Supporting Document Guidance

Site Certification

October 2007

Version 1.0
Revision 1

CCDB-2007-11-001

Foreword

This is a supporting document, intended to complement the Common Criteria and the Common Evaluation Methodology for Information Technology Security Evaluation.

Supporting documents may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the supporting document. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor: Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security

Document History:
V1.0 October 2007 (initial supporting document version)

General purpose:

This document defines the process, the criteria and methodology and interpretations respectively for the evaluation and certification of CC development sites. It enables the evaluation/certification of those sites in a modular fashion and without a relation to a specific TOE. The results of the Site Certification process can be re-used in a CC product evaluation later on.

Field of special use: Evaluation/certification of CC development environments

Table of contents

1. Intention

1 The "Bundesamt für Sicherheit in der Informationstechnik" (BSI) has taken the lead for a CC-project to develop and validate a procedure in order to perform reusable evaluations of ALC related aspects.

2 The motivation of this project is based on an increasing demand coming from different developers to avoid unnecessary evaluation efforts. In this context reuse of certified ALC material would be a significant benefit to developers who develop multiple products at one or more sites, particularly under the same procedures. This would lead to a significant reduction of time and money for evaluations which could also as a result improve the acceptance and the market of the CC.

3 To achieve this goal one possibility is the Site Certification approach which is the basis of this document. The underlying procedure of this approach leads to a TOE independent CC certificate which is issued to confirm that a specific development environment fulfils the CC requirements regarding the related ALC class. These certificates can be reused in a TOE evaluation later on.

4 Therefore the BSI together with several evaluation facilities developed a procedure that makes it possible to issue site certificates. This procedure has been validated by several trial evaluations. These trial evaluations have been carried out in accordance to the desciptions provided in this document.

5 The aim of this document is to become familiar with all phases of the Site Certification process itself and with the instructions how to apply a site certificate during a "normal" TOE evaluation. For this a theoretical introduction (chapter 2) to the underlying background is given. This is followed by a description of the underlying concept and a definition of the prerequisite for using the concept (chapter 3). Elementary part of the Site Certification concept is a so called Site Security Target (SST). Its content is described in chapter 4. To be able to apply the CC ALC requirements in a Site Certification context some adaptations and interpretations are necessary which are provided in chapter 5. A detailed step by step guideline provided by a flowchart including a respective explanation of all important process stages is given in chapter 6. Chapter 7 provides the security assurance requirement and the related methodology for the CC AST class which is needed for the evaluation of Site Security Targets. Important terms and abbreviations are explained in the chapters 8 and 9.

6 All terms and abbreviations used in this document are taken from the CC, Version 3.1 [1], [2], [3] and [4].

2. Introduction and Background

7 Some developers have a relatively simple Development Environment. Design, testing and TOE creation are all done in the same building, and perhaps mass-production of the TOE is done somewhere else. If these developers wish to evaluate several TOEs, that use the same development environment, it is relatively easy to evaluate the entire development environment of a TOE once and reuse that result for the next evaluation.

8 However, many development environments are much more complex, and may consist of a dozen or more sites, located all across the world (Figure **1**). Developers may develop multiple TOEs, each using a different subset of these sites.

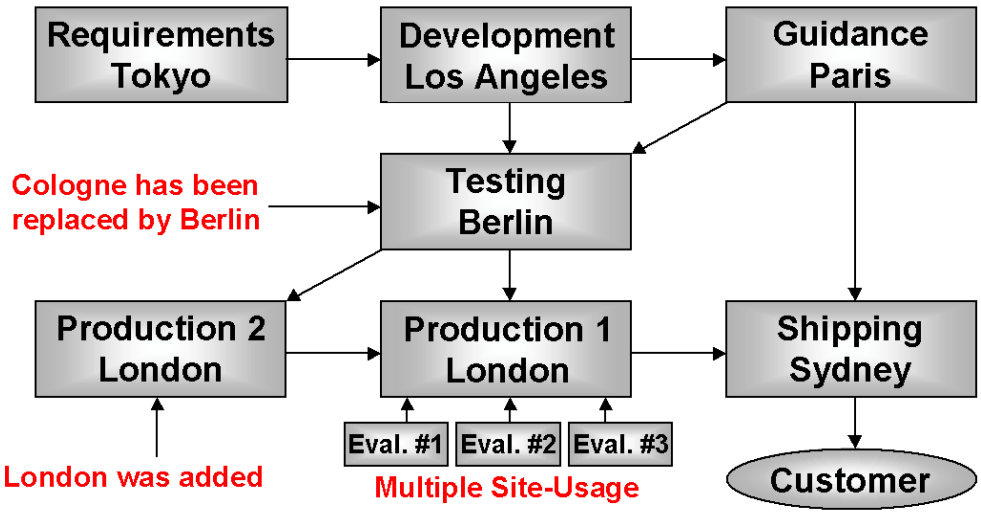


Figure 1: Example of a complex Development Environment

9 The developer may also decide to replace a specific site by another one. E.g. testing is now done in Berlin instead of Cologne. Some sites, e.g. mask shops, may be involved in many different evaluations of many different developers (done by different labs under different schemes).

10 Therefore it makes sense to divide the development environment of a TOE into parts which represent specific life-cycle phases of the TOE. These parts of the development environment can be evaluated and certified according to certain ALC-criteria. Once certified, an issued Site Certificate can be reused within its period of validity without further evaluation effort for these already certified development environment parts. That means, dividing one “big” site into “sub-sites” (and certifying them) makes it possible for a developer to combine them for a special TOE evaluation in an optimal manner. In the case of site changes not all sites would have to be re-evaluated, but only those that have changed.

3. Principle Concept

3.1. Capability of the Site Certification Process

11 This section gives an overview about the Site Certification process. Here the different starting positions for the application of the Site Certification process are explained followed by a principle description of the main process phases. Finally it will be explained how to get confidence that the process keeps the assurance required by ALC.

3.1.1. Starting Point

12 As already mentioned the motivation and intention for the development of a Site Certification process is to make reuse of ALC material possible in an efficient manner. This will lead to a significant reduction of time and money efforts. But the situation for potential users of the Site Certification process are different. So for some developers, it may be useful to evaluate the development environment as a whole and reuse those results. For some other developers it may be useful to evaluate the development environment in parts and reuse the partial results for different purposes later. This section will try to consider the main starting positions.

13 In general there are three possiblee situations:

- Situation 1: For further (re-)evaluations the developer wants to reuse a previously certified development environment that has not been changed in the meanwhile.

- Situation 2: The developer wants to split his development environment into specific parts which at least represent one special life-cycle phase. These different sites will be certified according to those ALC assurance requirements (SAR) which are in the scope of this specific site. He can then reuse these certified sites for all evaluations in a modular way as far as they fulfil the ALC-SARs of a specific TOE-ST.
  This possibility will be of particular importance for sub-contractors and/or integrators which have to provide/compose parts of a TOE. For them it will be very efficient to evaluate and certify their related sites only once, and reuse this result in a lot of different TOE evaluations (may be for different developers/integrators) using this site.

- Situation 3: The developer only has parts of his development environment certified. These certified parts can be claimed in a (re)-evaluation. Other parts may not be certified and can hence not be claimed in a later (re-)evaluation. Reasons for this could be that the validity of an issued Site Certificate has expired or a specific site has been changed somewhere and somehow or special ALC aspects are not in the scope in one of the claimed Site Certificates.

3.1.2. Structure of the Site Certification Process

14 Based on the capability of the Site Certification process and its principle intention the underlying process can be split into three independent procedures:

- Procedure “Site Certification” (refer to chapter 6.1)
- Procedure “Splicing” (refer to chapter 6.2)
- Procedure “Site Certificate Integration” (refer to chapter 6.3)

15 The Site Certification procedure contains all steps which have to be done to issue Site Certificates to development environments or parts of them. This procedure will be applied for sites that haven’t been certified in the past as well as for sites that already have a site certificate but which have to be updated for certain reasons (e.g. validity has expired or an update/augmentation is necessary).

16 Splicing represents the procedure that composes all certified and/or non-certified parts of a life-cycle to a bigger entity. This bigger entity can either be a site which covers an entire development environment of a TOE and can be used during a TOE evaluation later on (see Site Certification Integration procedure). But it is also possible to use the Splicing procedure to compose several sites to a bigger site (not necessarily making up an entire development environment of a TOE) which can obtain a Site Certificate.

17 The aim of the Site Certification Integration procedure is to reuse already certified ALC-material within a specific TOE evaluation. This can be done by claiming already certified sites which fulfil the ALC requirements (ALC-SARs) for the TOE evaluation. The procedure “Site Certificate Integration” gives clear instruction how to use/integrate Site Certificates in the TOE-ST.

3.1.3. Description of the main Phases of the Site Certification Process

18 The starting point in applying the Site Certification process to reuse ALC material is to define the scope for each Site (the ideal case would be the entire development environment of a company) which will be used in later TOE evaluations. Each site addresses at least one life-cycle phase. The definition and description of the site scope has to be stated in an individual Site Security Target (SST) for each site as shown in the following figure 2. As part of defining the scope of each single Site the concerning SSTs contain a section which describes according to which ALC-SAR a site is to be evaluated.

19 The next step for reusing the results would be to evaluate and certify the SSTs and the related developer documentation which fulfil the SARs claimed. In the end of this exemplary procedure five site certificates (for Site A to E) can be issued.

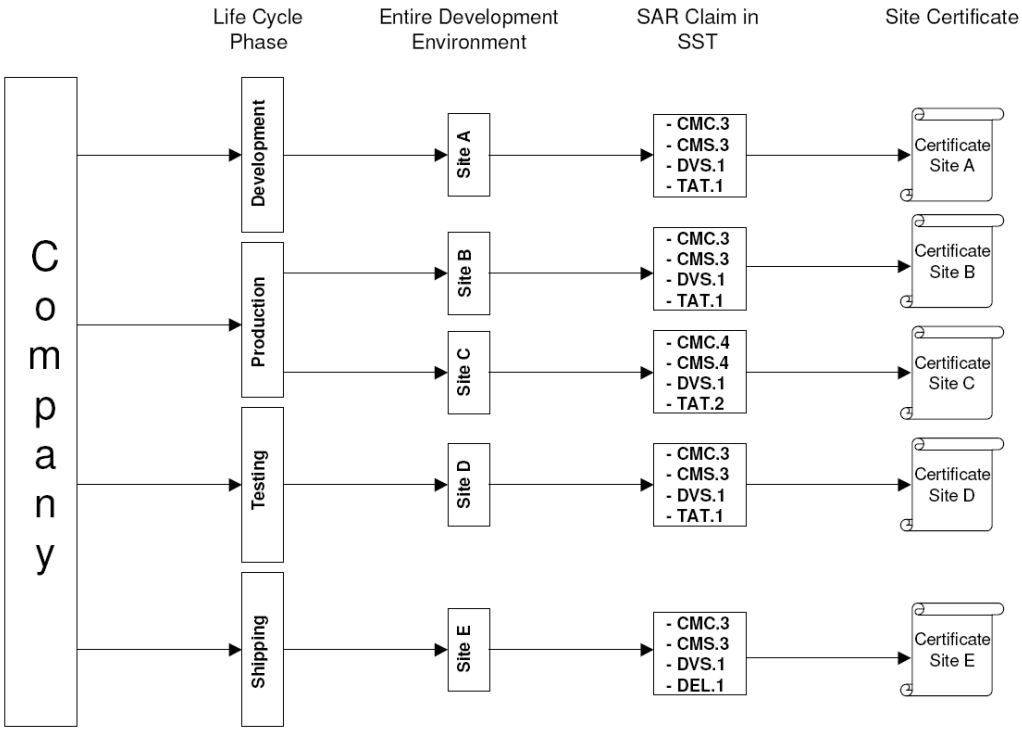


Figure 2: Site Certification

20 In a later TOE evaluation the developer now has the basis to reuse the ALC material which have been covered by the site certificates. While writing the TOE-ST the developer has to define the scope of the development environment by claiming the ALC requirements for the TOE. Here he has to consider all ALC components from an EAL the TOE shall be conformant with (see the figure below that is assuming a TOE evaluation at EAL3).

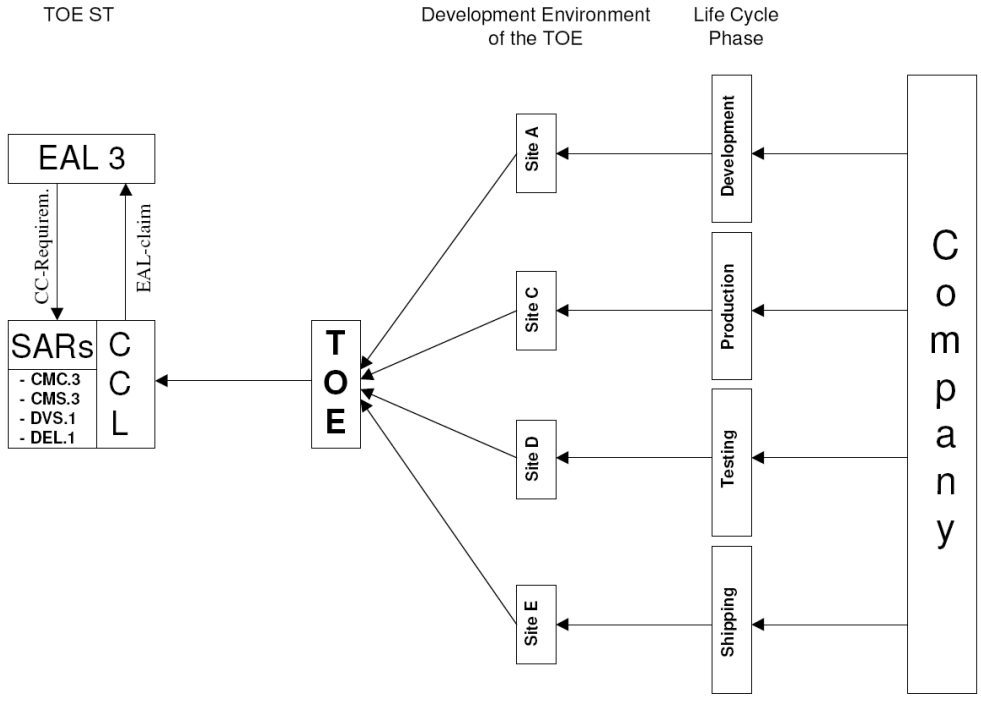


Figure 3: Reuse of Site Certificates in a TOE evaluation

21 Assumed that no changes have been made in the certified development environment the Site Certificates can be used for any TOE evaluation developed in that environment. Moreover if the Site Certificates fulfil all ALC related SARs of the TOE-ST, no additional evaluation and certification efforts are necessary in the TOE evaluation concerning ALC.

