Common Criteria for Information Technology Security Evaluation

Part 1: Introduction and general model

March 2004

Version 2.4
Revision 256

ASE/APE Trial Use version

CCIMB-2004-03-001

Foreword

This version of the Common Criteria for Information Technology Security Evaluation (CC 2.4) is based on CC v2.2, and includes an updated version of the Protection Profile and Security Target criteria (APE and ASE), together with significant changes in the rest of the CC that were necessary to accommodate these new criteria.

CC version 2.4 consists of the following parts:

- Part 1: Introduction and general model
- Part 2: Security functional requirements
- Part 3: Security assurance requirements

This Legal NOTICE has been placed in all Parts of the CC by request:

> *The seven governmental organisations (collectively called the "Common Criteria Project Sponsoring Organisations") listed just below, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.4 Parts 1 through 3 (called "CC 2.4"), hereby grant non-exclusive license to ISO/IEC to use CC 2.4 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, translate or modify CC 2.4 as they see fit.*
>
> *Canada: Communications Security Establishment*
> *France: Service Central de la Sécurité des Systèmes d'Information*
> *Germany: Bundesamt für Sicherheit in der Informationstechnik*
> *Netherlands: Netherlands National Communications Security Agency*
> *United Kingdom: Communications-Electronics Security Group*
> *United States: National Institute of Standards and Technology*
> *United States: National Security Agency*

Table of Contents

Table of contents

List of figures

List of tables

1 Scope

1 This multipart standard, the Common Criteria (CC), is meant to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience.

2 The CC will permit comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help consumers to determine whether the IT product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.

3 The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

4 The CC addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

5 The CC is applicable to IT security measures implemented in hardware, firmware or software. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this will be indicated within the relevant criteria statements.

6 Certain topics, because they involve specialised techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the CC. Some of these are identified below.

a) The CC does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security measures. However, it is recognised that a significant part of the security of a TOE can often be achieved through administrative measures such as organisational, personnel, physical, and procedural controls. Administrative security measures in the operating environment of the TOE are treated as secure usage assumptions where these have an impact on the ability of the IT security measures to counter the identified threats.

b) The evaluation of technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area. In particular, the CC addresses some aspects of physical protection of the TOE.

c) The CC addresses neither the evaluation methodology nor the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the CC will be used for evaluation purposes in the context of such a framework and such a methodology.

d) The procedures for use of evaluation results in product or system accreditation are outside the scope of the CC. Product or system accreditation is the administrative process whereby authority is granted for the operation of an IT product or system in its full operational environment. Evaluation focuses on the IT security parts of the product or system and those parts of the operational environment that may directly affect the secure use of IT elements. The results of the evaluation process are consequently a valuable input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related product or system security properties and their relationship to the IT security parts, accreditors should make separate provision for those aspects.

e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the CC. Should independent assessment of mathematical properties of cryptography embedded in a TOE be required, the evaluation scheme under which the CC is applied must make provision for such assessments.

2 Definitions

2.1 Common abbreviations

7 The following abbreviations are common to more than one part of the CC:

8	CC	Common Criteria
9	EAL	Evaluation Assurance Level
10	IT	Information Technology
11	OSP	Organizational Security Policy
12	PP	Protection Profile
13	SAR	Security Assurance Requirement
14	SFR	Security Functional Requirement
15	SFP	Security Function Policy
16	ST	Security Target
17	TOE	Target of Evaluation
18	TSC	TSF Scope of Control
19	TSF	TOE Security Functions
20	TSFI	TSF Interface
21	TSP	TOE Security Policy

2.2 Scope of glossary

22 This subclause 2.2 contains only those terms which are used in a specialised way throughout the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms. Some combinations of common terms used in the CC, while not meriting glossary definition, are explained for clarity in the context where they are used. Explanations of the use of terms and concepts used in a specialised way in CC Part 2 and CC Part 3 can be found in their respective “paradigm” subclauses.

2.3 Glossary

23 Assets (in the development environment):

entities that the developer of the TOE places value upon

24 Assets (in the operational environment):

entities that the owner of the TOE places value upon

25 Assignment:

The specification of an identified parameter in a component.

26 Assurance:

Grounds for confidence that an entity meets its security objectives.

27 Attack potential:

The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

28 Augmentation:

The addition of one or more assurance component(s) from Part 3 to an EAL or assurance package.

29 Authentication data:

Information used to verify the claimed identity of a user.

30 Authorised user:

A user who may, in accordance with the TSP, perform an operation.

31 Class:

A grouping of families that share a common focus.

32 Component:

The smallest selectable set of elements that may be included in a PP, an ST, or a package.

33 Connectivity:

The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

34 Dependency:

A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

35 Element:

An indivisible security requirement.

36 Evaluation:

Assessment of a PP, an ST or a TOE, against defined criteria.

37 Evaluation Assurance Level (EAL):

A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

38 Evaluation authority:

A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

39 Evaluation scheme:

The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

40 Extension:

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

41 External IT entity:

Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

42 Family:

A grouping of components that share security objectives but may differ in emphasis or rigour.

43 Formal:

Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

44 Guidance Documentation:

Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.

45 Human user:

Any person who interacts with the TOE.

46 Identity:

A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

47 Informal:

Expressed in natural language.

48 Internal communication channel:

A communication channel between separated parts of TOE.

49 Internal TOE transfer:

Communicating data between separated parts of the TOE.

50 Inter-TSF transfers:

Communicating data between the TOE and the security functions of other trusted IT products.

51 Iteration:

The use of a component more than once with varying operations.

52 Object:

An entity within the TSC that contains or receives information and upon which subjects perform operations.

53 Organisational security policies:

One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

54 Package:

A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

55 Product:

A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

56 Protection Profile (PP):

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

57 Reference monitor:

The concept of an abstract machine that enforces TOE access control policies.

58 Reference validation mechanism:

An implementation of the reference monitor concept that possesses the following properties: it is tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing.

59 Refinement:

The addition of details to a component.

60 Role:

A predefined set of rules establishing the allowed interactions between a user and the TOE.

61 Secret:

Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

62 Security attribute:

Characteristics of subjects, users, objects, information, and/or resources that are used for the enforcement of the TSP.

63 Security Function (SF):

A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

64 Security Function Policy (SFP):

The security policy enforced by an SF.

65 Security objective:

A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

66 Security Target (ST):

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

67 Selection:

The specification of one or more items from a list in a component.

68 Semiformal:

Expressed in a restricted syntax language with defined semantics.

69 Subject:

An entity within the TSC that causes operations to be performed.

70 System:

A specific IT installation, with a particular purpose and operational environment.

71 Target of Evaluation (TOE):

An IT product or system and its associated guidance documentation that is the subject of an evaluation.

72 TOE resource:

Anything useable or consumable in the TOE.

73 TOE Security Functions (TSF):

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

74 TOE Security Functions Interface (TSFI):

A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

75 TOE Security Policy (TSP):

A set of rules that regulate how assets are managed, protected and distributed within a TOE.

76 TOE security policy mode:

A structured representation of the security policy to be enforced by the TOE.

77 Transfers outside TSF control:

Communicating data to entities not under control of the TSF.

78 Trusted channel:

A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

79 Trusted path:

A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

80 TSF data:

Data created by and for the TOE, that might affect the operation of the TOE.

81 TSF Scope of Control (TSC):

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

82 User:

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

83 User data:

Data created by and for the user, that does not affect the operation of the TSF.

