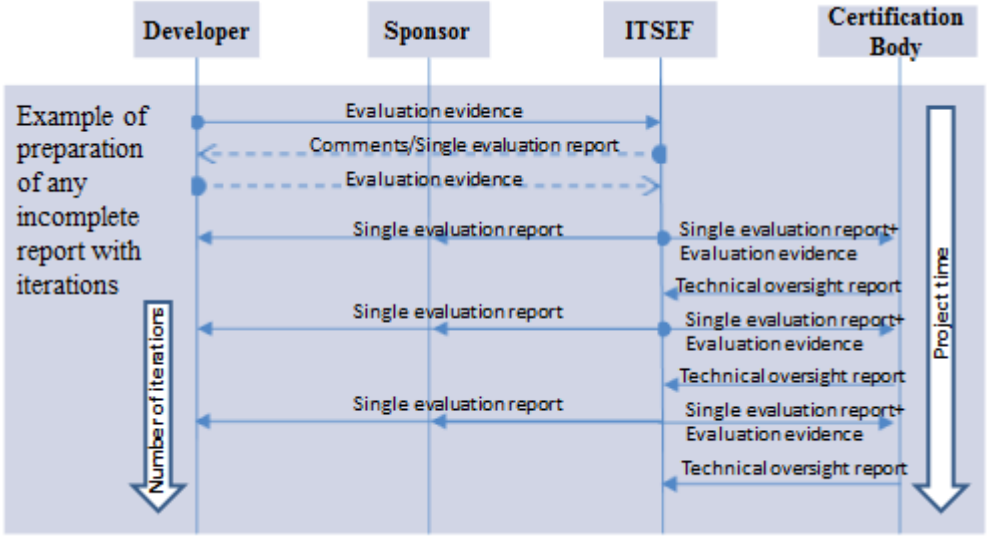
54 The Developer should fully understand the security claims made in the security target and ensure that the documentation provided to the Evaluator tells a coherent story supporting those claims. If the Developer does not relate the documentation to the security claims, he Evaluator is forced to spend additional time tying things together.

55 The Developer should help the Evaluator to understand the product by providing initial education and assistance during the evaluation. Without this support, the evaluation effort may become more costly for the Sponsor and may take longer than expected because the Evaluator will have to independently learn how to use and configure a potentially complex product. Well-trained Evaluators will also more easily understand the rationale that is presented by the Developer as to why the evidence fulfils the requirement.

56 Sample evidence documentation may be made available to Developers; however, such documentation should only serve as an example for the Developer to understand what is required, not as a template for the Developer. The existing documentation from the Developer should be used as a basis.

7.3 The Evaluation Process is Iterative

57 Evaluation is usually an iterative process; changes are made to documentation, the product, and the security target until the Evaluator is satisfied that the evidence meets the requirements of the Common Methodology and the Scheme. The Sponsor and Developer should be prepared for this and not assume that everything will pass in the first round.



58

59 *Figure 3– Iteration, interaction between the parties in an evaluation and certification*

60 Numerous iterations will slow the project down, see *figure 3*. It is therefore crusial for the Developer to deliver as timely and as complete as possible, otherwise it will take more time for the Evaluator and later, if the Evaluator has been forced to rush in shortage of time, it may take more time for the Certifier as well, both which may affect the number of iterations and the project time.

61 In the following sections, each assuance class is discussed, along with expectations about the assurance families in each class. The assurance families and the detail of information required is evaluation assurance level-dependent. To fully understand the requirements in order to make a more detailed estimate of the effort needed, we recommend that Sponsors and Developers consult the Common Criteria Part 3, sections 10-16. These sections identify the "Developer action elements" and the "Content and presentation of evidence elements" for each assurance family that is part of the selected evaluation assurance level or assurance requirements in the security target.

7.4 Security Target

[CC Part 3, Section 11]

Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.

62 The security target (ST) is the basis for the evaluation and is a formal document. A Sponsor or Developer without extensive Common Criteria experience may not be able to produce a suitable security target as the basis for an evaluation. However, Developer involvement is essential to produce a useful security target. Hence, the security target may be written using outside support, such as a consultancy, in close cooperation with the Developer. It typically takes several weeks to develop a good security target. This is an extra effort that Sponsors must plan for and that may require support from a highly-qualified Developer. It may also be useful to discuss the security target with some representative end users of the product before starting the evaluation. The purpose of including end users is to make certain that the end result of the evaluation will fulfil their real needs.