22 The next step as shown in figure **4** will be a more technical one from the CC point of view. That is the formal procedure to compose different certified sites to the entire development environment for a specific TOE. This procedure is called "Splicing". For the evaluation of the entire development environment, the evaluator has to get an understanding of the life-cycle model used by the developer. That means the evaluator of the TOE has to take care that the developer of the TOE claims the right sites and ensures that these sites and also the different life-cycle phases work together correctly. He also has to confirm that the Site Certificates claim an attack potential level which are commensurate with the claimed AVA_VAN level of the TOE. The correctness of the output generated by the Splicing procedure is checked later on by applying ALC_LCD criteria (for details please refer to chapter 3.1.4). Please note that not all certified aspects of a certified site are necessarily needed in the composed development environment. (e.g. assume that Site C as well as Site D have a certified development process but only the process from Site D is reused in the composed development environment). This is to ensure a maximum of reusing Site Certificates.

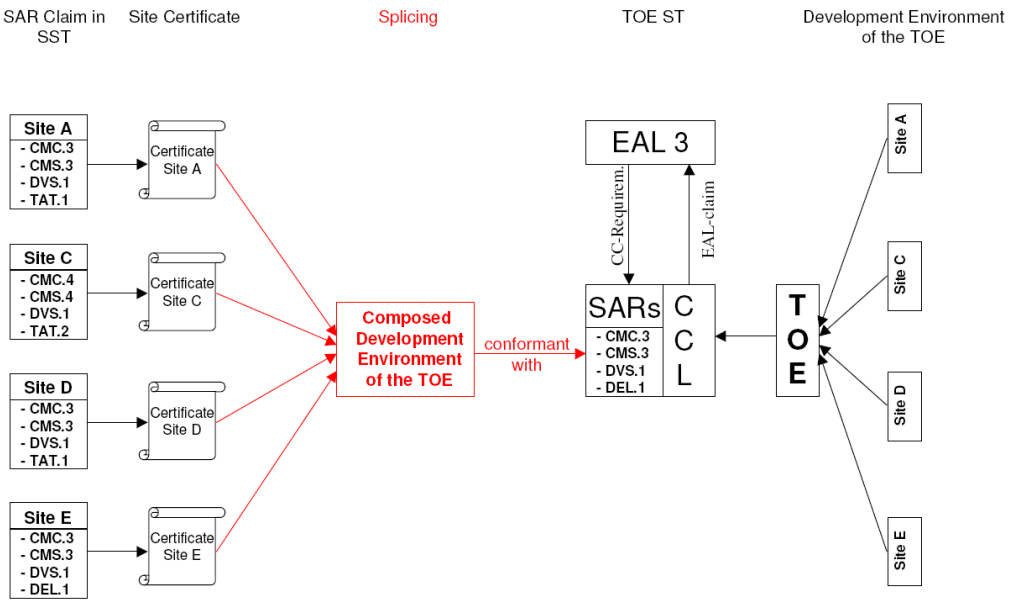


Figure 4: Splicing

23 The Splicing procedure can be used for both to built the composed development environment of a TOE as well as to merge several small certified sites to only one site (which also can be certified) for some reasons. Please note that a composed development environment can get a Site Certificate (if the developer applies for) but it does not need to have one to be reusable during a TOE evaluation.

24 In an evaluation of a specific TOE it is possible that not all ALC aspects of the TOEs development environment are covered by certified sites. In order to fulfil the ALC-SARs claimed by the TOE-ST, the non-certified portions needed for the TOE-evaluation have to be evaluated before Splicing can be performed. The possible outcomes of the Splicing procedure would then be either to

- Reuse the certified sites and evaluate the non-certified site portions during the TOE evaluation. By this the evaluated development environment will not have a site certificate and therefore can not be claimed in other TOE evaluations.

- Certify the development environment which contains the certified sites and the non-certified site portions as a new (updated) "bigger" site. This complete certified development environment can now be claimed as a (composed) site in the future.

- Certify the non-certified portions as a new site. The new and untouched ("old") Site Certificates can be reused in future TOE evaluations.

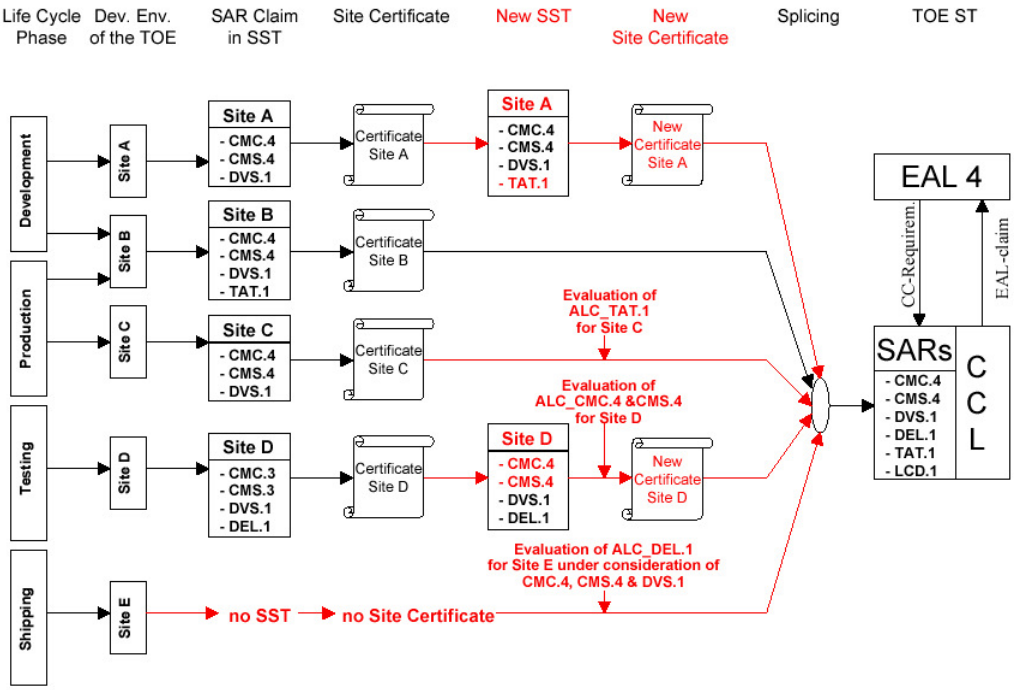


Figure 5: Involving non-certified parts into sites and/or the TOE evaluation

25 In principle there are four different possibilities to consider non-certified aspects into the Splicing procedure as shown in figure **5**:

a) The scope of Site A has not been certified according ALC_TAT.1. But the evaluation of the tools used for the TOE development is now needed to fulfil the requirements for the TOE evaluation. The developer now decides to augment the certificate of Site A. Therefore the tools applied in Site A are evaluated according TAT.1 and a new Site Certificate is issued. The prior evaluation results of Site A can be reused completely.

b) The same situation happens for Site C with regard to the production phase. But in this case for some reasons the developer comes to the decision not to have a new Site Certificate. The tools are evaluated according ALC_TAT.1 but that does not lead to a new site scope in order to have an updated Site Certificate. This ALC_TAT.1 evaluation is then part of the TOE evaluation.

c) In previous evaluations the testing procedures were sufficient to fulfil the EAL 3 requirements with respect to ALC. But now the developer wants to use Site D for testing and is aiming at conformance with the respective EAL4 ALC requirements. Therefore he has to evaluate his CM system according to ALC_CMC.4 and ALC_CMS.4. Furthermore he decides to augment the Site Certificate of Site D. For this augmentation the prior evaluation results can also be reused.

d) Site E has no valid Site Certificate yet but all delivery activities for the TOE are located there. For certain reasons he developer does not want a Site Certification for this site. But he can include all evaluation activities into the Splicing procedure as needed for the TOE evaluation. However he has to ensure that the delivery site also has a CM system and DVS measures in place which are subject to evaluation and do not contradict to the other relevant sites.

26 The following figure 6 illustrates a situation which explains one of the advantages of the Site Certification process. In this example the development of a specific product was done all across the world. Actually the company (developer) uses the sites shown also for other products which are intended to be evaluated in different schemes by different evaluation labs.

27 In order to save efforts (time and money wise) not only for his own company but also for the evaluation lab and certification body the company decided to carry out the Site Certification by schemes which are located physically close to the site. In the chosen example the certification of this TOE is performed under the responsibility of the Australian scheme. Many parts of the ALC material are evaluated through other schemes which define their parts in the respective SSTs in applying the Site Certification process. Finally it is the task of the Australian scheme to perform the Splicing procedure (by applying the LCD.1 requirements) which relies on the Site Certificates issued to the sites which are part of the development environment of the specific TOE. By that it is ensured that the developer chose the right sites and ensures that the sites and also the different life-cycle phases work together correctly. That means LCD.1 provides the assurance that the life-cycle phases (e.g. represented by different sites which have been evaluated and certified by different labs and schemes respectively) fit together.

28 It is quite obvious that the site visit of the entire development environment would be an extensive world tour which would cost an enormous amount of time and money if the complete ALC material would have been evaluated by one Australian lab. In particular if this has to be done for a number of TOE evaluations.

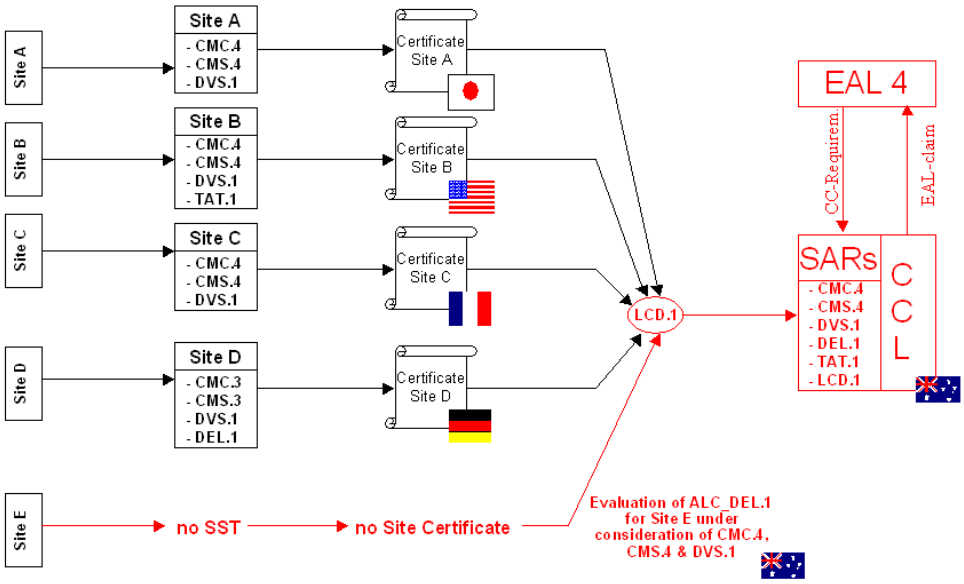


Figure 6: Complete example

3.1.4. Verification of the Splicing Procedure

29 The most crucial point in the Site Certification process is the Splicing procedure. The result of this has an important impact on the assurance which is achieved in the development environment of succeeding TOE evaluations.

30 The assurance of each individual certified site is guaranteed by the ALC criteria itself. However it is not necessarily ensured that a specific combination of certified sites (that means a composed site or an entire development environment of a specific TOE which is based on distributed locations/sites) will also provide the same level of assurance. Therefore there is a need for specific verification measures which can be used to examine whether different sites (including non-certified ALC portions) fit together. The Site Certification process handles this as follows:

31 The Life Cycle Definition criteria (ALC_LCD) are used to ensure that the life-cycle phases of a composed site do not contradict each other but are a mutually supportive combination of different ALC aspects. For the evaluation of an entire development environment or a composed part of the development environment (in choosing the right sites and ensuring that they and also the different life-cycle phases work together correctly), the evaluator has to get an understanding of the complete/composed life-cycle model used by the developer. Therefore the developer provides the underlying life-cycle model to the evaluator in order to describe how each site fulfils the ALC requirements needed for the TOE evaluation. That means ALC_LCD with the related few application notes (see chapter 5.6) gives the necessary confidence that the Splicing process was technically sound and provides the assurance that the life-cycle phases (e.g. represented by different sites) fit together. Besides the technical issues it also has to be confirmed that the Sites Certificates claim an attack potential level which are in line with the claimed AVA_VAN level of the TOE. This is done by checking that the attack potential claim in each Site

Security Target has at least the same level of the AVA_VAN claim as the TOE. This is necessary because the considered attack potential level in ALC_DVS and ALC_DEL has to be commensurate with the chosen AVA_VAN.

32 An efficient life-cycle model will address all aspects of the development and maintenance process and is carried out under an overall management structure that assigns responsibilities and monitors progress. That means it covers the whole life-cycle of the product (TOE) from its planning phase up to its delivery. The most benefit of such a life-cycle definition can be obtained when the information of the entire life-cycle definition is available. This gives assurance that all life-cycle phases used (e.g. represented by the specific sites) for the development fit together and do support each other mutually.