2.4 Reserved Terms

84 The following terms are used in accordance with the ISO definitions contained in ISO/IEC Directives Part 2, *Rules for the structure and drafting of International Standards*: All text should be considered “Normative” unless specifically denoted as “Informative”.

85 Normative:

Normative text is that which “describes the scope of the document, and which set out provisions.” (ISO/IEC Directives, Part 2) Within normative text, the verbs “shall”, “should”, “may”, and “can” have the ISO standard meanings described in this glossary and the verb “must” is not used. Unless explicitly labeled “informative”, all CC text is normative. Any text related to meeting requirements is considered normative.

86 Informative:

Informative text is that which “provides additional information intended to assist the understanding or use of the document.”(ISO/IEC Directives, Part 2). Informative text is not related to meeting requirements.

87 Shall:

Within normative text, “shall” indicates “requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.” (ISO/IEC Directives, Part 2)

88 Should:

Within normative text, should indicates “that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.”(ISO/IEC Directives, Part 2) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

89 May:

Within normative text, may indicates “a course of action permissible within the limits of the document”(ISO/IEC Directives, Part 2)

90 Can:

Within normative text, can indicates “statements of possibility and capability, whether material, physical or causal”(ISO/IEC Directives, Part 2)

3 Overview

91 This clause introduces the main concepts of the CC. It identifies the target audience, evaluation context, and the approach taken to present the material.

3.1 Introduction

92 Information held by IT products or systems is a critical resource that enables organisations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in IT products or systems remain private, be available to them as needed, and not be subject to unauthorised modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. The term IT security is used to cover prevention and mitigation of these and similar hazards.

93 Many consumers of IT lack the knowledge, expertise or resources necessary to judge whether their confidence in the security of their IT products or systems is appropriate, and they may not wish to rely solely on the assertions of the developers. Consumers may therefore choose to increase their confidence in the security measures of an IT product or system by ordering an analysis of its security (i.e. a security evaluation).

94 The CC can be used to select the appropriate IT security measures and it contains criteria for evaluation of security requirements.

3.1.1 Target audience of the CC

95 There are three groups with a general interest in evaluation of the security properties of IT products and systems: TOE consumers, TOE developers, and TOE evaluators. The criteria presented in this document have been structured to support the needs of all three groups. They are all considered to be the principal users of this CC. The three groups can benefit from the criteria as explained in the following paragraphs.

3.1.1.1 Consumers

96 The CC plays an important role in supporting techniques for consumer selection of IT security requirements to express their organisational needs. The CC is written to ensure that evaluation fulfils the needs of the consumers as this is the fundamental purpose and justification for the evaluation process.

97 Consumers can use the results of evaluations to help decide whether an evaluated product or system fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Consumers can also use the evaluation results to compare different products or systems. Presentation of the assurance requirements within a hierarchy supports this need.

98 The CC gives consumers -- especially in consumer groups and communities of interest -- an implementation-independent structure termed the Protection Profile (PP) in which to express their special requirements for IT security measures in a TOE.

3.1.1.2 Developers

99 The CC is intended to support developers in preparing for and assisting in the evaluation of their products or systems and in identifying security requirements to be satisfied by each of their products or systems. It is also quite possible that an associated evaluation methodology, potentially accompanied by a mutual recognition agreement for evaluation results, would further permit the CC to support someone, other than the TOE developer, in preparing for and assisting in the evaluation of a developer s TOE.

100 The CC constructs can be used to specify requirements for the TOE to conform to. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). One or more PPs may provide the requirements of a broad consumer base.

101 The CC can then be used to determine the responsibilities and actions to support evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

3.1.1.3 Evaluators

102 The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out and the SFRs on which to perform these actions. Note that the CC does not specify procedures to be followed in carrying out those actions

3.1.1.4 Others

103 While the CC is oriented towards specification and evaluation of the IT security properties of TOEs, it may also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that can benefit from information contained in the CC are:

a) system custodians and system security officers responsible for determining and meeting organisational IT security policies and requirements;

b) auditors, both internal and external, responsible for assessing the adequacy of the security of a system;

c) security architects and designers responsible for the specification of the security content of IT systems and products;

d) accreditors responsible for accepting an IT system for use within a particular environment;

e) sponsors of evaluation responsible for requesting and supporting an evaluation; and

f) evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

3.2 Evaluation context

104 In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform.

105 The CC does not state requirements for the regulatory framework. However, consistency between the regulatory frameworks of different evaluation authorities will be necessary to achieve the goal of mutual recognition of the results of such evaluations. Figure **1** depicts the major elements that form the context for evaluations.

106 Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results could be submitted to a certification process. The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval. The certificate is normally publicly available. It is noted that the certification process is a means of gaining greater consistency in the application of IT security criteria.

107 The evaluation scheme, methodology, and certification processes are the responsibility of the evaluation authorities that run evaluation schemes and are outside the scope of the CC.

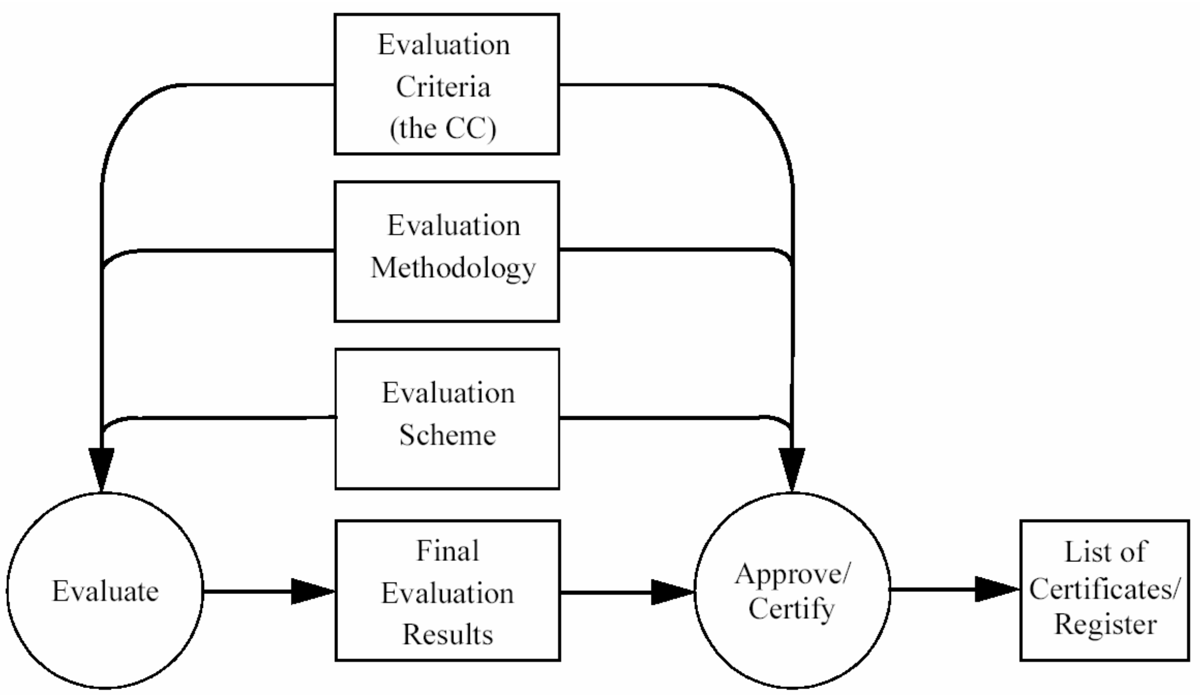

Figure 1 - Evaluation Context

3.3 Organisation of the Common Criteria

108 The CC is presented as a set of distinct but related parts as identified below. Terms used in the description of the parts are explained in clause 4.

a) **Part 1, Introduction and general model**, is the introduction to the CC. It defines general concepts and principles of IT security evaluation and presents a general model of evaluation. Part 1 also presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. In addition, the usefulness of each part of the CC is described in terms of each of the target audiences.

b) **Part 2, Security functional requirements**, establishes a set of functional components as a standard way of expressing the functional requirements for TOEs. Part 2 catalogues the set of functional components, families, and classes.

c) **Part 3, Security assurance requirements**, establishes a set of assurance components as a standard way of expressing the assurance requirements for TOEs. Part 3 catalogues the set of assurance components, families and classes. Part 3 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined CC scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

109 In support of the three parts of the CC listed above, it is anticipated that other types of documents will be published, including technical rationale material and guidance documents.