63 *Expected availability:* Unless this is a re-evaluation, there will be no initial security target to use as a starting point, so one must be created. However, there is usually a lot of useful input available, including security targets that may have been published for other (potentially similar) products. If compliance to a specific protection profile is intended, the protection profile may provide a basis for the work of authoring the security target.

64 *Expected effort:* If the product is not too complicated and is a relatively known type of product, it usually takes a few weeks to develop a good security target, assuming the availability of experts with sufficient skills and experience. Updates to the security target should be expected during the evaluation, as the product's behaviour becomes better known.

7.5 Development

[CC Part 3, Section 12]

Assurance class ADV:
The requirements of the Development class provide information about the TOE. The knowledge obtained by this information is used as the basis for conducting vulnerability analysis and testing upon the TOE, as described in the AVA and ATE classes.

65 The Developer must provide documentation of the design and implementation of the SFRs (at the various levels of abstraction) of the architecture-oriented features. Starting at EAL2 , domain separation, TSF self-protection and non-bypassability of the security functionality shall be provided. At EAL6 a security policy model and for correspondence mappings between security policy model and the functional specification. At EAL 5 the internal structure of the TSF, which covers aspects such as modularity, layering, and minimisation of complexity shall be provided

66 The Common Criteria concepts of functional specification and TOE design might match the previous experience of the Developer. However, an existing functional specification might not identify and describe all the externally-visible security interfaces (TSFI) in sufficient detail to satisfy the Common Criteria requirements. Existing TOE design documentation might not divide the subsystems into security-enforcing and other subsystems, as required by the Common Criteria.

67 The TOE design shall provides decomposition of the TOE into subsystem and from EAL4 also into modules. A module is the most specific description of functionality: If modules are is required (i.e., for an EAL 4 or higher evaluation), design documents at this level may not exist at all, or may not be sufficient to meet the requirements for certification, which include describing the purpose and method of use of all interfaces to the modules of the security function, and providing details of effects, exceptions, and error messages. The shall also describe the separation of the modules into TSP-enforcing and other modules, which is usually not available in existing design documentation.

68 A security policy model (required for EAL 6 and above) is not usually available, so this document must also be written.

69 *Expected availability:* The level of detail already documented very much depends on the culture of the Developer. The level of detail in a well-defined product usually can meet EAL 2 or possibly EAL 3 requirements, with the exception of the Common Criteria-specific aspects listed in this section. For a product that is not well documented, a significant effort is required at EAL 2 or EAL 3. In many cases, sufficient module design documentation is not available or is not up to date. For this reason, significantly more effort should be expected for an EAL 4 evaluation.

70 *Expected effort:* It is usually a major effort to produce this set of evidence. Much depends on the size and complexity of the product, the amount of available design documentation, and the assurance level. It is almost always necessary to create some new documentation, such as the security architecture (at EAL 2 and above) and the security policy model (at EAL 6 and above). The Developer should not assume that existing documentation is complete or contains the required content. The effort increases as the assurance level increases.

7.6 Guidance Documents

[CC Part 3, Section 13]

The guidance documents class provides the requirements for guidance documentation for all user roles. For the secure preparation and operation of the TOE it is necessary to describe all relevant aspects for the secure handling of the TOE. The class also addresses the possibility of unintended incorrect configuration or handling of the TOE.

71 Products are usually shipped with guidance documentation describing how to install, administer, and use the product.

72 Even very good guidance documentation normally cannot meet all the requirements for certification. This is due to the fact that evaluation-specific information, such as intended use, assumptions, and the definition of the evaluated configuration as stated in the security target cannot be written in any guidance until they have been documented in the security target.

73 *Expected availability:* Good existing guidance documentation usually provides a very good basis, but it must be extended. Usually security-specific information is not sufficient addressed, and the specifics of the evaluated configuration are not covered. The Developer may consider having a separate document dedicated to the specifics of the evaluated configuration.