33 But sometimes it can be reasonable to have a description of the life-cycle which does not cover the entire product (TOE) life-cycle but that is only applied to parts of it (e.g. sites which address only parts of the product life-cycle). Therefore the Site Certification process explicitly allows to claim ALC_LCD also for sites which contain only certain life-cycle phases. This leads to the fact that beside all other composed ALC-aspects, LCD itself is probably also a combination of life-cycles aspects/phases related to different sites. In this case the LCD examination done for each individual Site ensures that the contribution of the Site is useful and sound with respect to the product life-cycle of a future TOE. This analysis is done as part of the Site Certification procedure as outlined in chapter 6.1. In addition as already mentioned above an overall LCD analysis is necessary during the Splicing procedure (refer to chapter 6.2) to assess whether the combination of certified with other certified and non-certified Sites fit together in a technical way.

34 For scenarios where the LCD criteria is applied to a partial life-cycle during the Site Certification procedure, application notes are provided in ALC_LCD (for details please refer to chapter 5). For checking the validity of a combination of certified/noncertified Sites during the Splicing procedure application notes can also be found in chapter 5.

3.2. Basic Requirements

35 In order to establish Site Certification within the Common Criteria a few conditions to the Site Certification process have to be defined. They will be described in the following:

3.2.1. Definition of a Site

36 Developers are free to define any part (or the whole) of an existing or anticipated TOE development environment as a site. More specifically:

- A site can be the whole development environment
- A site may consist of one geographical location, be a part of one locations or may span (parts of) multiple locations.

- A site may consist of one organisational unit, be part of an organisational unit, or may span (parts of) multiple organisational units.

37 The scope of a site is defined by a logical and physical boundary. The logical boundary describes the role which the site plays in a product development life-cycle. Whereas the physical boundary is defined by one or more physical locations.

3.2.2. Evidence of the scope of a certified site

38 In order to evaluate a site, first a Site Security Target (SST) must be written which is related to SARs from the ALC family only. The criteria and Evaluation Methodology for SSTs can be found in "Site Security Criteria" (Assurance Class AST – Site Security Target Evaluation, chapter 7 of this document).

39 The SST defines the scope of the certified site and describes aspects of how the site meets the SARs, in particular aspects that are of interest when re-using the site. The list of aspects which has to be covered by an SST are given below:

- SST-Introduction
- Conformance Claim
- Security Problem Definition
- Security Objectives for the development environment
- Extended Components Definition
- Security Requirements
- Site Summary Specification

40 Further guidance on what shall be in each of these SST section will be given in chapter 4.

3.2.3. Minimum Site Requirements

41 For every site a minimum set of requirements has to be fulfilled. One is the assumption that at each site the developer uses a CM system that uniquely identifies all configuration items handled by that Site. The CM system shall have the capability to modify these items in a properly controlled manner. Therefore

- Each site shall be conformant to ALC_CMC.3 or a hierarchically higher CMC component.
- Each site shall be conformant to ALC_CMS.3 or a hierarchically higher CMS component.

42 Another assumption is that the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. In the case that the TOE evaluation is based on more than one certified site these security controls have to be comparable. Therefore

- Each site shall be conformant to ALC_DVS.1 or a hierarchically higher DVS component

43 The Splicing procedure describes in which way several sites can be composed to a bigger site or even whole development environment. But at this point in time a final examination whether the sites fit together in an accurate manner is still missing. Therefore the description how the sites fit together has to be provided by a life-cycle definition of the whole TOE life-cycle which has to be checked against the ALC_LCD.1 (or hierarchically higher) requirements.

44 When using Site Certificates within a TOE evaluation the developer has to provide a life-cycle definition which has to be evaluated according to ALC_LCD.1 (or a hierarchically higher component) (please note that this is valid for evaluation at EAL3 and above). In the case that the development environment of a TOE consists of sites which have valid Site Certificates the certified LCD parts can be reused for this. But the evaluator has to confirm that the sites used are both consistent to each other and in line with the life-cycle definition of the TOE.

45 Please note that it has to be ensured that all ALC requirement dependencies imposed by the CC have to be fulfilled. Since the Site Certification and Splicing procedure do not have a real TOE in the background dependencies outside of ALC do not have to be fulfilled. Nevertheless these dependencies become relevant during the Site Certification Integration procedure, where a TOE is subject to analysis.

3.2.4. Optional Site Requirements

46 Optional Site Requirements are such ALC requirements which can be claimed by a site in addition (or because of a higher EAL) to the Minimum Site Requirements mentioned above. Optional Site Requirements come from following ALC families:

- All other ALC components not mentioned as being mandatory can be claimed as an optional requirement.

- FLR can be claimed as an Optional Site Requirement which is then related to specific life cycle phases but it is up to the Splicing procedure to confirm that FLR is fulfilled completely.

47 While the Minimum Site Requirements (ALC-SARs) have to be fulfilled by every certified site not all sites need necessarily fulfil an Optional Site Requirement. E.g. this will happen in the case that there is no need for a Site to fulfil a certain ALC component because of a lower EAL (E.g. the development

phase of a TOE is almost impossible without using development tools. Requirements on these tools are covered by ALC_TAT but ALC_TAT is not a mandatory requirement for an EAL3 evaluation).

48 Please note that it has to be ensured that all ALC requirement dependencies imposed by the CC have to be fulfilled. Since the Site Certification and Splicing procedure do not have a real TOE in the background dependencies outside of ALC do not have to be fulfilled. Nevertheless these dependencies become relevant during the Site Certification Integration procedure, where a TOE is subject to analysis.

4. Content of a Site Security Target (SST)

49 The SST describes the security features of a site and therefore defines the scope of the site. Evaluating an SST is required to demonstrate that the SST is sound and internally consistent. These properties are necessary for the SST to be suitable for use as the basis for the Site Evaluation/Certification. The criteria and evaluation methodology for SSTs are expressed by the Assurance Class AST – Site Security Target Evaluation (refer to chapter 7).

4.1. Mandatory Contents of an SST

50 The separate sections of an SST and the contents of those sections are briefly summarised below and described in much more detail in the chapters 4.2 to 4.9. An SST normally contains:

a) an SST introduction containing two narrative descriptions of the Site on different levels of abstraction;

b) a conformance claim, showing how the SST claims conformance to the CC;

c) a security problem definition, showing the threats and OSPs that must be countered, and enforced by the Site;

d) security objectives, showing how the Site will counter the threats and enforce the OSPs;

e) extended components definition, where new components (i.e. not included in CC Part 3) may be defined. These new components are needed to define extended assurance requirements;

f) security requirements, where a translation of the security objectives into a standardized language is provided in the form of the SARs

g) a Site summary specification, summarizing how the Site implements the SARs.

51 Each section is described in more detail in the following sections.

4.2. SST Introduction (AST_INT)

52 The SST introduction describes the Site in a narrative way on two levels of abstraction:

a) the SST reference and the Site reference, which provide identification material for the SST and the Site that the SST refers to;

b) the Site description, which describes the Site in more detail.

4.2.1. ST reference ad TOE reference

53 An SST contains a clear SST reference that identifies that particular SST. A typical ST reference consists of title, version, authors and publication date. The reference must be unique so that it is possible to distinguish between different SSTs and different versions of the same SST.

54 An SST also contains a Site reference that identifies the Site itself. A typical Site reference identifies the geographical location of the Site and the organisation(s) at that Site.

4.2.2. Site description

55 A Site description is a narrative description of the Site. The Site description should provide evaluators and developers with a general understanding of the Site.

56 The Site description discusses the physical scope of the Site: a list of all geographical locations that the Site consists of, consisting of the full address and general nature (e.g. plant, building, floor) of the Site. A photograph or map of the Site may assist comprehension.

57 The Site description should also discuss the logical scope of the Site: organisation(s) at the Site, the general processes occurring at the Site, and the various items and/or documents processed at the Site, and the relation that the Site may have with any lifecycle phases of TOEs likely to be designed, developed, produced or otherwise processed at the Site.

58 If the Site consists of more than one geographical location, the logical scope should be discussed separately for each geographical location. If there are multiple organisations at the same geographical location, the logical scope should be discussed separately for each organisation.

4.3. Conformance claims (AST_CCL)

59 This section of an SST describes how the SST conforms with the Common Criteria itself. This description consists of three items:

- The version of the CC that is used and whether the SST contains extended assurance requirements or not.
- Identification of the SARs which are in the scope of the site.
- The level of attack potential the site is appropriate to.

4.4. Security problem definition (AST_SPD)

4.4.1. Introduction

60 The security problem definition defines the security problem that is to be addressed. The security problem definition is, as far as the CC is concerned,

axiomatic. That is, the process of deriving the security problem definition is outside the scope of the CC.

61 Note that it is not mandatory to have statements in all sections, an SST can have no threats, or no OSPs, or no assumptions. However, if an SST has no threats, it must have OSPs, and if an SST has no OSPs it must have threats.

62 Also note that if the Site has multiple geographical locations, or multiple organisations, it may be better to discuss the relevant threats and OSPs separately for distinct locations/organisations.

4.4.2. Threats

63 This section of the security problem definition shows the threats that are to be countered by the Site.

64 A threat consists of a threat agent, an asset in the Site and an adverse action of that threat agent on that asset.

65 Threat agents are entities that can adversely act on assets. Examples of threat agents are hackers, users, computer processes, TOE development personnel, and accidents. Threat agents may be further described by aspects such as expertise, resources, opportunity and motivation.

66 Assets can be files, documents, processes at that site that are likely to be used in the design, development, production or other processing of a TOE, and, when the asset is damaged, will likely negatively impact that TOE.

67 Adverse actions are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value.

68 Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential TOE design files from the Sites network;
- a TOE developer employee making an accidental error affecting the correctness of the low-level design of the TOE;
- a malicious TOE developer employee (with very substantial expertise on the source code, but not many other IT security skills) modifying the source code;
- a cleaner stealing confidential design information and/or source code.

4.4.3. Organisational security policies (OSPs)

69 This section of the security problem definition shows the OSPs that are to be enforced by the Site.

70 OSPs are rules, practises, or guidelines. These may be laid down by the organisation controlling the Site, or they may be laid down by legislative or regulatory bodies.

71 Examples for OSPs are "All products that are used by the MoD must be developed by developers that obey National Defense Guidelines for Development, v1974-2" or “The internal audit and maintenance tasks shall ensure the correct and continuous operation of the equipment and tools used to control and secure the site”.

4.5. Security objectives (AST_OBJ)

72 The Site contains technical and procedural measures to provide assurance that any TOE or part thereof that is developed on that Site will work correctly. This is described by the security objectives for the Site and consists of a set of statements describing the security goals that should be achieved in the Site.

73 Examples of security objectives for the Site are:

- The Site shall ensure that any TOE is delivered to the consumer without compromising the integrity of the TOE;
- The Site shall ensure that the integrity of all TOE-relevant documents is protected;
- The development environment shall conform with EAL 4 augmented with ADV_IMP.2.

74 If the Site consists of multiple geographical locations or organisations, it may be better to subdivide the security objectives for the Site into several sections to reflect this.

4.6. Relation between security objectives and the security problem definition

75 The SST also contains a security objectives rationale containing two sections:

- a tracing that shows which security objectives address which threats and OSPs (and assumptions). This tracing is identical to the tracing required for security objectives in STs.
- a set of justifications that shows that all threats and OSPs are effectively addressed by the security objectives. These justifications are identical to the justifications required for security objectives in STs.

4.7. Extended Components Definition (AST_ECD)

76 This section is identical to the Extended Components Definition of an ST. The only difference is that it is not allowed to define SFRs for a Site and the SARs defined in a SST need to have a relation to ALC.

4.8. Security requirements (AST_REQ)

77 The security requirements section for an SST consists of a set of SARs (SSTs have no SFRs). The SARs are a description of how the TOE is to be evaluated. The SARs are identical to that of an ST, with two major exceptions:

- An SST may only contain SARs from the ALC class;
- An SST must contain at least:
  - ALC_CMS.1: without this requirement it is unknown which configuration items are processed by the Site;
  - ALC_CMC.3: without this requirement it is unknown how the configuration items are identified and whether this is correctly and consistently done;
  - ALC_DVS.1: without this requirement it is unknown whether the confidentiality and integrity of the configuration items is sufficiently protected;

78 In addition, the SST must contain a security requirements rationale. This security requirements rationale must contain:

- a tracing that shows which SARs address which security objectives;
- a set of justifications that show that all security objectives for the Site are effectively addressed by the SARs.

4.9. Site summary specification (AST_SSS)

79 The Site Summary Specification (SSS) is the most important section of an SST. It should identify all evidence that was needed for the Site to meet the SARs, and describe aspects of how the Site met the SARs and regarding ALC_DEL and ALC_DVS how it fulfils the attack potential claim made in the SST.

80 It is up to the developer to determine the extent and granularity of these aspects.

81 However, as SSTs are intended to allow re-use of the certified Site in other evaluations, certain points should be taken into consideration. It is especially important to describe all relevant aspects of the external behaviour of the Site, that is: how it interacts with the remainder of the Development Environment. The SSS has to describe WHAT will be

- required from the remainder of the development environment
- provided to the remainder of the development environment

82 but not HOW this is provided (the detailed process). Internal behavior can and should be described in the SSS as long as it is deemed necessary for the fulfillment of the objectives.

83 It is allowed to give as much detail as one wants. Too little detail will fail evaluations that try to re-use this SST, as it cannot be determined what the site does. Too much detail will lead to problems with clarity and understanding. One should also realize that the SST may be a public document so confidential Site security issues may be left out.

84 Each description must have a reference to the underlying evaluation documentation as well. Furthermore all documents used as evaluation evidence during the Site Certification procedure have to be listed as well.

85 For ALC_CMS, one should describe in the SSS only those configuration items that are provided to the site from outside the site and those items that are provided by the site to outside the site. Any items that exist only "inside" the site should not be described.

86 For ALC_CMC, one should describe all elements that are relevant for identifying and labeling different versions of the configuration items listed by ALC_CMS and the relation between these two. Usually, no other CM information has to be provided, as this is internal to the Site.

87 For ALC_DVS, one should describe the security of the configuration items listed for ALC_CMS while being transported to/from the site and what is expected from the other side. Here he has to give a clear statement that the underlying DVS procedures are appropriate for the attack potential level claimed in the SST because the considered attack potential level in ALC_DVS has to be commensurate with the chosen AVA_VAN in later TOE evaluations. No other DVS information has to be provided as this is internal to the Site.