110 The following table presents, for the three key target audience groupings, how the parts of the CC will be of interest.

	Consumers	Developers	Evaluators
Part 1	Use for background information and reference purposes. Guidance structure for PPs.	Use for background information and reference for the development of requirements and formulating security specifications for TOEs.	Use for background information and reference purposes. Guidance structure for PPs and STs.
Part 2	Use for guidance and reference when formulating statements of requirements for a TOE.	Use for reference when interpreting statements of functional requirements and formulating functional specifications for TOEs.	Use as mandatory statement of evaluation criteria when determining whether a TOE effectively meets claimed security functions.
Part 3	Use for guidance when determining required levels of assurance.	Use for reference when interpreting statements of assurance requirements and determining assurance approaches of TOEs.	Use as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

Table 1 Roadmap to the Common Criteria

4 General model

111 This clause presents the general concepts used throughout the CC, including the context in which the concepts are to be used and the CC approach for applying the concepts. Part 2 and Part 3 expand on the use of these concepts and assume that the approach described is used. This clause assumes some knowledge of IT security and does not propose to act as a tutorial in this area.

112 The CC discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of the CC. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which the CC is applicable.

4.1 Security context

4.1.1 Security in the operational environment

113 Security is concerned with the protection of assets. Examples of assets include:

- contents of a file or a server
- number of votes cast (in an election)
- an electronic commerce process

114 The environment(s) in which these assets are located is called the operational environment. Examples of operational environments are:

- the computer room of a bank;
- the Internet;
- the connection of a LAN to the WAN;
- a general office environment.

115 Assets in the operational environment need to be protected from threats, where threats are categorised as the potential for abuse of protected assets. All categories of threats should be considered, but in the domain of security greater attention is given to those threats that are related to malicious or other human activities. Figure **2** illustrates high level concepts and relationships.

General model

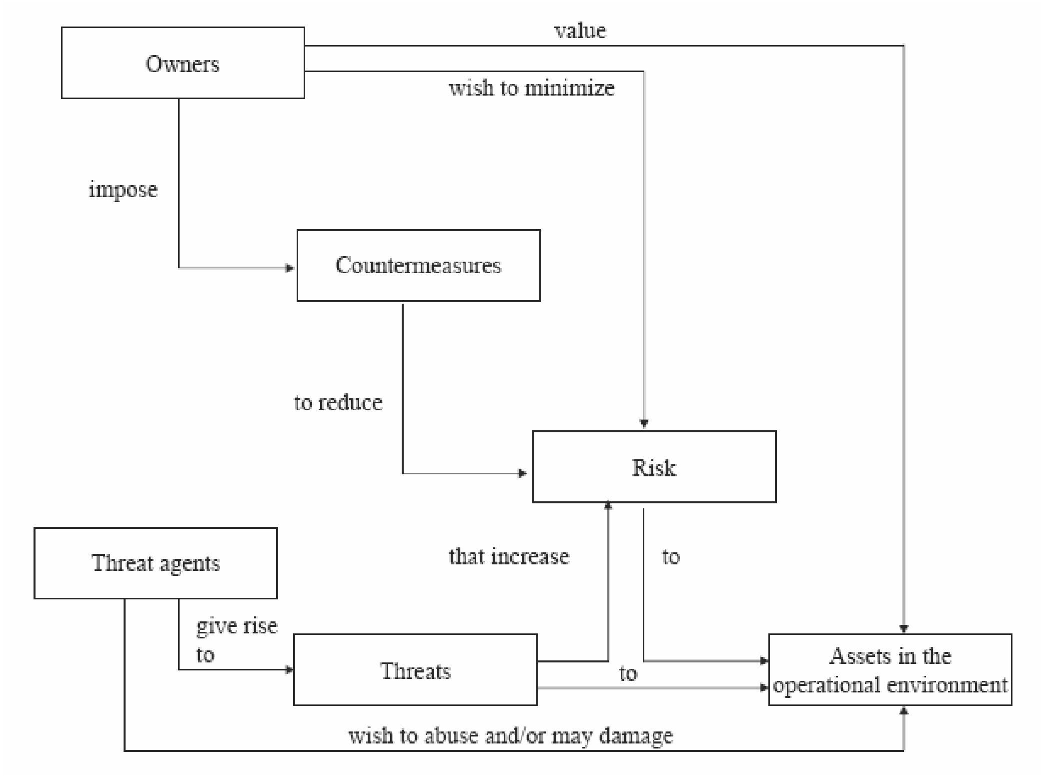

Figure 2 - Security concepts and relationships

116 Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner. Examples of threat agents include hackers, users, computer processes, viruses and acts of God.

117 Owners will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security specific impairment commonly includes, but is not limited to, damaging disclosure of the asset to unauthorised recipients (loss of confidentiality), damage to the asset through unauthorised modification (loss of integrity), or unauthorised deprivation of access to the asset (loss of availability).

118 The owners of the assets will analyse the possible threats to determine which ones apply to their operational environment. The results are known as risks. This analysis can aid in the selection of countermeasures to counter the risks and reduce it to an acceptable level.

119 Countermeasures are imposed to reduce risks to assets and to meet security policies of the owners of the assets in the operational environment (either directly or indirectly by providing direction to other parties).

4.1.2 Security in the development environment

120 However, these countermeasures may possess vulnerabilities. Such vulnerabilities may be exploited and thereby lead to damage and/or abuse of the assets in spite of the countermeasures being employed.

121 These vulnerabilities arise from the development environment: the environment or environments in which the countermeasures are designed, developed, produced, and delivered. Problems in the development environment, such as accidental errors made during development, or the intentional addition of malicious code, may lead to countermeasures with vulnerabilities.

122 The development environment therefore also has assets, such as design documents and source code. Similarly, the development environment has threat agents, such as cleaners, viruses, development staff and acts of God.