74 *Expected effort:* Updates to the existing guidance documentation are normally necessary. A separate guide should be considered for evaluation-specific information. Assuming that good basic product documentation exists, it might take a few weeks to update the existing documentation and to produce a new guide documenting the evaluated configuration.

7.7 Life Cycle Support

[CC Part 3, Section 14]

Assurance class ALC
Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities.

75 Life-cycle support deals with the policies, procedures, tools, and security measures used in the development environment to protect the product during its life-cycle. The level of protection required depends on the type of product and its intended use.

76 The The Developer must provide configuration management documentation describing the configuration management system and how it is used to maintain the product. The Developer must also provide configuration lists and records showing that the system is used as described.

77 The Developer shall provide a unique reference for the product, which shall be unique to each version of the product. The product shall be labelled with its reference. It shall be demonstrated that changes made to the product will result in a new reference. In order to be able to show this, the items comprising the product must be under configuration management[2]. This also applies to the documentation, test cases, and test results. The configuration management system may be manual or automatic[3]. The Developer shall be able to show that the configuration items are under access control to protect the integrity of the product.

[2] This requirement is EAL-dependent.
[3] The configuration management system may be entirely manual up to EAL 3; for EAL 4 and above, some aspects of configuration management must be automated.

78 Developer must provide documentation showing how the security of the product is maintained from the time the product leaves the development environment until it is operational at the customer site. This includes the packaging, delivery, installation, and start-up of the product. This activity ensures that the product is not replaced or tampered with until it reaches the operational environment. Usually, internal Developer documentation describes the delivery process, while installation instructions are found in an installation guide, which is considered separately from the administrator and user guidance.*Expected availability*: Life-cycle evidence is required starting at EAL 3. Most development organisations will be able to meet the requirements of EAL 3 or EAL 4, provided their procedures are reasonably well documented.

79 In any good development environment, all software is expected to be under configuration management control. This is sufficient for EAL 2, but for higher evaluation levels, all Developer evidence must be under configuration control, and for EAL 4 and above, automated configuration management tools must be used to support generation of the TOE.

80 Any well-defined and documented delivery and installation procedures can be used as a basis for the required evidence. What might be missing is sufficient documentation of the internal processes on delivery, as well as a description of how to install the evaluated configuration of the product.

81 *Expected effort*: Documentation of life cycle procedures may be necessary for EAL 3 and is more likely for EAL 4.

82 The effort to handle any deficiencies for configuration management requirements is expected to be rather limited and fairly easy to address.

83 The effort to handle any deficiencies for the delivery and operation is expected to be rather limited and fairly easy to address.

84

7.8 Tests

[CC Part 3, Section 15]

Assurance class ATE:
Testing provides assurance that the TSF behaves as described (in the functional specification, TOE design, and implementation representation).

85 The performance of functional tests and penetration testing take significant time in every evaluation. The Sponsor must make the product available to the Evaluator, along with any necessary hardware and software platforms[4], including any additional peripheral components required in order to be able to perform these tests. Normally the Developer gives the product to the Evaluation Facility, which then installs it in its own test laboratory. However, sometimes the platform and peripherals of a product are so complex that testing on the premises of the Evaluation Facility would not be cost-effective. In such cases, the functional tests and penetration testing may be carried out at the Developer site. The precise arrangements for testing the product are specified during the pre-evaluation phase.

86 *Expected availability:* Product testing is performed in any normal product development; however, routine product testing is almost never sufficient for certification (with the exception of EAL 1, which requires no Developer testing evidence). During routine product testing, usually the product's functionality and some, but not all, of the security behaviour of the security functions are tested. The comprehensive testing of security functions is the core testing interest for Common Criteria certification.

[4] Hardware and software platforms can be computer hardware, operating systems, database systems, etc.

87 *Expected effort:* For EAL 1, all testing is performed by the Evaluator. The testing framework used by the Developer for functionality testing may be extended to include the security tests necessary for certification. This approach usually works for EAL 2, but may be insufficient for EAL 3 and EAL 4. For higher assurance levels, much more effort is normally required to show completeness and more in-depth testing. The effort increases with the number of platforms and configurations.