88 For ALC_LCD, one should describe what the role of the site is in making TOEs, and where it will fit in a likely life-cycle model for that TOE. This should be identical to the life-cycle information in the Site Description provided as part of AST_INT.

89 For ALC_TAT, in general all use of Tools and Techniques is "inside" the Site. This means that usually NO information on ALC_TAT has to be provided here.

90 For ALC_DEL, one only has to list all parts of the TOE that are delivered to the consumer. The process of delivery does not have to be described. In addition he has to give a clear statement that the underlying delivery procedures are appropriate for the attack potential level claimed in the SST because the considered attack potential level in ALC_DEL has to be commensurate with the chosen AVA_VAN in later TOE evaluations.

5. Interpretation of the ALC Requirements in terms of the Site Certification Process

91 It is neither the intention nor the necessity to change the general content of the criteria and/or the methodology of the Common Criteria. Merely some adaptations or specific explanations are needed to apply the Site Certification procedures in a correct manner. Most of them can be done by including a few new terms and by defining Site Certification related Application Notes which give instructions how to use (interpret) certain CC-Requirements (C-Element).

92 This chapter describes in the following all these parts of the CC ([1], [2] and [3]) and CEM ([4]) which need clarification in terms of the Site Certification process.

General Application Note for all ALC requirements

How to interpret the term "TOE" concerning Site Certification

93 According to the CC, part 1, paragraph 224 it is possible to evaluate a TOE (or parts of a TOE) in parallel to its development. This means especially for the ALC requirements that the examination of the development environment is probably done without having a (final) TOE available. Even more it is common sense that for a CC conformant development environment appropriate procedures are in place before the actual TOE development/evaluation starts.

94 Therefore most of the ALC requirements should be applicable to a development environment without a TOE. Only certain ALC requirements which are inseparably linked to a TOE would have to be interpreted if subject to a Site Certification process. For these requirements, the processes themselves rather than the actual outcome would move into the focus of the examination. E.g. considering CMC.x.1C it would be important now to check whether there is a process in place which ensures an appropriate labelling of a TOE rather than checking the labels on a TOE itself.

Which Configuration Items are in the scope of the Site Certification Process

95 For the term "Configuration Items" the following distinction has to be made. For configuration items which are not closely linked to a TOE or are not part of a TOE (e.g. development tools, ALC documentation, ...) no further interpretation is necessary and the ALC criteria can be applied as it is. For configuration items which have a strong relation to a TOE or are a part of it (e.g. design documentation, implementation representation, ...) the processes to manage those items move into the focus of the site evaluation.

How to consider Dependencies and the required Input Documents

96 As already mentioned above it has to be ensured that all ALC requirement dependencies imposed by the CC have to be fulfilled. Since the Site Certification and Splicing procedures do not have a real TOE in the background dependencies outside of ALC do not have to be fulfilled. Nevertheless these dependencies become relevant during the "Site Certification Integration" process, where a TOE is subject of an analysis.

97 Input documents as required by ALC CEM workunits are relevant if they are not related to a specific TOE. TOE specific input documents (e.g. like ST, implementation representation) have to be considered during the "Site Certification Integration" process. The input requirement ST has to be interpreted as SST for the "Site Certification" and "Splicing" procedure. Please consider also more specific interpretations given together with the work units below.

5.1. Application Notes for ALC_CMC

98 For Site Certification the processes of the CM system are subject of examination in ALC_CMC.

99 For some requirements ALC_CMC can not be applied the way it is written, as it assumes that a site handles a specific TOE. This is not necessarily the case because the Site Certification procedure by definition allows to certify sites independently to a TOE evaluation.

100 There is a dependency from ALC_CMC.3 (and hierarchically higher) to ALC_LCD.1. Since LCD is not necessarily covered by a site (because it is an Optional Site Requirement) which is under Site Certification this dependency can not be fulfilled at that time. The reason for this dependency is to ensure that there is a CM system in place for the entire development environment of the TOE. To assess this knowledge of all life cycle phases (and in terms of Site Certification knowledge of all sites) and confidence that different life-cycle phases work together correctly is necessary. But this can not be done for a single site if the site does not represent the entire development environment. The analysis of the life-cycle is therefore part of the Splicing procedure which will be performed later on. That means the dependency from ALC_CMC to ALC_LCD is covered during the TOE evaluation (by applying the Splicing procedure) in any case.
Please note that a site which claims ALC_LCD and does not represent the whole development environment of the TOE does not completely fulfil this dependency.

101 In the following application notes are given for those requirements which need interpretation. ALC_CMC.5 is used because all lower ALC_CMC components can be derived from this.

Application Notes for Site Certification:

ALC_CMC.5.1D The developer shall provide the TOE.

The processes rather than a TOE are in the focus of the CMC examination (i.e. there is no need to provide a TOE for Site Certification). The developer requirements to provide the required process descriptions are covered by ALC_CMC.5.2D and ALC_CMC.5.3D. It is imaginable that a TOE could be provided as an evidence for the application of the procedures.

ALC_CMC.5.1C The CM documentation shall show that a process is in place to ensure an appropriate and consistent labelling.

If a site does not handle the entire TOE/product the criteria should be interpreted in a way that only the parts of a TOE/product which are relevant to the site are subject of the examination.

ALC_CMC.5.8C The CM system shall clearly identify the configuration items that comprise the TSF.

Since there is no specific TOE in the main focus of the Site Certification the evaluator should only select such kind of configuration items which are in the scope of the certified site like CM tools/documentation or development tools for example.

ALC_CMC.5.12C The CM documentation shall include a CM plan.

A CM plan is normally not available before a specific TOE/product development project started. Therefore the CM documentation shall include instructions that TOE/product developments to have to be performed according a well defined CM plan. The aspects on which the CM plan is based are given in CEM workunit ALC_CMC.5-15 (ALC_CMC.13C).

ALC_CMC.5.13C The CM plan shall describe how the CM system is used for the development of the TOE.

Refer to ALC_CMC.5.12C.

ALC_CMC.5.16C The evidence shall demonstrate that all configuration items have been and are being maintained under the CM system.

Refer to ALC_CMC.5.8C.

ALC_CMC.5-20: The evaluator shall determine that the application of the production support procedures results in a TOE as provided by the developer for testing activities.

The Processes rather than the TOE are in the focus of this workunit. It is imaginable that applying the procedures to a TOE/product (or e.g. earlier versions of them) can be used as additional evidence.

5.2. Application Notes for ALC_CMS

102 ALC_CMS can not be applied to all sites the way it is written, as it enforces use of configuration items that a site may neither possess nor control. Furthermore there is not necessarily a specific TOE (because of the definition of Site Certification) in the background. That means the configuration list (which is the basis of the ALC_CMS requirements) can not contain TOE specific configuration items.

103 Nevertheless there is a need to ensure that for all developers there is a procedure in place which ensures both the existence of an configuration list for all products under evaluation and a well defined structure and content of that configuration list. The ALC related aspects itself, which have to be covered by a configuration list must be considered as required in the criteria already

during the Site Certification activities. For all other configuration items which are TOE dependent the evaluation of them in terms of the required CMS activities are covered while evaluation all other remaining CC aspects.

104 In the following application notes are given for those requirements which need interpretation. ALC_CMS.5 is used because all lower ALC_CMS components can be derived from this.

Application Notes for Site Certification:

ALC_CMS.5.1C The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; the parts that comprise the TOE; the implementation representation; security flaws; and development tools and related information. The CM documentation shall include a CM plan.

Since a TOE is not directly in the focus of Site Certification parts of the requirement are not applicable. Nevertheless all items of the CM list which are not TOE dependent and relevant for the site (e.g. development, test and production tools, ALC evaluation evidence) have to be provided on the CM list and are subject of CMS the analysis.

For the consideration of the TOE/product specific configuration items in the configuration list the CM system (CM documentation) has to provide clear instructions how to consider these items in the list. That means there must be a procedure which gives directions about the structure and the content of the required configuration list and that the configuration list at least shall fulfil the CMS.x requirements. E.g. for workunit ALC_CMS.5-1 that point a), b) c) and e) are not applicable for site certification as it is written. For them the evaluator has to focus on the procedure mentioned above. He has to ensure that all configuration items are considered which have to be included in the configuration list required by the claimed CMS component in the SST. Point d) refers to the SARs claimed in the SST and point f) to the tools which are in the scope of the site.
During the TOE evaluation every configuration item will be checked again anyway. While evaluating all CC aspects the evaluator has to check which configuration items are relevant for the evaluation. This information is provided by the configuration list of the TOE which contains now all TOE related items required by the claimed CMS component. In the case there are configuration items missing one would have an inconsistency between this special CC aspect to the evaluated CMS requirement claimed in the SST. That would lead to a non-fulfilment of paragraph 57 in the CEM and a fail verdict of that special CC aspect.

ALC_CMS.5.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Not applicable for Site Certification as it is written. For this requirement a process shall be in place that makes it mandatory for the developer to indicate which subcontractor developed which configuration item and that the subcontractors have to be listed (and

linked to the related configuration item) in the configuration list.

5.3. Application Notes for ALC_DEL

105 ALC_DEL should only be applied to sites that actually deliver to users, as it will fail otherwise. The delivery documentation shall cover all delivery procedures which are in the scope of the site. Thus, different (evaluated) delivery measures can be applied by the same site and therefore makes this site more efficient as defined by the Site Certification process.

106 The developers who are going to claim ALC_DEL for a specific site should take into account that the delivery procedures which are under evaluation consider the nature of the intended TOE/product developments. An accurate delivery procedure shall commensurate with both the chosen component of the Vulnerability Assessment (AVA_VAN) and the security aspects integrity, confidentiality and availability which are deemed relevant for a specific TOE/product.

Application Notes for Site Certification:

107 None. CEM paragraph 1078 also sufficiently covers Site Certification.

5.4. Application Notes for ALC_DVS

108 ALC_DVS can be applied to all sites but shall consider following application notes in detail.

Application Notes for Site Certification:

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

If the Site is unequal to the entire development environment of a TOE, workunit ALC_DVS.2-1 is clarified to:
[...]
The development security documentation should identify the physical locations within the site at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations within the site and transportation from/to the site and the remainder of the development environment. Transport of the finished TOE to the user does not fall under ALC_DVS but is dealt with in Delivery (ALC_DEL).
[...]

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

As there is not necessarily a TOE evaluation running the evidence needed may be taken from previous TOE/product developments. At least the evaluator should assess the evidence of security measures

which are TOE independent.

Another possibility to get evidence that the security measures stated in the development documentation are followed can be achieved while performing a site visit which is handled by ALC_DVS.2.2E.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

The Site Certification process is by definition independent from a specific TOE evaluation. Even more a site once certified should fulfil various levels of security needs dependent on future TOE developments. Thereby specific circumstances of the intended TOE developments are covered as much as possible. This means the focus of ALC_DVS.2.3C is not a justification of security measures related to only one specific TOE, but it is a justification related to possibly different combinations of security measures implemented in the site. Each of this justified combination can be applied for further TOE evaluations. Of course for sites where it is obvious that only one type of TOE is developed by using the same security measures it is sufficient to justify this specific case (combination of measures).

5.5. Application Notes for ALC_FLR

109 The objective of this sub-activity is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

110 The basis of ALC_FLR is the same as for all other ALC aspects while applying the Site Certification process. At the time of the evaluation of the flaw remediation procedures there is not necessarily a specific TOE already there. As for the other ALC aspects it is task to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.

111 Although FLR is based on very special procedures which could be described in separate documentation and guidance the flaw remediation procedures do not have to be in contradiction to the certified ALC aspects like the CM system for example. On the contrary it is likely that the flaw remediation process uses most of the procedures related to the other ALC families.

112 Therefore with regard to the Site Certification, FLR is an Optional Site Requirement. But it is important to note that FLR covers almost all life cycle phases of the development environment of the TOE (i.e. if a corrective action has to be implemented it is likely that this will be done in a similar way to the actual development of the product itself). That leads to the fact that in the case of a distributed development environment it is likely that FLR as whole is distributed in a similar way. That means an individual site can claim FLR for all or parts of the claimed life cycle phases in the related SST but it is up to the Splicing procedure to confirm that FLR is fulfilled completely.

5.6. Application Notes for ALC_LCD

113 By definition, the life-cycle spans the entire development environment of a TOE, and a site may only cover part of the development environment. If the site is not equal to the entire development environment, the ALC_LCD criteria have to be interpreted in a way that only those life-cycle phases have to be evaluated which are in the scope of the site.

114 ALC_LCD addresses the requirements to a specific TOE life-cycle. However it is the intention of the Site Certification process to evaluate life-cycle models once and use them for a couple of TOE/products under the same life-cycle model. Therefore the life-cycle models which are intended to be used should be examined independent from a specific TOE. For this the developer shall classify the types of TOEs he is going to develop and provide clear process instruction how to define/instantiate a TOE specific life-cycle model. The evaluator focuses his examination on the developers TOE classification and the LCD process instruction.

Application Notes for Site Certification:

ALC_LCD.2.4D The developer shall provide life-cycle output documentation

Rather than the life-cycle output itself the process documentation which describes which kind of metrics have been chosen and why those metrics have been chosen are subject of the developer element. Those metrics are subject which help to increase the quality of the product(s) and/or development process, which in turn increases assurance in the security of the TOE/product.

ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

This element requires information about the life-cycle used by a subcontractor if any. But it is not in every case possible to determine in advance whether parts of the TOE which are developed by third parties will be integrated in the final TOE. Therefore the evaluator has to examine the developer documentation that it gives clear instructions under what conditions (in terms of the life-cycle model which has to be used) a subcontractor has to develop his products that are intended to integrate into the TOE.

ALC_LCD.2.3C The life-cycle output documentation shall provide the results of the measurements of the TOE development using using the measurable life-cycle model.

Assurance should be gained on the documents required by the interpretation of ALC_LCD.2.4D and not on specific life-cycle output documentation.

Application Notes for Splicing:

115 If ALC_LCD is used for Splicing the following interpretation shall apply. Rather than examining those life-cycle phases which are in the scope of the site now the interfaces between the sites which have to be spliced together become subject. This shall ensure that the Splicing is done in a sound manner and the Sites fit together.