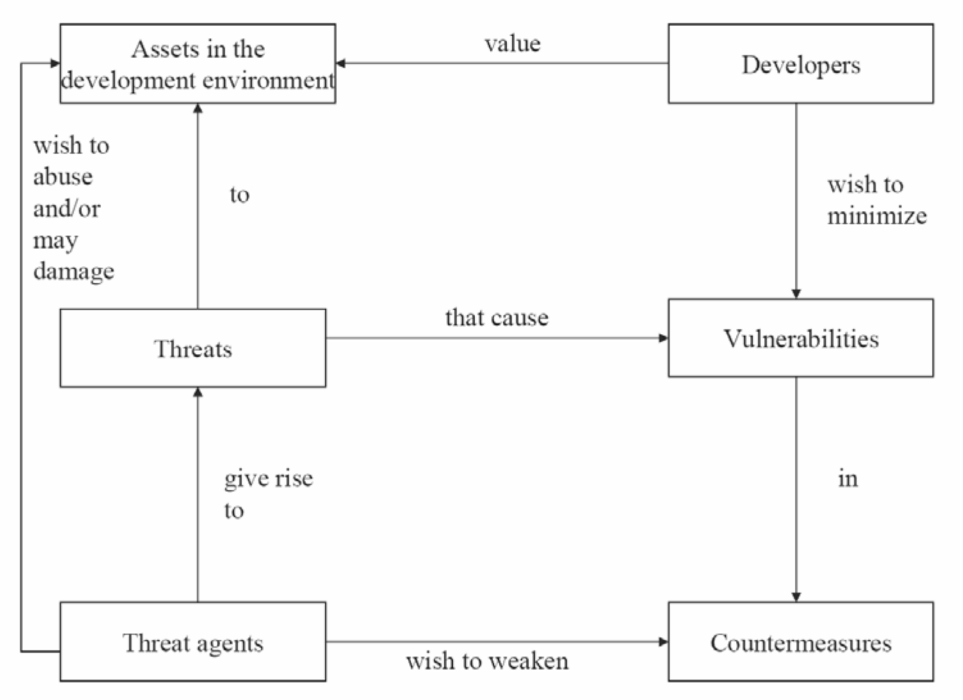

Figure 3 - Developer concepts and relationships

4.1.3 Evaluation concepts

123 Owners of assets in the operational environment will need to be confident that the countermeasures are:

a) sufficient: they counter the threats to assets in the operational environment;

b) correct: they contain no exploitable vulnerabilities

before they will allow exposure of their assets to the specified threats. Owners may not themselves possess the capability to judge all aspects of the countermeasures, and may therefore seek evaluation of the countermeasures.

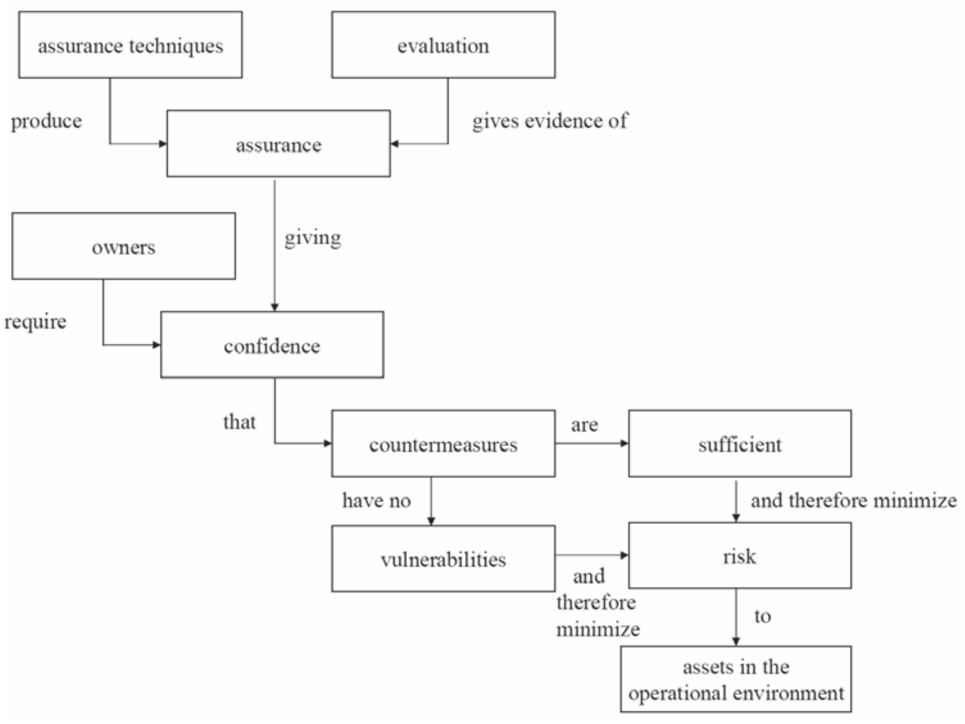

Figure 4 - Evaluation concepts and relationships

124 The outcome of evaluation is a statement about the extent to which assurance is gained that the countermeasures can be trusted to reduce the risks to the protected assets. The statement assigns an assurance rating of the countermeasures, assurance being that property of the countermeasures that gives grounds for confidence in their proper operation. This statement can be used by the owner of the assets in deciding whether to accept the risk of exposing the assets to the threats. Figure **4** illustrates these relationships.

125 Owners of assets will normally be held responsible for those assets and should be able to defend the decision to accept the risks of exposing the assets to the threats. This requires that the statements resulting from evaluation are defensible. Thus, evaluation should lead to objective and repeatable results that can be cited as evidence.

4.1.4 Information technology security context

126 Many assets in the operational environment are in the form of information that is stored, processed and transmitted by IT products or systems to meet requirements laid down by owners of the information. Information owners may require that dissemination and modification of any such information representations (data) be strictly controlled. They may demand that the IT product or system implement IT specific security controls as part of the overall set of security countermeasures put in place to counteract the threats to the data.

127 IT systems are procured and constructed to meet specific requirements and may, for economic reasons, make maximum use of existing commodity IT products such as operating systems, general purpose application components,

and hardware platforms. IT security countermeasures implemented by a system may use functions of the underlying IT products and depend upon the correct operation of IT product security functions. The IT products may, therefore, be subject to evaluation as part of the IT system security evaluation.

128 Where an IT product is incorporated or being considered for incorporation in multiple IT systems, there are cost advantages in evaluating the security aspects of such a product independently and building a catalogue of evaluated products. The results of such an evaluation should be expressed in a manner that supports incorporation of the product in multiple IT systems without unnecessary repetition of work required to examine the product's security.

129 An IT system accreditor has the authority of the owner of the information to determine whether the combination of IT and non-IT security countermeasures furnishes adequate protection for the data, and thus to decide whether to permit the operation of the system. The accreditor may call for evaluation of the IT countermeasures in order to determine whether the IT countermeasures provide adequate protection and whether the specified countermeasures are properly implemented by the IT system. This evaluation may take various forms and degrees of rigour, depending upon the rules imposed upon, or by, the accreditor.

4.2 Common Criteria approach

130 Confidence in IT security can be gained through actions that may be taken during the processes of development, evaluation, and operation.

4.2.1 Development

131 The CC does not mandate any specific development methodology or life cycle model. Figure 5 depicts the relationship between the security requirements and the TOE. The figure is used to provide a context for discussion and should not be construed as advocating a preference for one methodology (e.g. waterfall) over another (e.g. prototyping).

132 It is essential that the security requirements imposed on the development environment be effective in the reducing of risks to assets. Unless suitable requirements are established at the start of the development process, the resulting end product, however well engineered, may not meet the objectives of its anticipated consumers.