7.9 Vulnerability Assessment

[CC Part 3, Section 16]

The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

88 The level of information required for vulnerability assessment depends on the assurance level. The vulnerability assessment is performed by the evaluator.

89 *Expected availability:* n.a

90 *Expected effort:* No effort.

8 Who Produces the Developer Evidence?

91 The required Developer evidence and records must be provided by the Sponsor or Developer. Developer evidence is documentation of the product or its development environment, and is discussed in this section. Records are evidence that the procedures documented are being used; records are not discussed here.

92 Please note that if evidence is changed in any way, the Developer shall notify the Evaluator.

93 While some required Developer documentation is likely to be available or is fairly easy to produce, some required documentation is less likely to be available and may be rather difficult to produce because it requires in-depth knowledge of the product, in-depth understanding of IT security or Common Criteria evaluation requirements, or both. The required understanding of IT security and Common Criteria increases with the evaluation assurance level.

94 The development of Developer documentation can take a number of forms, for example:

- The Developer produces the necessary documentation as part of the normal development process. This is the least expensive alternative if the certification is performed in parallel with development of the product. However, it may be difficult for a Developer without previous evaluation experience to understand what documentation is expected. Therefore, this alternative may be more expensive than originally expected if adequate Common Criteria experience is not available in the project.
- In the course of the certification process, the existing documentation, which may not initially be ideal in all respects, is improved, with the Evaluator and the Certifier providing information about what is required. This alternative may sometimes be preferred since it involves the Evaluator and the Certifier during the evaluation process. However, it is likely that the Evaluator and/or Certifier will need extra time to complete their work if the evidence is not complete when the process starts.
- The existing documentation is examined in a pre-evaluation phase, compared with the requirements of the Common Criteria, the Common Methodology, and the Scheme. Any deficiencies are identified. This pre-evaluation can be performed by one of the Evaluation Facilities. The advantage of this approach is that only documentation that is really necessary is prepared. The certification process can then get under way and be completed in a relatively short time.
- A qualified external party may prepare missing documentation on behalf of the Sponsor or Developer. Preferably, the external party will be someone who has previously been through the complete process for a similar product at the same or higher evaluation assurance level.
- An Evaluation Facility may act as a qualified external party assisting in preparing the evidence needed. However, if the Evaluation Facility is also tasked with the evaluation of the product, then to ensure that the subsequent evaluation is entirely objective as required, the Evaluators performing the evaluation must have played no part in preparing the documents. This alternative may seem expensive, but it has the advantage that the Sponsor or Developer usually ends up with a set of documents that comply with the requirements before the evaluation starts.

9 Estimating Effort

95 It is difficult to estimate the Sponsor effort for an evaluation, especially if the Sponsor organisation has no previous evaluation experience.

96 The Evaluator and Certifier have extensive experience with evaluations and can usually accurately predict the scope of their own efforts for a project. Evaluator and Certifier effort tends to be driven mainly by the evaluation assurance level and the complexity of the product.

97 It should be noted that because they are required to maintain strict independence, the Evaluator and Certifier can never guarantee that an evaluation project will result in a successful certification.

98 The effort to the Developer to develop *new* documentation to pass certification (the security target, correspondence analysis, strength-of-function analysis, vulnerability analysis, etc.) usually can be accurately estimated. The effort to enhance *existing* documentation (guidance documentation, internal process documentation, design documents, etc.) to satisfy Common Criteria requirements is difficult to estimate and depends on the quality of existing documentation, the maturity of the developer environment, the evaluation assurance level, and the complexity of the product.

99 The effort to make changes in the product due to Evaluator findings, such as vulnerabilities, is almost impossible to estimate. The effort involved depends on the level at which the problems were identified and the severity of the problems.

Appendix A Recommended Reading

[PP/ST Guide] Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets, ISO/IEC TR 15446, 2009-03-01.

Appendix B References

[CC Part 1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
[CC Part 2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements
[CC Part 3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology
[SP-001]	Certification and Evaluation Scheme - Scheme Overview
[SP-002]	Evaluation and Certification
[SP-004]	Licensing of Evaluation Facilities
[SP-007]	Quality Manual