5.7. Application Notes for ALC_TAT

116 ALC_TAT in principle can be applied to any site but have to be claimed by sites which develop, analyse and implement TOEs (for EAL >=4 or augmented EALs). However, with regard to the Site Certification process there are following interpretations of special requirements necessary.

117 For some requirements ALC_TAT can not be applied the way it is written, as it assumes that a site already developed a specific TOE. This is not necessarily the case because the Site Certification process by definition allows to certify sites independently to a TOE evaluation. Therefore in context of ALC_TAT the TOE shall be read as a TOE/product which will be developed in the future by using the development tools that have to be certified according ALC_TAT. For these kind of requirements no further application notes will be provided in the following.

118 There is a dependency from ALC_TAT.1 (and hierarchically higher) to ADV_IMP.1. Since there is not necessarily a specific TOE while evaluating/certifying a site this dependency can not be fulfilled at that time. The reason for this dependency is to determine whether the developer has used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results. Beside the development tool documentation the evaluator needs evidence also at least a subset of the implementation representation. As already stated in the criteria this work can be done while evaluating ADV_IMP which means a possible fail verdict can be issued during the TOE evaluation.

Application Notes for Site Certification:

ALC_TAT.3.2D The developer shall document the selected implementation-dependent options of the development tools.

Since not necessarily a TOE is in the background of a Site Certification the requirement is not applicable as it is. Furthermore it is the task of the developer to show that he has procedures in place that ensure that such implementation-dependent options are recorded/documented during the development process.

Confidence that these procedures are in place can be gained e.g. by presenting documentation which shows how those options have to be documented. Furthermore it can be supported by showing the application of those documented procedures for former or different TOEs/products or by gaining assurance during a site visit.

ALC_TAT.3.3D The developer shall describe the implementation standards for all parts of the TOE.

First of all it has to be clear that all tools and techniques in terms of the definition of ALC_TAT have to be described which are intended to be used for TOE/product developments. Up to ALC_TAT.2 only those tools and techniques are in the focus that are applied by the main developer only. Parts of the TOE/product which are (partly) developed by a subcontractor are not in the scope of an evaluation.

In addition to this ALC_TAT.3 requires also information about the

tools and techniques used by a subcontractor. But it is not in every case possible to determine in advance whether parts of the TOE which are developed by third parties will be integrated in the final TOE. Therefore the evaluator has to examine the developer documentation that it gives clear instructions under what conditions (in terms of development, analysis and implementation) a subcontractor has to develop his products which are intended to be integrated into the TOE.

ALC_TAT.3.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

Since there is not necessarily a TOE evaluation running at the time the site is going to be certified this requirement is not applicable as it is written. However the evaluator can gain confidence that the development tool documentation covers all statements which will be used for TOE developments in the future by following measures:

- The developer provides process instructions for the development staff which makes it mandatory that only such statements should be used in the implementation representation that are defined in the development tool documentation.

- The evaluator may have the opportunity to verify certain implementation representations developed for former TOEs/products in order to confirm that the development process instruction have actually been followed.

- Interviews with the development staff to check that all development process instructions and the underlying development tools and techniques documentation are well known.

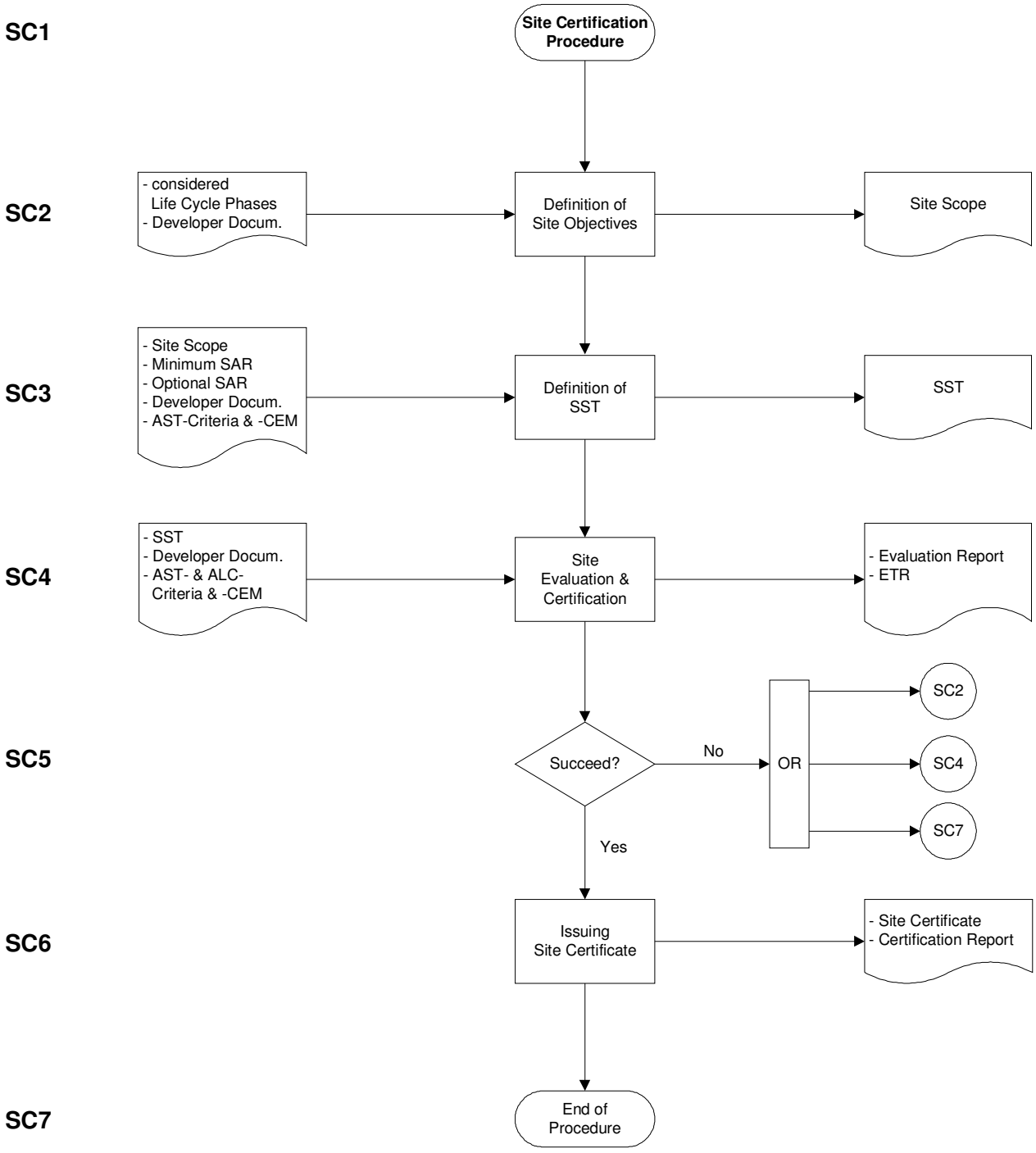
ALC_TAT.3.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Refer to the interpretation given for ALC_TAT.3.2D.

6. Process description

6.1. Site Certification Procedure

6.1.1. Symbolic Description (Flowchart)



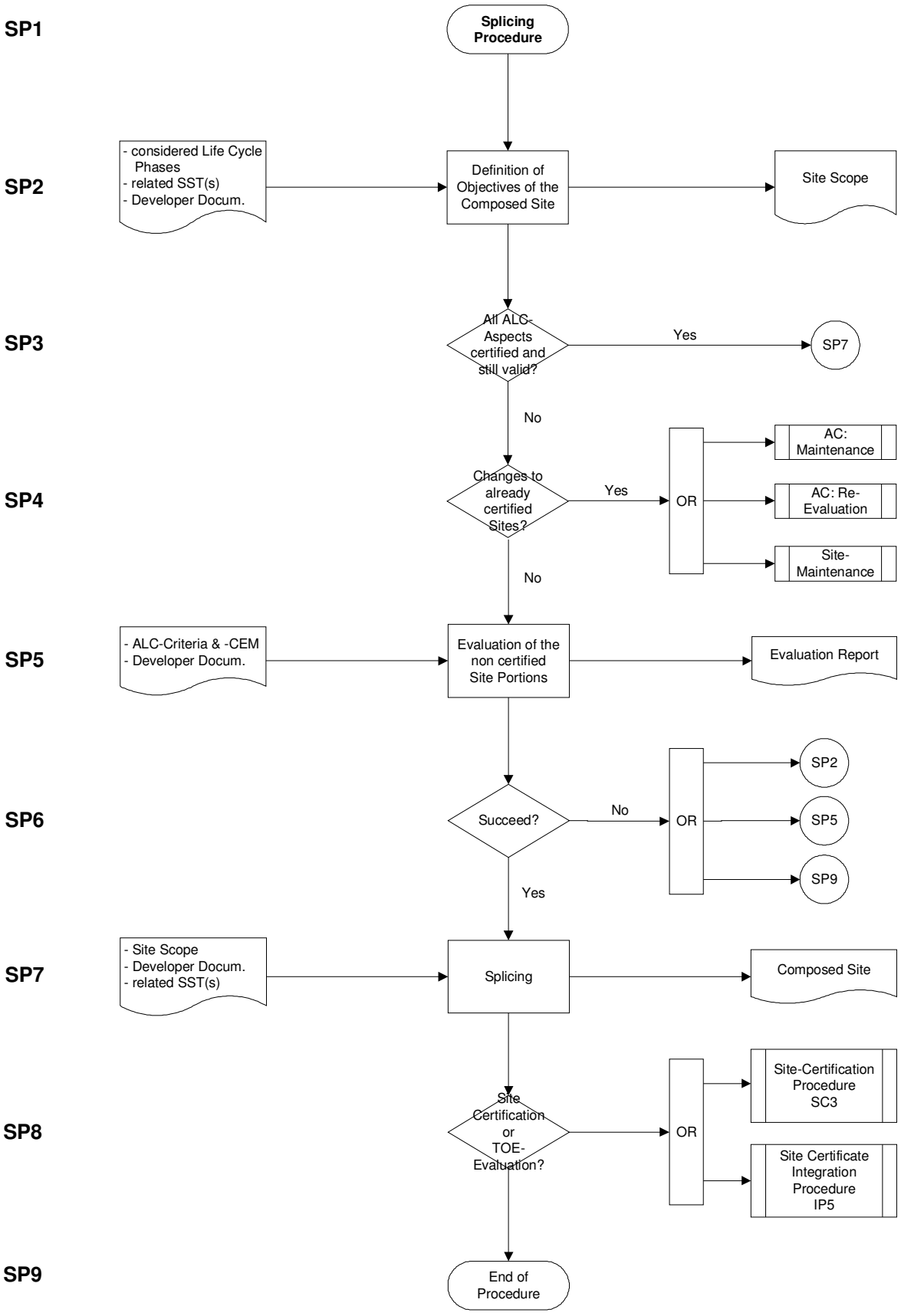
6.1.2. Informal Description

Process Step	Explanation
SC1	Initialisation of a Site Certification Procedure This process is used to certify one site which covers one or more life-cycle phases or parts of it of a potential TOE/product. Please note that if a composed site shall be certified the Splicing procedure has to be used first. **This procedure can be used for both sites which have not been certified yet and sites whose site certificates are going to be updated.**
SC2	The developer has to define the objectives for the site to be certified. As an input he needs (as a minimum): • Knowledge which life-cycle phases are covered by the site. • Developer documentation which would be used as evidence during an evaluation. The developer documentation has to be complete in terms of these ALC aspects which will be covered by the site certificate. As a result the scope of the site to be certified is defined and will be used as an input for the SST (in SC3). Detailed information on how a site has to be defined (logically and physically) are given in chapter 3.2.1 and in chapter 7.
SC3	The SST can be defined and written by using: • the site scope (defined in SC2), • the Minimum and Optional Site Requirements (SARs), • the complete ALC documentation of the developer which are relevant for the specific Site Certification and • the AST criteria the SST can be defined and written. An overview on the content of an SST are given in chapter 4. For detailed information what is required for an SST please refer to the AST criteria and methodology in chapter 7.
SC4	The evaluation and certification of the site is done by examining the SST according the AST criteria and the relevant ALC documentation of the site itself according the ALC criteria [3] and its methodology [4]. The ALC evaluation procedure applied are identical to usual evaluations. To document the results of the examination evaluation reports and an ETR have to be provided to the certification body. Please note that the ALC and AST related application notes as defined in chapters 5 and 7 have to be used.
SC5	If no successful evaluation is possible the process is set up again at the

Process Step	Explanation
	respective process steps. A jump to SC2 would mean to re-define the site scope/site objectives. A formal evaluation fault could lead to a re-definition of the SST (jump to SC3). If fundamental problems are encountered during the evaluation/certification the procedure can be terminated by jumping to SC7.
SC6	If the evaluation/certification was successful a site certificate can be issued and a certification report will be compiled.
SC7	End of procedure.