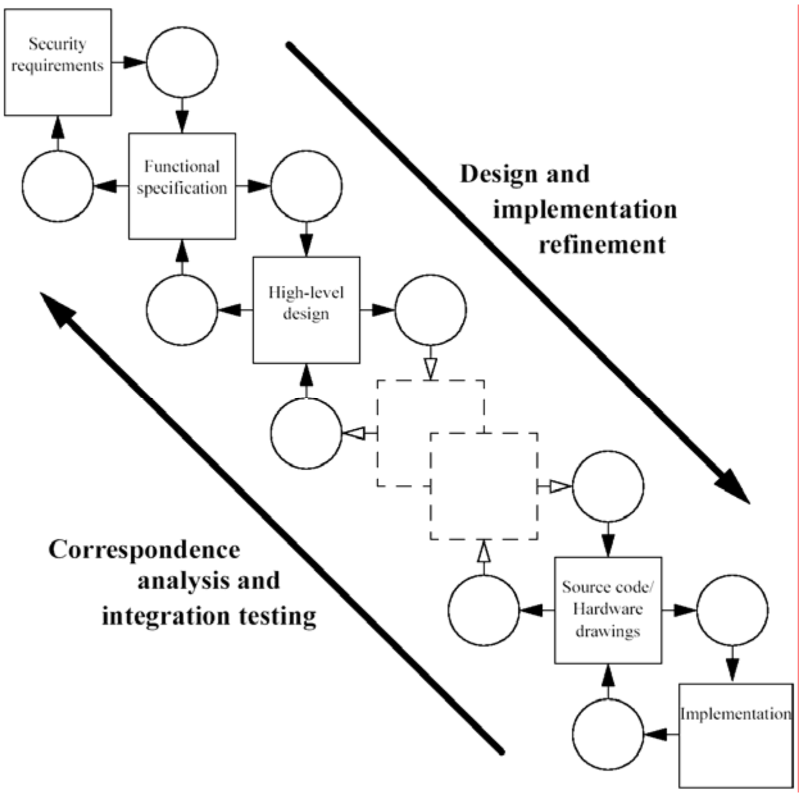
Security requirements
Functional specification
High-level design
Source code/ Hardware drawings
Implementation
Design and implementation refinement
Correspondence analysis and integration testing

Figure 5 - TOE development model

133 The process is based on the refinement of the security requirements expressed in the security target. Each lower level of refinement represents a design decomposition with additional design detail. The least abstract representation is the TOE implementation itself.

134 The CC does not mandate a specific set of design representations. The CC requirement is that there should be sufficient design representations presented at a sufficient level of granularity to demonstrate where required:

a) that each refinement level is a complete instantiation of the higher levels (i.e. all security functionality, properties, and behaviour defined at the higher level of abstraction must be demonstrably present in the lower level);

b) that each refinement level is an accurate instantiation of the higher levels (i.e. there should be no security functionality, properties, and behaviour defined at the lower level of abstraction that are not required by the higher level).

135 The CC assurance criteria identify the design abstraction levels of functional specification, high-level design, low-level design, and implementation. Depending upon the assurance level specified, developers may be required to show how the development methodology meets the CC assurance requirements.

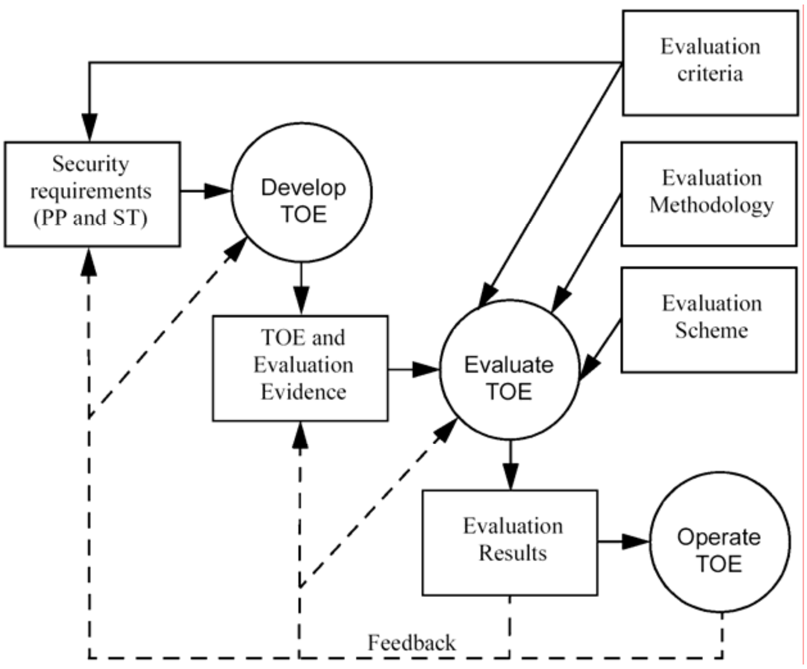

Figure 6 - TOE evaluation process

4.2.2 TOE evaluation

136 The TOE evaluation process as described in Figure **6** may be carried out in parallel with development, or it may follow. The principal inputs to TOE evaluation are:

a) the set of TOE evidence, which includes an ST as the basis for TOE evaluation;

b) the TOE for which the evaluation is required;

c) the evaluation criteria, methodology and scheme.

137 In addition, informative material (such as application notes of the CC) and the IT security expertise of the evaluator and the evaluation community are likely to be used as inputs to the evaluation.

138 The expected result of the evaluation process is a confirmation that the TOE satisfies its security requirements as stated in the ST with one or more reports documenting the evaluator findings about the TOE as determined by the evaluation criteria. These reports will be useful to actual and potential consumers of the product or system represented by the TOE as well as to the developer.

139 The degree of confidence gained through an evaluation depends on the assurance requirements (e.g. Evaluation Assurance Level) met.

140 Evaluation can lead to better IT security products in two ways. Evaluation is intended to identify errors or vulnerabilities in the TOE that the developer may correct, thereby reducing the probability of security failures in future

operation. Also in preparing for the rigours of evaluation, the developer may take more care in TOE design and development. Therefore, the evaluation process can exert a strong, though indirect, positive effect on the initial requirements, the development process, the end product, and the operational environment.

4.2.3 Operation

141 Consumers may elect to use evaluated TOEs in their environments. Once a TOE is in operation, it is possible that previously unknown errors or vulnerabilities may surface or environmental assumptions may need to be revised. As a result of operation, feedback could be given that would require the developer to correct the TOE or redefine its security requirements or security objectives for the operational environment. Such changes may require the TOE to be re-evaluated or the security of its operational environment to be strengthened. In some instances this may only require that the needed updates are evaluated in order to regain confidence in the TOE. Procedures for re-evaluation, including reuse of evaluation results, are outside the scope of the CC.

4.3 CC descriptive material

142 The CC presents the framework in which an evaluation can take place. By presenting the requirements for evidence and analysis, a more objective, and hence useful evaluation result can be achieved. The CC incorporates a common set of constructs and a language in which to express and communicate the relevant aspects of IT security, and permits those responsible for IT security to benefit from the prior experience and expertise of others.

4.3.1 Expression of security requirements

143 The CC defines a set of constructs that combine into meaningful assemblies of security requirements of known validity, which can be used in establishing security requirements for prospective products and systems. The relationships among the various constructs for requirements expression are described below and illustrated in Figure **7**

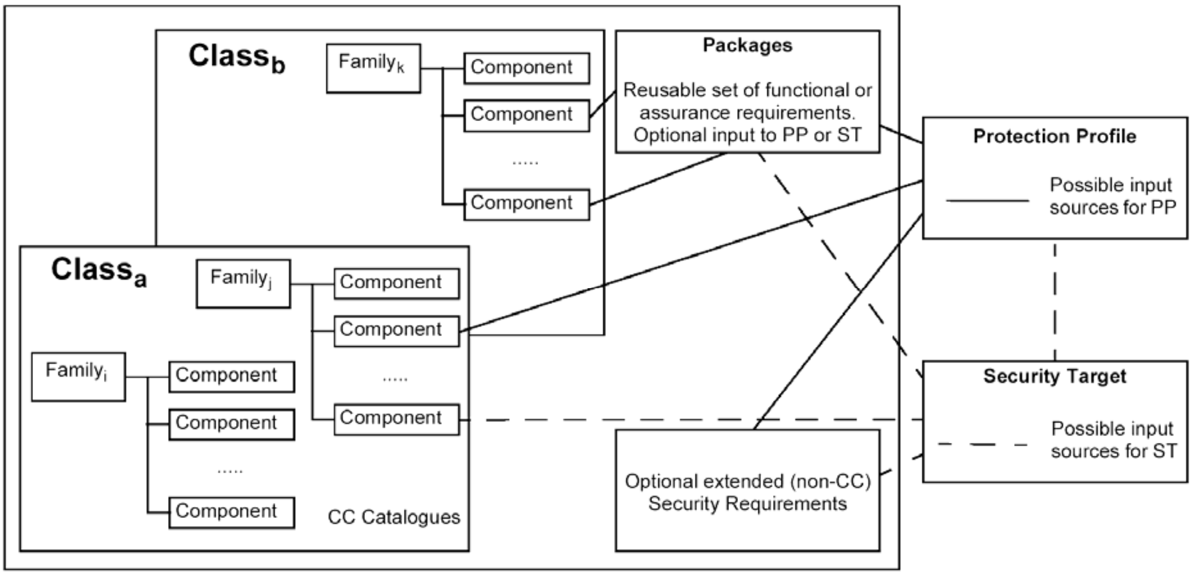

Figure 7 - Organisation and construction of requirements

144 The organisation of the CC security requirements into the hierarchy of class - family - component is provided to help consumers to locate specific security requirements.

145 The CC presents requirements for functional and assurance aspects in the same general style and uses the same organisation and terminology for each.

4.3.1.1 Class

146 The term class is used for the most general grouping of security requirements. All the members of a class share a common focus, while differing in coverage of security objectives.

147 The members of a class are termed families.

4.3.1.2 Family

148 A family is a grouping of sets of security requirements that share security objectives but may differ in emphasis or rigour.

149 The members of a family are termed components.

4.3.1.3 Component

150 A component describes a specific set of security requirements and is the smallest selectable set of security requirements for inclusion in the structures defined in the CC. The set of components within a family may be ordered to represent increasing strength or capability of security requirements that share a common purpose. They may also be partially ordered to represent related non-hierarchical sets. In some instances, there is only one component in a family so ordering is not applicable.

151 The components are constructed from individual elements. The element is the lowest level expression of security requirements, and is the indivisible security requirement that can be verified by the evaluation.

4.3.1.3.1 Dependencies between components

152 Dependencies may exist between components. Dependencies arise when a component is not self sufficient and relies upon the presence of another component. Dependencies may exist between functional components, between assurance components, and between functional and assurance components.

153 Component dependency descriptions are part of the CC component definitions. In order to ensure completeness of the TOE requirements, dependencies should be satisfied when incorporating components into PPs and STs where appropriate.

154 In other words: if security requirement A has a dependency on security requirement B, this means that whenever a PP/ST contains security requirement A, the PP/ST must contain:

a) security requirement B, or

b) a security requirement that is hierarchical to B, or

c) a justification why the PP/ST does not contain security requirement B

155 In cases a) and b), when a security requirement is included because of a dependency, it may be necessary to use operations on that security requirement to make sure that it actually satisfies the dependency.

156 For example, if FCS_COP.1 Cryptographic operation is included in the statement of security requirements to express the use of single DES for encryption, and FCS_CKM.1 Cryptographic key generation is also included in the statement of requirements, FCS_CKM.1 Cryptographic key generation should have its second assignment completed to “56 bits”.

157 In case c), the justification that a security requirement is not included should address either:

- why the dependency is not necessary or useful, in which case no further information is required, or
- that the dependency has been addressed by the operational environment of the TOE, in which case the justification should describe how the security objectives for the operational environment address this dependency.

158 An example of a valid justification that a dependency is not necessary is an ST that contains the SFR FCS_COP.1 Cryptographic operation to specify the use of an hashing algorithm. As this particular hashing algorithm uses no keys, the ST author indicates that all dependencies (FDP_ITC.1 Import of

user data without security attributes, FCS_CKM.1 Cryptographic key generation, FCS_CKM.4 Cryptographic key destruction, and FMT_MSA.2 Secure security attributes) are unnecessary because they deal with creating, destroying and security attributes of keys, and this algorithm does not use keys.

159 An example of a valid justification that a dependency has been addressed by the operational environment is an ST that contains the SFR FAU_STG.3 Action in case of possible audit data loss. This requirement has a dependency on FAU_STG.1 Protected audit trail storage. The ST author indicates that this dependency will be addressed by the operational environment with the justification that "Security Objective for the operational environment #12 specifies that the environment will provide 1GB storage of audit data protected from disclosure to and modification by non-sysadmin personnel, and will signal the TOE when less than 50MB is free."

4.3.1.3.2 Permitted operations on components

160 CC functional and assurance components may be used exactly as defined in the CC, or they may be tailored through the use of permitted operations in order to meet a security objective. When using operations, the PP/ST author must also be careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

– Iteration: allows a component to be used more than once with varying operations;

– Assignment: allows the specification of parameters;

– Selection: allows the specification of one or more items from a list; and

– Refinement: allows the addition of details.

161 The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components. The operations are described in more detail below.

The iteration operation

162 The iteration operation can be performed on every requirement. The PP/ST author performs an iteration operation by including the same requirement two or more times. Each iteration of a requirement must be different from all other iterations of that requirement, which is realised by applying different operations (or the same operations in a different way) to it. An example of an iteration is FRU_FLT.1 Degraded fault tolerance being iterated twice to:

a) The TSF shall ensure the operation of **digital signing** when the following failures occur: **failure of the digital signature verification mechanism**.

b) The TSF shall ensure the operation of **digital signature verification** when the following failures occur: **failure of the digital signing mechanism**.

The assignment operation

163 An assignment operation occurs where a given requirement contains an element with a parameter that may be set by the PP/ST author. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. An example of an element with an assignment is: FIA_AFL.1.2 When the defined number of authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions]**.

164 Whenever an element in a PP contains an assignment, a PP author may do one of three things:

a) leave the assignment uncompleted. The PP author could include FIA_AFL.1.2 "When the defined number of authentication attempts has been met or surpassed, the TSF shall **[assignment: list of actions]**." in the PP.

b) complete the assignment. As an example, the PP author could include FIA_AFL.1.2 "When the defined number of authentication attempts has been met or surpassed, the TSF shall **disable that users account**." in the PP

c) transform the assignment to a selection, thereby narrowing the assignment. As an example, the PP author could include FIA_AFL.1.2 "When the defined number of authentication attempts has been met or surpassed, the TSF shall **[selection: disable that users account, notify the administrator]**." in the PP.

165 Whenever an element in an ST contains an assignment, an ST author must complete that assignment, as indicated in b) above. Options a) and c) are not allowed for STs.

166 The values of the parameters and variables chosen to complete the assignment in b) above and of all parameters and values in c) above, must comply with the indicated type required by the assignment. An assignment may only be completed with "None" and an assignment may only be transformed into a selection with "None" as choice, if the component on which the requirement is based specifically allows this.