6.2. Splicing Procedure

6.2.1. Symbolic Description (Flowchart)



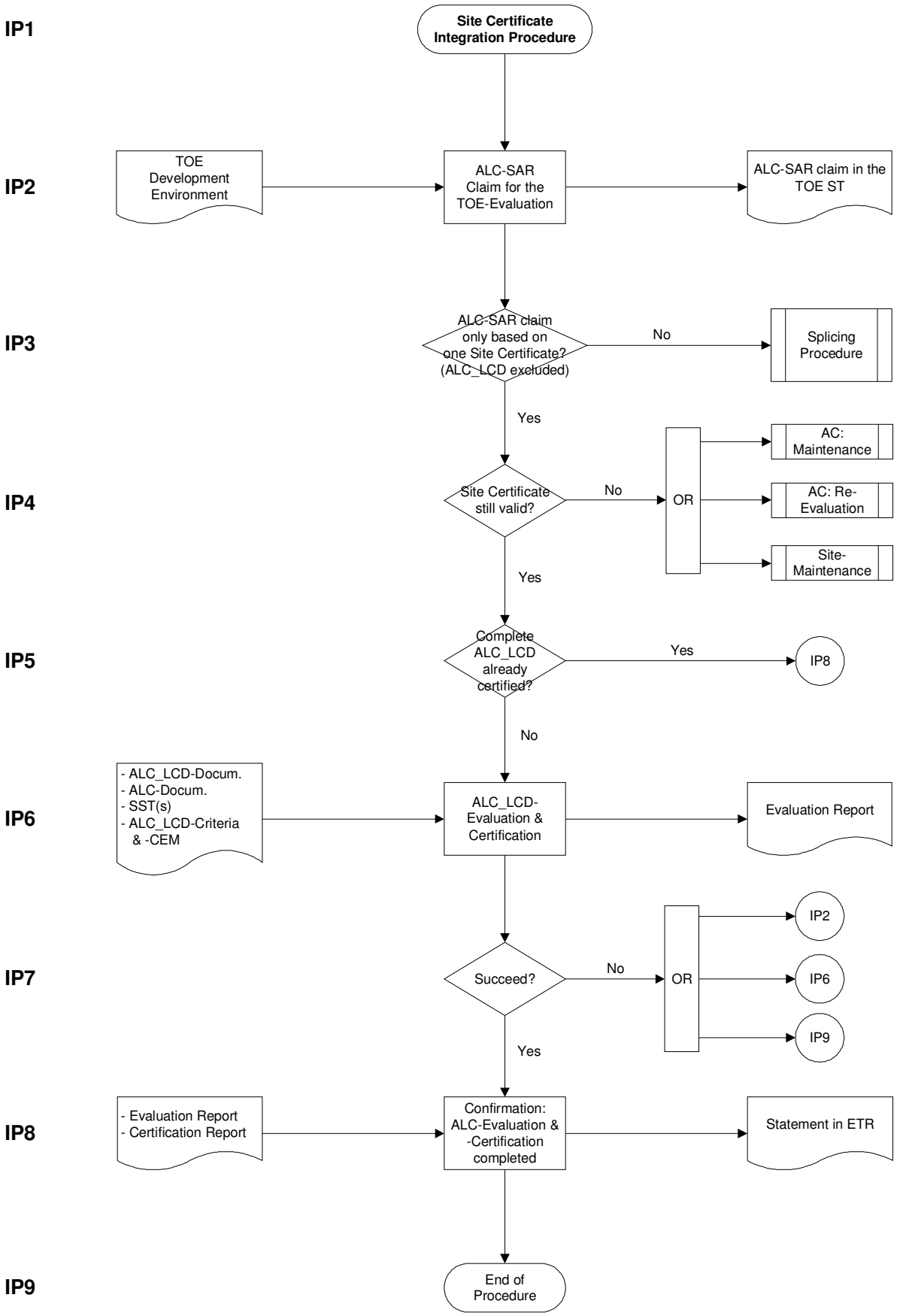
6.2.2. Informal Description

Process Step	Explanation
SP1	Initialisation of the Splicing Procedure This procedure is used by the developer to combine certified sites and non-certified ALC portions to a useful composed site. The intention to start this procedure is either to get a certificate for a composed site or use the composed site in a TOE evaluation (without a certificate on the composed site). Please note that it is not required that all splicing inputs have to be in the scope of one of the certified sites used. It is allowed to consider also these ALC items in the case that they have been evaluated separately. For more details please refer to chapter 3.1.
SP2	The developer has to define the objectives for the composed site to be certified. As an input he needs (as a minimum): • Knowledge which life-cycle phases are covered by the composed site; • SSTs of certified sites used as part of the composed site and • Developer documentation of non-certified ALC-portions of the composed site which would be used as evidence during an evaluation (of non-certified portions). As a result the scope of a composed site will be defined. In case the background of the Splicing Procedure is to do a TOE evaluation the site scope shall cover the whole development environment required for the intended TOE evaluation. If the intention is to combine two different sites to only one bigger site then the site scope covers not necessarily all life-cycle phases of a TOE/product. Detailed information on how to define a site (logically and physically) are given in chapter 3.2.1 and in chapter 7.
SP3	In this process step the validity of a Site Sertificate is checked by the evaluator. This check has to consider two different aspects: • Compliance of the content in terms of both technical aspects as well as required assurance aspects • Compliance of validity in terms of the time-limited site certificates If the certificate are still valid the process continues with SP7.
SP4	In the case that a Site Certificate is not valid any more there are the following options possible: • Only minor changes to the site have happened and thus Assurance Maintenance as defined in the CC Assurance Continuity process can be applied

Process Step	Explanation
	• Bigger changes have happened and the site has to be re-certified to be able to use a certificate in this Splicing procedure • Site-Certification-Maintenance by using the CC Assurance Continuity process. • If the certificate is outdated only a re-evaluation is possible.
SP5	Use the Developer documentation and the ALC criteria [3] and its methodology [4] to evaluate the non-certified portions of the composed site. The ALC evaluation procedures applied are identical to usual evaluations. Results of this step are evaluation reports and an ETR of the non-certified portions.
SP6	If the evaluation of the non-certified portions was not successful the process is set up again at the respective process steps. A jump to SP2 would mean to re-define the composed site scope/composed site objectives. A formal evaluation fault would lead to a repetition of the evaluation cycle (jump to SP5). If fundamental problems are encountered during the evaluation the procedure can be terminated by jumping to SP9
SP7	In this process step the actual Splicing takes place. This is to combine the certified sites and evaluated non-certified portions to a composed site. Detailed information on how to do Splicing is given in chapter 3.1.
SP8	The result of the Splicing process can now be used either for certification of the composed site (jump to procedure “Site Certification”, step SC2) or in a regular TOE evaluation (jump to procedure “Site Certificate Integration”, step IP5).
SP9	End of procedure.

6.3. Site Certificate Integration Procedure

6.3.1. Symbolic Description (Flowchart)



6.3.2. Informal Description

Process Step	Explanation
IP1	Initialisation of a Site Certificate Integration procedure This procedure describes how already certified ALC material (as a result of the Site Certification procedure and the Splicing procedure) can be re-used during a regular TOE evaluation / certification.
IP2	Starting from the development environment of a specific TOE and considering the targeted EAL, the ALC relevant SARs can be deduced by the developer. Those SARs can then be claimed in a TOE Security Target according the ASE criteria [3] and its methodology [4].
IP3	There are three different scenarios imaginable. The TOE life-cycle is based on a) only one certified site, b) more than one certified site or c) more than one certified site and uncertified additional portions. In case of b) or c) the Splicing procedure would have to be applied first. For a) it will be proceeded with the next step of the procedure. Detailed information in this matter is given in chapter 3.1 particularly figure **5**. Since it is not mandatory to include ALC_LCD into a site certificate this aspect need not to be considered for the decision which has to be done under IP3. This issue will be checked in any case under step IP5 later on.
IP4	In case that the Site Certificate is not valid any more there are following options possible: • Only minor changes to the affected site have happened and thus Assurance Maintenance as defined in the CC Assurance Continuity process can be applied • Bigger changes have happened and the affected Site has to be re-certified to be able to be used • Site-Certification-Maintenance by using the CC Assurance Continuity process. • If the certificate is outdated only a re-evaluation is possible.
IP5	If the entire life-cycle of the TOE is covered by the certified site no additional work has to be done by the evaluator and it can be proceeded with IP8. Please note that the Site Certification process requires LCD.1 also for EAL3 evaluations. For more background on this requirement please refer to chapter 3.2.3.
IP6	In this process step the Site Certificate does not contain ALC_LCD. Therefore this assurance requirement has to be evaluated and certified. As an input for

Process Step	Explanation
	this activity the following information is used: • Developer documentation of ALC_LCD • SST(s) and • Additional Developer Documentation as necessary ALC_LCD documentation will be evaluated according to CC [3] and CEM [4]. The ALC evaluation procedure applied are identical to usual evaluations. An evaluation report about ALC_LCD is written as result of this process step.
IP7	If the evaluation of ALC_LCD was not successful the process is set up again at the respective process steps. A jump to IP2 would mean to re-define the development environment. A formal evaluation fault would lead to a repetition of the evaluation cycle (jump to IP6). If fundamental problems are encountered during the evaluation the procedure can be terminated by jumping to IP9.
IP8	All ALC requirements as claimed in the TOE Security Target have been considered at this point (either by Site Certificates, by Splicing or ALC_LCD in IP6).
IP9	End of procedure.

7. Class AST: Site Security Target evaluation

119 *This chapter defines the Security Assurance Requirements used to evaluate Site Security Targets (SSTs) as defined and used in the Site Certification process. It contains a mix of CC and CEM information, in order to make the chapter self-contained. For each section of the SST, first the criteria are listed and then the methodology is provided.*

120 *Please note that SSTs can not claim compliance to PPs or packages. There are no Site PPs.*

121 A SST shall meet all the components listed in this chapter.

122 Evaluating an SST is required to demonstrate that the SST is sound and internally consistent. These properties are necessary for the SST to be suitable for use as the basis for a Site evaluation.

123 This chapter should be used in conjunction with Chapter 4 of the process description of the Site Certification process, as this chapter clarifies the concepts used here and provides many examples.

124 Figure 7 shows the families within this class, and the hierarchy of components within the families.

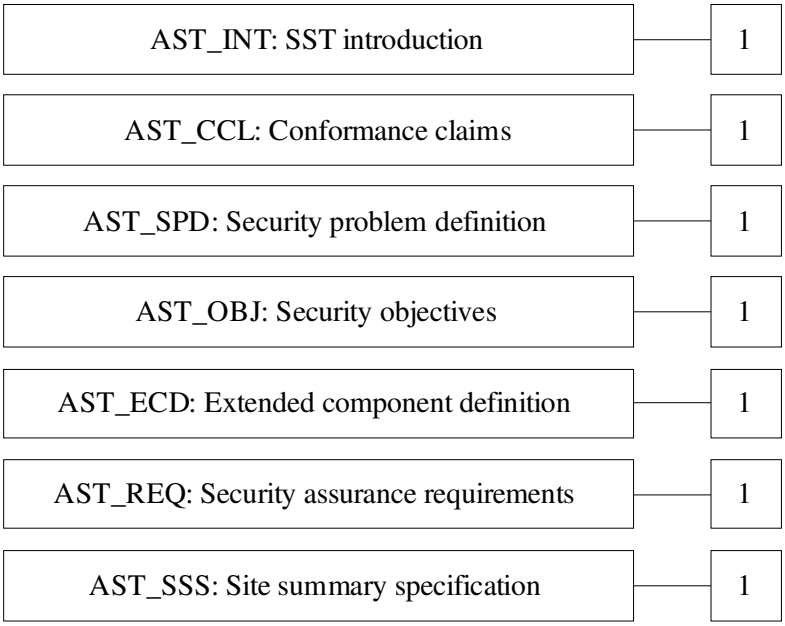


Figure 7 - AST: Site Security Target evaluation class decomposition

Overview

125 Assurance class AST: Site Security Target evaluation defines requirements for the evaluation of an SST, to demonstrate that the SST is sound and internally consistent.

Methodology introduction

126 This chapter describes the evaluation of an SST. The SST evaluation should be started prior to any Site evaluation sub-activities since the SST provides the basis and context to perform these sub-activities. The evaluation methodology in this section is based on the requirements on the SST as specified in CC assurance class AST.

127 This chapter should be used in conjunction with chapter 4 of the process description, as this chapter clarifies the concepts used here and provides many examples.

Methodology objectives

128 The SST describes the security features of a Site. As such it is expected to identify the security requirements that enforce the defined OSPs and counter the defined threats.

129 Evaluating an SST is required to demonstrate that the SST is sound and internally consistent. These properties are necessary for the SST to be suitable for use as the basis for the Site evaluation.

7.1. SST introduction (AST_INT)

Objectives

130 The objective of this family is to describe the Site in a narrative way on two levels of abstraction: Site reference and Site description.

131 Evaluation of the SST introduction is required to demonstrate that the Site is correctly identified, correctly described at two levels of abstraction and that these two descriptions are consistent with each other.

Overview

132 The SST introduction describes the Site in a narrative way on two levels of abstraction.

AST_INT.1 SST introduction

Objectives

133 The objective of this sub-activity is to determine whether the SST and the Site are correctly identified, whether the Site is correctly described in a narrative way at two levels of abstraction (Site reference and Site description), and whether these two descriptions are consistent with each other.

Input

134 The evaluation evidence for this sub-activity is:

a) the SST.

Dependencies: No dependencies.

Developer action elements:

AST_INT.1.1D The developer shall provide an SST introduction.

Content and presentation elements:

AST_INT.1.1C The SST introduction shall contain an SST reference, a Site reference and a Site description.

AST_INT.1.2C The SST reference shall uniquely identify the SST.

AST_INT.1.3C The Site reference shall identify the Site.

AST_INT.1.4C The Site description shall describe the physical scope of the Site.

AST_INT.1.5C The Site description shall describe the logical scope of the Site.

Evaluator action elements:

AST_INT.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_INT.1-1 **AST_INT.1.1C** The evaluator ***shall check*** that the SST introduction contains an SST reference, a Site reference and a Site description.

AST_INT.1-2 **AST_INT.1.2C** The evaluator ***shall examine*** the SST reference to determine that it uniquely identifies the SST.

135 The evaluator determines that the SST reference identifies the SST itself, so that it can be easily distinguished from other SSTs, and that it also uniquely identifies each version of the SST, e.g. by including a version number and/or a date of publication.

AST_INT.1-3 **AST_INT.1.3C** The evaluator ***shall examine*** the Site reference to determine that it identifies the Site.

136 The evaluator determines that the Site reference identifies the:

- the organisation(s) that the Site belongs to;
- the geographical location of the Site.

137 The Site reference should not be misleading: situations if only a part of a geographical location or organisation is evaluated, the Site reference should reflect this.

AST_INT.1-4 **AST_INT.1.4C** The evaluator ***shall examine*** the Site description to determine that it describes the physical scope of the Site.

138 The evaluator determines that the Site description discusses the physical scope of the Site: address and general nature (plant, building, floor, etc.) to a level of detail that is sufficient to give the reader a general understanding.