167 The Part 2 Annexes provide the guidance on the valid completion of assignments for SFRs. This guidance provides normative instructions on how to complete assignmentss, and those instructions shall be followed unless the PP/ST author justifies the deviation.

The selection operation

168 The selection operation occurs where a given requirement contains an element where a choice from several items has to be made by the PP/ST author. An example of an element with a selection is: FMT_AMT.1.1 The TSF shall run a suite of tests **[selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions]** to demonstrate the correct operations of the security assumptions provided by the abstract machine that underlies the TSF.

169 Whenever an element in a PP contains a selection, the PP author may do one of three things:

a) leave the selection uncompleted. As an example, the PP author could include FMT_AMT.1.1 “The TSF shall run a suite of tests **[selection: during initial start-up, periodically during normal operation, at the request of an authorised user, other conditions]** to ....” in the PP.

b) complete the selection by choosing one or more items. As an example, the PP author could include FMT_AMT.1.1 “The TSF shall run a suite of tests **during initial start-up and periodically during normal operation** to ....” in the PP.

c) restrict the selection by removing some of the choices, but leaving two or more. As an example, the PP author could include FMT_AMT.1.1 “The TSF shall run a suite of tests **[selection: periodically during normal operation, at the request of an authorised user]** to ....” in the PP.

170 Whenever an element in an ST contains a selection, an ST author must complete that selection, as indicated in b) above. Options a) and c) are not allowed for STs.

171 The item or items chosen in b) and c) must be taken from the items provided in the selection. If the component on which the requirement is based explicitly states “choose one of” for this selection, only one item may be selected in b).

172 The Part 2 Annexes provide the guidance on the valid completion of selections for SFRs. This guidance provides normative instructions on how to complete selections, and those instructions shall be followed unless the PP/ST author justifies the deviation.

The refinement operation

173 The refinement operation can be performed on every requirement. The PP/ST author performs a refinement by altering that requirement. The only rule for a refinement is that it must not “weaken” the original requirement: a TOE meeting the refined requirement must also meet the unrefined requirement in the context of the PP/ST. If a requirement exceeds this boundary it is considered to be an extended requirement and must be treated as such.

174 An example of an refinement is the first element of FTA_MCS.1 Basic limitation on multiple concurrent sessions "The TSF shall restrict the maximum number of concurrent sessions that belong to the same user." which is refined to "The TSF shall restrict the maximum number of concurrent FTP sessions that belong to the same user." If only FTP sessions are possible, this is a valid refinement. If it is also possible to telnet to the TOE, this would not be a valid refinement.

175 A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar. This change is not allowed to modify the meaning of the requirement in any way. Two examples of editorial refinements are:

– The requirement FMT_MTD.3 Secure TSF data "The TSF shall ensure that only **user names other than root and administrator** are accepted for user names" given later on, could be further refined to: "The TSF shall ensure that **root and administrator** are not accepted for **user names**"

– The requirement FAU_ARP.1 Security alarms with a single action: "The TSF shall take **inform the operator** upon detection of a potential security violation" could be refined to: "The TSF shall **inform the operator** upon detection of a potential security violation".

176 Another special case of refinement is where multiple iterations of the same requirement are used, each with different refinements, where some of the refined iterations do not meet the full scope of the original requirement. This is acceptable, provided that all iterations of the refined requirement taken collectively, meet the entire scope of the original requirement.

177 An example of this is a TOE with only two types of TSF data: user names and passwords. It uses iteration and refinement of FMT_MTD.3 Secure TSF data as follows:

– The TSF shall ensure that only user names other than root and administrator are accepted for user names

– The TSF shall ensure that only strings longer than 12 characters are accepted for passwords

178 Neither iteration covers the entire requirement, but the two iterations together do and this is therefore an acceptable refinement.

179 In addition, a refinement should be related to the original requirement. Refining an audit requirement with an extra element on prevention of electromagnetic radiation is not allowed. A PP/ST author wishing to add an unrelated element should add this refinement to a related requirement or, lacking this, write a extended requirement.

4.3.1.4 Use of security requirements

180 The CC defines three types of requirement constructs: package, PP and ST. The CC further defines a set of IT security criteria that can address the needs of many communities and thus serve as a major expert input to the production of these constructs. The CC has been developed around the central notion of using wherever possible the security requirements components defined in the CC, which represent a well-known and understood domain. Figure **8** shows the relationship between these different constructs.

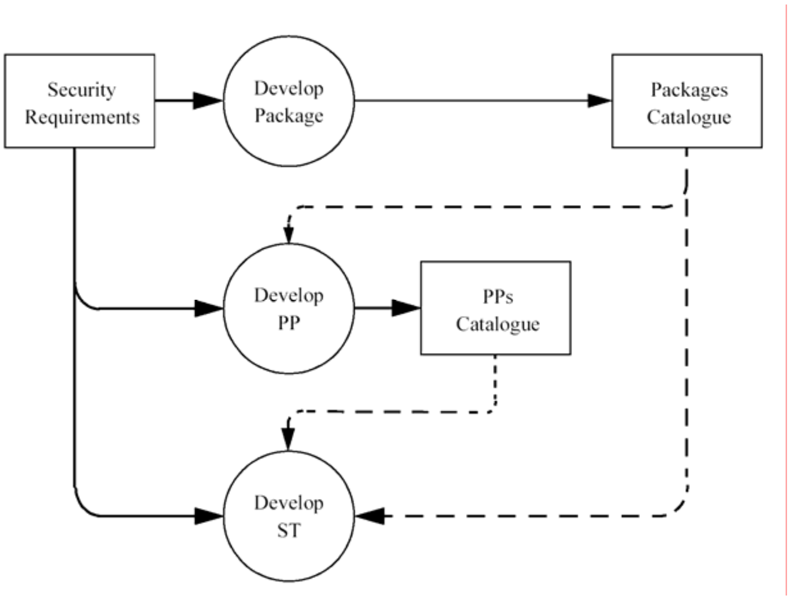

Figure 8 - Use of security requirements

4.3.1.4.1 Package

181 An intermediate combination of components is termed a package. The package permits the expression of a set of SFRs or a set of SARs. A package is intended to be reusable and to define requirements that are known to be useful and effective. A package may be used in the construction of larger packages, PPs, and STs.

182 The evaluation assurance levels (EALs) are predefined assurance packages contained in Part 3. An EAL is a baseline set of assurance requirements for evaluation. EALs each define a consistent set of assurance requirements. Together, the EALs form an ordered set that is the predefined assurance scale of the CC.

4.3.1.4.2 Protection Profile

183 A PP contains a set of security requirements that may be made by reference to another PP, directly by reference to CC functional or assurance components, or stated explicitly. The PP permits the implementation independent expression of security requirements for a set of TOEs that will comply fully with a set of security objectives. A PP is intended to be

reusable and to define TOE requirements that are known to be useful and effective in meeting the identified security objectives. A PP also contains the rationale for security objectives and security requirements.

184 A PP could be developed by user communities, IT product developers, or other parties interested in defining such a common set of requirements. A PP gives consumers a means of referring to a specific set of security needs and facilitates future evaluation against those needs.

185 Protection Profiles are discussed in detail in Annex B of this document.

4.3.1.4.3 Security Target

186 An ST contains a set of security requirements that may be made by reference to a PP, directly by reference to CC functional or assurance components, or stated explicitly. An ST permits the expression of security requirements for a specific TOE that are shown, by evaluation, to be useful and effective in meeting the identified security objectives.