AST_INT.1-5 **AST_INT.1.5C** The evaluator ***shall examine*** the Site description to determine that it describes the logical scope of the Site.

139 The evaluator determines that the Site description discusses the organisation(s) at the Site.

140 The evaluator determines that the Site description describes the general processes occurring in those organisation(s) Site, and the various items and/or documents processed or produced by the Site at a level of detail that is sufficient to give the reader a general understanding of those organisation(s), processes, items and/or documents .

141 If the Site consists of more than one geographical location, the evaluator determines that the Site description describes how the various organisation(s), processes, items and/or documents are distributed over the various geographical locations.

142 The evaluator also determines that the Site description discusses the relation of the Site with any lifecycle phases of TOEs likely to be designed, developed, produced or otherwise processed at the Site.

AST_INT.1.2E The evaluator ***shall confirm*** that the Site reference and the Site description are consistent with each other.

AST_INT.1-6 The evaluator ***shall examine*** the Site reference and the Site description to determine that they are consistent with each other.

7.2. Conformance claims (AST_CCL)

Objectives

143 The objective of this family is to determine the validity of the conformance claim.

Overview

144 Conformance claims describes how the SST conforms to CC Part 2 and CC Part 3.

AST_CCL.1 Conformance claims

Dependencies:

AST_INT.1 SST introduction
AST_ECD.1 Extended assurance components definition
AST_REQ.1 Derived security assurance requirements

Objectives

145 The objective of this sub-activity is to determine the validity of various conformance claims. These describe how the SST and the Site conform to the CC.

Input

146 The evaluation evidence for this sub-activity is:

a) the SST;

Developer action elements:

AST_CCL.1.1D The developer shall provide a conformance claim.

Content and presentation elements:

AST_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the SST and the Site claim conformance.

AST_CCL.1.2C The CC conformance claim shall describe the conformance of the SST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

AST_CCL.1.3C The CC conformance claim shall be consistent with the extended components definition.

AST_CCL.1.4C The CC conformance claim shall identify the SARs.

Evaluator action elements:

AST_CCL.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_CCL.1-1 **AST_CCL.1.1C** The evaluator ***shall check*** that the conformance claim contains a CC conformance claim that identifies the version of the CC to which the SST and the Site claim conformance.

147 The evaluator determines that the CC conformance claim identifies the version of the CC that was used to develop this SST. This should include the version number of the CC and, unless the International English version of the CC was used, the language of the version of the CC that was used.

AST_CCL.1-2 **AST_CCL.1.2C** The evaluator ***shall check*** that the CC conformance claim states a claim of either CC Part 3 conformant or CC Part 3 extended for the SST.

AST_CCL.1-3 **AST_CCL.1.3C** The evaluator ***shall examine*** the CC conformance claim for CC Part 3 to determine that it is consistent with the extended components definition.

148 If the CC conformance claim contains CC Part 3 conformant, the evaluator determines that the extended components definition does not define assurance components.

149 If the CC conformance claim contains CC Part 3 extended, the evaluator determines that the extended components definition defines at least one extended assurance component.

AST_CCL.1-4 **AST_CCL.1.4C** The evaluator ***shall check*** that the conformance claim identifies the SARs.

150 The evaluator determines that the SARs are identified and that this identification is consistent with the statement of security requirements.

7.3. Security problem definition (AST_SPD)

Objectives

151 This part of the SST defines the security problem to be addressed by the Site.

152 Evaluation of the security problem definition is required to demonstrate that the security problem intended to be addressed by the Site is clearly defined.

Overview

153 The security problem definition defines the problem addressed by the Site.

AST_SPD.1 Security problem definition

Objectives

154 The objective of this sub-activity is to determine that the security problem intended to be addressed by the Site is clearly defined.

Input

155 The evaluation evidence for this sub-activity is:

a) the SST.

Dependencies: No dependencies.

Developer action elements:

AST_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

AST_SPD.1.1C The security problem definition shall describe the threats.

AST_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

AST_SPD.1.3C The security problem definition shall describe the OSPs.

Evaluator action elements:

AST_SPD.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_SPD.1-1 **AST_SPD.1.1C** The evaluator ***shall check*** that the security problem definition describes the threats.

156 If all security objectives are derived from OSPs only, the statement of threats need not be present in the SST. In this case, this work unit is not applicable and therefore considered to be satisfied.

157 The evaluator determines that the security problem definition describes the threats that must be countered by the Site.

AST_SPD.1-2 **AST_SPD.1.2C** The evaluator ***shall examine*** the security problem definition to

determine that all threats are described in terms of a threat agent, an asset, and an adverse action.

158 If all security objectives are derived from OSPs only, the statement of threats need not be present in the SST. In this case, this work unit is not applicable and therefore considered to be satisfied.

159 Threat agents may be further described by aspects such as expertise, resource, opportunity, and motivation.

AST_SPD.1-3 **AST_SPD.1.3C** The evaluator ***shall check*** that the security problem definition describes the OSPs.

160 If all security objectives are derived from threats only, OSPs need not be present in the SST. In this case, this work unit is not applicable and therefore considered to be satisfied.

161 The evaluator determines that OSP statements are made in terms of rules, practises or guidelines that must be followed by the Site.

162 The evaluator determines that each OSP is explained and/or interpreted in sufficient detail to make it clearly understandable; a clear presentation of policy statements is necessary to permit tracing security objectives to them.

7.4. Security objectives (AST_OBJ)

Objectives

163 The security objectives are a concise statement of the intended response to the security problem defined through the Security problem definition (AST_SPD) family.

164 Evaluation of the security objectives is required to demonstrate that the security objectives adequately and completely address the security problem definition.

Overview

165 The security objectives are a concise statement of the intended response to the security problem.

AST_OBJ.1 Security objectives for the development environment

Dependencies: AST_SPD.1 Security problem definition

Objectives

166 The objective of this sub-activity is to determine whether the security objectives adequately and completely address the security problem definition problem.

Input

167 The evaluation evidence for this sub-activity is:

a) the SST.

Developer action elements:

AST_OBJ.1.1D The developer shall provide a statement of security objectives.

AST_OBJ.1.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

AST_OBJ.1.1C The statement of security objectives shall describe the security objectives for the development environment.

AST_OBJ.1.2C The security objectives rationale shall trace each security objective for the development environment back to threats countered by that security objective and OSPs enforced by that security objective.

AST_OBJ.1.3C The security objectives rationale shall demonstrate that the security objectives counter all threats.

AST_OBJ.1.4C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

Evaluator action elements:

AST_OBJ.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_OBJ.1-1 **AST_OBJ.1.1C** The evaluator ***shall check*** that the statement of security objectives defines the security objectives for the development environment.

AST_OBJ.1-2 **AST_OBJ.1.2C** The evaluator ***shall check*** that the security objectives rationale traces the security objectives for the development environment back to threats countered by that security objective and OSPs enforced by that security objective.

168 Each security objective for the development environment may trace back to threats or OSPs, or a combination of threats and OSPs, but it must trace back to at least one threat or OSP.

169 Failure to trace implies that either the security objectives rationale is incomplete, the security problem definition is incomplete, or the security objective for the development environment has no useful purpose.

AST_OBJ.1-3 **AST_OBJ.1.3C** The evaluator ***shall examine*** the security objectives rationale to determine that it justifies for each threat that the security objectives are suitable to counter that threat.

170 If no security objectives trace back to the threat, this work unit fails.

171 The evaluator determines that the justification for a threat shows whether the threat is removed, diminished or mitigated.

172 The evaluator determines that the justification for a threat demonstrates that the security objectives are sufficient: if all security objectives that trace back to the threat are achieved, the threat is removed, sufficiently diminished, or the effects of the threat are sufficiently mitigated.

173 Note that the tracings from security objectives to threats provided in the security objectives rationale may be part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective is merely a statement reflecting the intent to prevent a particular threat from being realised, a justification is required, but this justification could be as minimal as “Security Objective X directly counters Threat Y”.

174 The evaluator also determines that each security objective that traces back to a threat is necessary: when the security objective is achieved it actually contributes to the removal, diminishing or mitigation of that threat.

AST_OBJ.1-4 **AST_OBJ.1.4C** The evaluator ***shall examine*** the security objectives rationale to determine that for each OSP it justifies that the security objectives are suitable to enforce that OSP.

175 If no security objectives trace back to the OSP, this work unit fails.

176 The evaluator determines that the justification for an OSP demonstrates that the security objectives are sufficient: if all security objectives that trace back to that OSP are achieved, the OSP is enforced.

177 The evaluator also determines that each security objective that traces back to an OSP is necessary: when the security objective is achieved it actually contributes to the enforcement of the OSP.

178 Note that the tracings from security objectives to OSPs provided in the security objectives rationale may be part of a justification, but do not constitute a justification by themselves. In the case that a security objective is merely a statement reflecting the intent to enforce a particular OSP, a justification is required, but this justification could be as minimal as "Security Objective X directly enforces OSP Y".

7.5. Extended components definition (AST_ECD)

Objectives

179 Extended assurance requirements are requirements that are not based on components from CC Part 3, but are based on extended components: components defined by the SST author.

180 Evaluation of the definition of extended components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they could not have been clearly expressed using existing CC Part 3 components.

Overview

181 Extended components are defined wherever it is impossible to clearly express assurance requirements using only components from CC Part 3.

AST_ECD.1 Extended assurance components definition

Objectives

182 The objective of this sub-activity is to determine whether extended assurance components have been clearly and unambiguously defined, and whether they are necessary, i.e. they could not have been clearly expressed using existing CC Part 3 components.

Input

183 The evaluation evidence for this sub-activity is:

a) the SST.

Dependencies: No dependencies.

Developer action elements:

AST_ECD.1.1D The developer shall provide a statement of security requirements.

AST_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

AST_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

AST_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

AST_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

AST_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

AST_ECD.1.5C The extended components shall consist of measurable and objective elements such that compliance or noncompliance to these elements can be demonstrated.

Evaluator action elements:

AST_ECD.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_ECD.1-1 **AST_ECD.1.1C** The evaluator ***shall check*** that all security requirements in the statement of security requirements that are not identified as extended requirements are present in CC Part 3.

AST_ECD.1-2 **AST_ECD.1.2C** The evaluator ***shall check*** that the extended components definition defines an extended component for each extended security requirement.

184 If the SST does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

185 A single extended component may be used to define multiple iterations of an extended security requirement, it is not necessary to repeat this definition for each iteration.

AST_ECD.1-3 **AST_ECD.1.3C** The evaluator ***shall examine*** the extended components definition to determine that it describes how each extended component fits into the existing CC components, families, and classes.

186 If the SST does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

187 The evaluator determines that each extended component is either:

a) a member of an existing CC Part 3 family, or

b) a member of a new family defined in the SST.

188 If the extended component is a member of an existing CC Part 3 family, the evaluator determines that the extended components definition adequately describes why the extended component should be a member of that family and how it relates to other components of that family.

189 If the extended component is a member of a new family defined in the SST, the evaluator confirms that the extended component is not appropriate for an existing family.

190 If the SST defines new families, the evaluator determines that each new family is either:

a) a member of an existing CC Part 3 class, or

b) a member of a new class defined in the SST.

191 If the family is a member of an existing CC Part 3 class, the evaluator determines that the extended components definition adequately describes why the family should be a member of that class and how it relates to other families in that class.

192 If the family is a member of a new class defined in the SST, the evaluator confirms that the family is not appropriate for an existing class.

AST_ECD.1-4 **AST_ECD.1.3C** The evaluator ***shall examine*** the extended components definition to determine that each definition of an extended component identifies all applicable dependencies of that component.

193 If the SST does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

194 The evaluator confirms that no applicable dependencies have been overlooked by the SST author.

AST_ECD.1-5 **AST_ECD.1.4C** The evaluator ***shall examine*** the extended components definition to determine that each definition of an extended assurance component uses the existing CC Part 3 components as a model for presentation.

195 If the SST does not contain extended SARs, this work unit is not applicable and therefore considered to be satisfied.

196 The evaluator determines that the extended assurance component definition is consistent with CC Part 3 section 7.1.3.

197 If the extended assurance component uses operations, the evaluator determines that the extended assurance component is consistent with CC Part 1 Annex C.4.

198 If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with CC Part 3 section 7.1.5.

AST_ECD.1-6 **AST_ECD.1.4C** The evaluator ***shall examine*** the extended components definition to determine that, for each defined extended assurance component, applicable methodology has been provided.

199 If the SST does not contain extended SARs, this work unit is not applicable and therefore considered to be satisfied.

200 The evaluator determines that, for each evaluator action element of each extended SAR, one or more work units is provided and that successfully performing all work units for a given evaluator action element will demonstrate that the element has been achieved.

AST_ECD.1-7 **AST_ECD.1.4C** The evaluator ***shall examine*** the extended components definition to determine that each definition of a new assurance family uses the existing CC assurance families as a model for presentation.

201 If the SST does not define new assurance families, this work unit is not applicable and therefore considered to be satisfied.

202 The evaluator determines that all new assurance families are defined consistent with CC Part 3 Section 7.1.2.

AST_ECD.1-8 **AST_ECD.1.4C** The evaluator ***shall examine*** the extended components definition to determine that each definition of a new assurance class uses the existing CC assurance classes as a model for presentation.

203 If the SST does not define new assurance classes, this work unit is not applicable and therefore considered to be satisfied.

204 The evaluator determines that all new assurance classes are defined consistent with CC Part 3 Section 7.1.1.

AST_ECD.1-9 **AST_ECD.1.5C** The evaluator ***shall examine*** the extended components definition to determine that each element in each extended component is measurable and states objective evaluation requirements, such that compliance or noncompliance can be demonstrated.

205 If the SST does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

206 The evaluator determines that elements of extended assurance components avoid the need for subjective evaluator judgement.

207 The evaluator is reminded that whilst being measurable and objective is appropriate for all evaluation criteria, it is acknowledged that no formal method exists to prove such properties. Therefore the existing CC assurance components are to be used as a model for determining what constitutes compliance with this requirement.

AST_ECD.1.2E The evaluator ***shall confirm*** that no extended component can be clearly expressed using existing components.

AST_ECD.1-10 The evaluator ***shall examine*** the extended components definition to determine that each extended component can not be clearly expressed using existing components.

208 If the SST does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

209 The evaluator should take components from CC Part 3, other extended components that have been defined in the SST, combinations of these components, and possible operations on these components into account when making this determination.

210 The evaluator is reminded that the role of this work unit is to preclude unnecessary duplication of components, that is, components that can be clearly expressed by using other components. The evaluator should not undertake an exhaustive search of all possible combinations of components including operations in an attempt to find a way to express the extended component by using existing components.

7.6. Security assurance requirements (AST_REQ)

Objectives

211 The SARs form a clear, unambiguous and canonical description of the expected activities that will be undertaken to gain assurance in the Site.

212 Evaluation of the security requirements is required to ensure that they are clear, unambiguous and well-defined.

Overview

213 The SARs form a clear, unambiguous and well-defined description of the expected activities that will be undertaken to gain assurance in the Site.

AST_REQ.1 Derived security assurance requirements

Dependencies: AST_OBJ.1 Security objectives for the development environment
AST_ECD.1 Extended assurance components definition

Objectives

214 The objective of this sub-activity is to determine whether the SARs are clear, unambiguous and well-defined, whether they are internally consistent, and whether they meet the security objectives for the development environment.

Input

215 The evaluation evidence for this sub-activity is:

a) the SST.

Developer action elements:

AST_REQ.1.1D The developer shall provide a security requirements rationale.

Content and presentation elements:

AST_REQ.1.1C The statement of security requirements shall describe the SARs.

AST_REQ.1.2C The statement of security requirements shall identify all operations on the security requirements.

AST_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

AST_REQ.1.4C All operations shall be performed correctly.

AST_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

AST_REQ.1.6C The statement of security requirements shall contain only SARs drawn from components in the ALC class.

AST_REQ.1.7C The statement of security requirements shall contain ALC_DVS.1, ALC_CMC.3 and ALC_CMS.1 or hierarchically higher SARs.

AST_REQ.1.8C The security requirements rationale shall trace each SAR back to the security objectives for the development environment.

AST_REQ.1.9C The security requirements rationale shall demonstrate that the SARs meet all security objectives for the development environment.

Evaluator action elements:

AST_REQ.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_REQ.1-1 **AST_REQ.1.1C** The evaluator ***shall check*** that the statement of security requirements describes the SARs.

216 The evaluator determines that all SARs are identified by one of the following means:

a) by reference to an individual component in CC Part 3;

b) by reference to an extended component in the extended components definition of the SST;

c) by reproduction in the SST.

217 It is not required to use the same means of identification for all SARs.

AST_REQ.1-2 **AST_REQ.1.2C** The evaluator ***shall examine*** the statement of security requirements to determine that it defines all terms that are used in the requirements that are not defined in the CC.

218 The evaluator determines that the statement of security requirements defines all terms that are introduced in the SARs by completing operations, if these terms are not immediately clear to a wide audience, or are used outside their dictionary definition.

219 The goal of this work unit is to ensure that the SARs are well-defined and that no misunderstanding may occur due to the introduction of vague terms. This work unit should not be taken into extremes, by forcing the SST writer to define every single word. The general audience of a set of security requirements should be assumed to have a reasonable knowledge of IT, security and Common Criteria.

220 All of the above may be presented in groups, classes, roles, types or other groupings or characterisations that allow easy understanding.

221 The evaluator is reminded that these lists and definitions do not have to be part of the statement of security requirements, but may be placed (in part or in whole) in different sections. This may be especially applicable if the same terms are used in the rest of the SST.

AST_REQ.1-3 **AST_REQ.1.3C** The evaluator ***shall check*** that the statement of security requirements identifies all operations on the security requirements.

222 The evaluator determines that all operations are identified in each SAR where such an operation is used. Identification can be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

AST_REQ.1-4 **AST_REQ.1.4C** The evaluator ***shall examine*** the statement of security requirements to determine that all assignment operations are performed correctly.

223 Guidance on the correct performance of operations may be found in CC Part 1 Annex C.4.

AST_REQ.1-5 **AST_REQ.1.4C** The evaluator ***shall examine*** the statement of security requirements to determine that all iteration operations are performed correctly.

224 Guidance on the correct performance of operations may be found in CC Part 1 Annex C.4.

AST_REQ.1-6 **AST_REQ.1.4C** The evaluator ***shall examine*** the statement of security requirements to determine that all selection operations are performed correctly.

225 Guidance on the correct performance of operations may be found in CC Part 1 Annex C.4.

AST_REQ.1-7 **AST_REQ.1.4C** The evaluator ***shall examine*** the statement of security requirements to determine that all refinement operations are performed correctly.

226 Guidance on the correct performance of operations may be found in CC Part 1 Annex C.4.

AST_REQ.1-8 **AST_REQ.1.5C** The evaluator ***shall examine*** the statement of security requirements to determine that each dependency of the security requirements is either satisfied, or that the security requirements rationale justifies the dependency not being satisfied.

227 A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to it) within the statement of security requirements. The component used to satisfy the dependency should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

228 A justification that a dependency is not met should address why the dependency is not necessary or useful, in which case no further information is required; or

AST_REQ.1-9 **AST_REQ.1.6C** The evaluator ***shall check*** that all SARs are based on components from the ALC class.

AST_REQ.1-10 **AST_REQ.1.7C** The evaluator ***shall check*** that the statement of security

requirements contains ALC_DVS.1, ALC_CMC.3 and ALC_CMS.1 (or hierarchically higher SARs).

AST_REQ.1-11 **AST_REQ.1.8C** The evaluator ***shall check*** that the security requirements rationale traces each SAR back to the security objectives for the development environment.

229 The evaluator determines that each SAR is traced back to at least one security objective for the development environment.

230 Failure to trace implies that either the security requirements rationale is incomplete, the security objectives for the development environment are incomplete, or the SAR has no useful purpose.

AST_REQ.1-12 **AST_REQ.1.9C** The evaluator ***shall examine*** the security requirements rationale to determine that for each security objective for the development environment it justifies that the SARs are suitable to meet that security objective for the development environment.

231 If no SARs trace back to the security objective for the development environment, this work unit fails.

232 The evaluator determines that the justification for a security objective for the development environment demonstrates that the SARs are sufficient: if all SARs that trace back to the objective are satisfied, the security objective for the development environment is achieved.

233 The evaluator also determines that each SAR that traces back to a security objective for the development environment is necessary, when the SAR is satisfied, it actually contributes to achieving the security objective.

234 Note that the tracings from SARs to security objectives for the development environment provided in the security requirements rationale may be a part of the justification, but do not constitute a justification by themselves.

AST_REQ.1.2E The evaluator ***shall confirm*** that the statement of security requirements is internally consistent.

AST_REQ.1-13 The evaluator ***shall examine*** the statement of security requirements to determine that it is internally consistent.

235 The evaluator determines that the combined set of all SARs is internally consistent.

236 The evaluator determines that on all occasions where different security requirements apply to the same types of developer evidence, tests to be performed etc. that these requirements do not conflict.

7.7. Site summary specification (AST_SSS)

Objectives

237 The Site summary specification describes aspects of how the Site meets the SARs, in particular aspects that are of interest when re-using the Site.

238 Evaluation of the Site summary specification is required to demonstrate that it is consistent with the other narrative descriptions of the Site.

Overview

239 The Site summary specification describes how the Site meets the SARs, in particular aspects that are of interest when re-using the Site.

AST_SSS.1 Site Summary Specification

Dependencies: AST_INT.1 SST introduction
AST_REQ.1 Derived security assurance requirements

Objectives

240 The objective of this sub-activity is to determine whether the Site summary specification is consistent with other narrative descriptions of the Site.

Input

241 The evaluation evidence for this sub-activity is:

a) the SST.

Developer action elements:

AST_SSS.1.1D The developer shall provide a Site summary specification.

Content and presentation elements:

AST_SSS.1.1C The Site summary specification shall identify all evidence for the SARs.

AST_SSS.1.2C The Site summary specification shall describe aspects of how the Site meets the SARs.

AST_SSS.1.3C The Site summary specification shall trace the aspects to the evidence.

Evaluator action elements:

AST_SSS.1.1E The evaluator ***shall confirm*** that the information provided meets all requirements for content and presentation of evidence.

AST_SSS.1-1 **AST_SSS.1.1C** The evaluator ***shall check*** that the Site summary specification identifies all evidence for the SARs

242 The evaluator determines that all evidence that has been used for evaluating the SARs is identified, with name and version number (if applicable).

243 The evaluator is reminded that this work unit can normally only be completed at the end of the Site evaluation, as the final versions of the evidence are not determined before that.

AST_SSS.1-2 **AST_SSS.1.2C** The evaluator ***shall examine*** the Site summary specification to determine that it describes aspects of how the Site meets each SAR.

244 The evaluator determines that the Site summary specification describes aspects of how the Site meets the SARs.

245 The evaluator is reminded that the objective of each description is to allow re-use of the Site evaluation in TOE evaluations. It is therefore up to the SST author to determine which aspects are described, and in which amount of detail. It is therefore also allowed to provide no aspects of a given SAR if the SST author so chooses.

AST_SSS.1-3 **AST_SSS.1.3C** The evaluator ***shall check*** the Site summary specification to determine that it traces the aspects to the evidence.

246 The evaluator determines that all aspects in the Site summary specification can be traced back to the evidence.

247 The evaluator is reminded that the objective of this tracing is to allow the evaluator in the TOE evaluation to examine the underlying evidence if the aspects are insufficient. It is therefore up to the SST author to determine the granularity of the tracing. This could range from "See the QA manual v1.2" to "See section 2.6.4 2nd paragraph of the CM Manual v2.3 and Chapters 4, 5 and Annex A of the "Mega-CM Programmer's Guide".

248 The evaluator is also reminded that in this work unit only the existence of the tracing (and not the correctness) is determined.

AST_SSS.1.2E The evaluator ***shall confirm*** that the Site summary specification is consistent with the Site description.

AST_SSS.1-4 The evaluator ***shall examine*** the Site summary specification to determine that it is consistent with the Site description.

AST_SSS.1.3E The evaluator ***shall confirm*** that the aspects and the tracing of the aspects is consistent with the evidence for the SARs.

AST_SSS.1-5 The evaluator ***shall examine*** the aspects and the tracing of the aspects to determine that they are consistent with the evidence for the SARs.

249 The evaluator determines that the aspects are consistent with the evidence: no aspects are provided that do not also appear in the evidence. The evaluator also determines that the aspects are correctly traced to the evidence.

250 The evaluator is reminded that this work unit can normally only be completed at the end of the Site evaluation, as the final versions of the evidence are not determined before that.

8. Terminology

251 All terms used in this document are taken from the CC, version 3.1. Additional terms which have been used in this document are listed and defined in the following:

Complete Life-Cycle A life-cycle is said to be complete if all ALC requirements (EAL3 and higher) are covered by a site.

Composed Site Result of the Splicing procedure. Combination of at least one certified sites with additional certified sites or non-certified ALC portions.

Logical Site Scope Purpose (functionality) of the site with respect to the product life cycle.

Minimum SAR(s) An Minimum SAR (Minimum Site Requirement) is an ALC requirement that every site has to fulfil (ALC_DVS.1, ALC_CMC.3).

Mutually supportive This term describes a relationship between a group of entities, indicating that the entities possess properties which do not conflict with, and may assist the other entities in performing their tasks. It is not necessary to determine that every individual entity in question directly supports other entities in that grouping; rather, it is a more general determination that is made.

Non-certified ALC portions ALC aspects which are not covered by a Site Certificate but are needed for a TOE development environment. They are introduced in the Splicing Procedure.

Optional SAR(s) An Optional SAR (Optional Site Requirement) is an ALC requirement that defines the objectives/purpose of a Site. This has to be seen in contrast to the Minimum SARs which every site has to fulfil.

Physical Site Scope One or more physical location(s) of a site.

Site A part or the whole of an existing or anticipated TOE development environment. A site may consist of one geographical location, be a part of one locations, or may span (parts of) multiple locations. A site may consist of one organisational unit, be part of an organisational unit, or may span (parts of) multiple organisational units.

Site Certificate CC certificate awarded to a site which fulfils certain CC (Minimum and claimed Optional SARs) ALC requirements.

Site-Certification-Maintenance Maintenance of ALC measures in the development environment. As the typical life-cycle of a development environment shows, continuous monitoring and review activities are essential. This fact suggests that a continuos maintenance might improve the assurance in the ability

	of a product developers Site to keep its security level over time. It includes the definition of second level procedures, with which he audits his security measures and adapts them to new circumstances, if necessary.
Splicing	The process of combining at least one certified site with additional certified sites or non-certified ALC portions. The result is a composed site which can either be certified or can be used (with uncertified portions) as TOE development environment in a TOE evaluation.

9. Abbreviations

252 Please not that all abbreviations used in this document are taken from the CC, version 3.0.

AC	Assurance Continuity
ALC	CC Assurance Class for Life Cycle Support
AST	CC Assurance Class for Site Security Target Evaluation
CC	Common Criteria
CCDB	Common Criteria Development Board
CM	Configuration Management
CMC	CC Assurance Family ALC_CMC for CM Capabilities
CMS	CC Assurance Family ALC_CMS for CM Scope
DEL	CC Assurance Family ALC_DEL for Delivery Procedures
DVS	CC Assurance Family ALC_DVS for Development Security
EAL	Evaluation Assurance Level
FLR	CC Assurance Family ALC_FLR for Flaw Remediation
LCD	CC Assurance Family ALC_LCD for Life Cycle Definition
SAR	Security Assurance Requirement
SSS	Site Summary Specification (Section of the SST)
SST	Site Security Target
ST	Security Target
TAT	CC Assurance Family ALC_TAT for Tools and Techniques
TOE	Target of Evaluation

10. References

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, September 2006, Version 3.1, Revision 1

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, September 2007, Version 3.1, Revision 2

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, September 2007, Version 3.1, Revision 2

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1, Revision 2