187 An ST contains the TOE summary specification, together with the security requirements and objectives, and the rationale for each. An ST is the basis for agreement between all parties as to what security the TOE offers.

188 Security Targets are discussed in detail in Annex A of this document.

4.3.1.5 Sources of security requirements

189 Security requirements can be constructed by using the following inputs:

a) Existing PPs

The security requirements in an ST may be adequately expressed by, or are intended to comply with, a pre-existing statement of requirements contained in an existing PP.

Existing PPs may be used as a basis for a new PP.

b) Existing packages

Part of the security requirements in a PP or ST may have already been expressed in a package that may be used.

Examples of packages are the EALs defined in Part 3.

c) Existing functional or assurance requirements components

The functional or assurance requirements in a PP or ST may be expressed directly, using the components in Part 2 or 3.

d) Extended requirements

Additional functional requirements not contained in Part 2 and/or additional assurance requirements not contained in Part 3 may be used in a PP or ST.

190 Existing requirements material from Parts 2 and 3 should be used where available. The use of an existing PP will help to ensure that the TOE will meet a well known set of needs of known utility and thus be more widely recognised.

4.3.2 Types of evaluation

4.3.2.1 PP evaluation

191 The PP evaluation is carried out against the evaluation criteria for PPs contained in Part 3. The goal of such an evaluation is twofold: first to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a statement of requirements for an evaluatable TOE; second, in the case where a PP claims conformance to a PP or package, to demonstrate that the PP properly meets the requirements of the PP or package.

4.3.2.2 ST evaluation

192 The evaluation of the ST for the TOE is carried out against the evaluation criteria for STs contained in Part 3. The goal of such an evaluation is twofold: first to demonstrate that the ST is complete, consistent, and technically sound and hence suitable for use as the basis for the corresponding TOE evaluation; second, in the case where an ST claims conformance to a PP or package, to demonstrate that the ST properly meets the requirements of the PP or package.

4.3.2.3 TOE evaluation

193 The TOE evaluation is carried out against the evaluation criteria contained in Part 3 using an ST as the basis. The result of a TOE evaluation is to demonstrate that the TOE meets the security requirements contained in the evaluated ST.

5 Common Criteria requirements and evaluation results

5.1 Introduction

194 This clause presents the expected results from PP and TOE evaluation. PP or TOE evaluations lead respectively to catalogues of evaluated PPs or TOEs. ST evaluation leads to intermediate results that are used in the frame of a TOE evaluation.

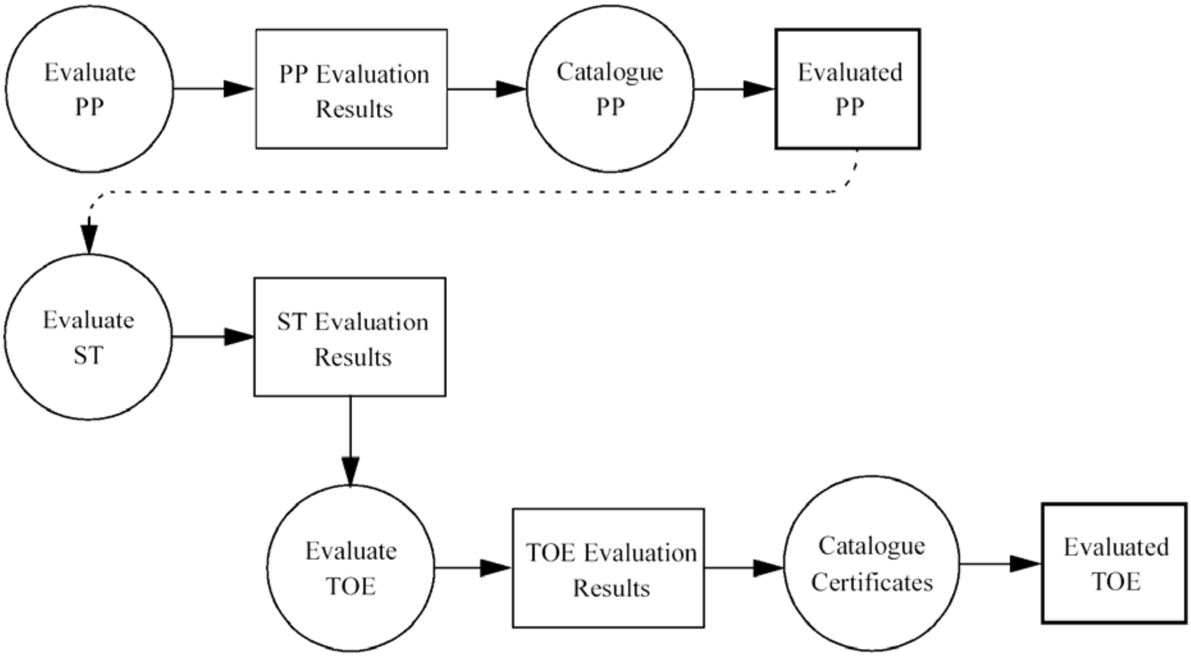

Figure 9 - Evaluation results

195 Evaluation should lead to objective and repeatable results that can be cited as evidence, even if there is no totally objective scale for representing the results of an IT security evaluation. The existence of a set of evaluation criteria is a necessary pre-condition for evaluation to lead to a meaningful result and provides a technical basis for mutual recognition of evaluation results between evaluation authorities. But the application of criteria contains both objective and subjective elements, that's why precise and universal ratings for IT security are not, therefore, feasible.

196 A rating made relative to the CC represents the findings of a specific type of investigation of the security properties of a TOE. Such a rating does not guarantee fitness for use in any particular application environment. The decision to accept a TOE for use in a specific application environment is based on consideration of many security issues including the evaluation findings.

5.2 Requirements in PPs and STs

197 The CC defines a set of IT security criteria that can address the needs of many communities. The CC has been developed around the central notion that the use of the security functional components contained in Part 2, and the EALs and assurance components contained in Part 3, represents the preferred course of action for expression of TOE requirements in PPs and STs, as they represent a well-known and understood domain.

198 Components in CC Part 2 and Part 3 can therefore be considered as pre-defined templates for SFRs and SARs, to be filled in and modified by operations in an PP/ST.

5.2.1 When to define extended components

199 Use of these pre-defined templates is mandatory, with two exceptions:

a) the TOE contains security functionality unique to that TOE, or a more general security functionality need is not covered by the CC (e.g. electro-magnetic emanations, strength of cryptographic algorithms);

b) a security objective can be translated, but only with great difficulty and/or complexity based on security requirements components in CC Part 2 and/or Part 3.

200 An example of this second case is already present in the CC in the form of FIA_AFL.1 Authentication failure handling. This component can also be expressed with FAU_GEN.1 Audit data generation, FAU_SAA.1 Potential violation analysis, and FAU_ARP.1 Security alarms. FIA_AFL.1 Authentication failure handling could therefore be considered redundant, but was nevertheless included into CC Part 2 because it very clearly expresses a specific instance of the use of requirements that is often used and provides a much clearer description that the combination of the three other components.

201 In both cases the PP/ST author is required to define his own components: new templates to base SFRs and SARs on. These newly defined components are called extended components. A precisely defined extended component is needed to provide context and meaning to the extended SFRs and SARs based on that component.

202 After the new components have been defined correctly, the PP/ST author can then base one or more SFRs or SARs on these newly defined extended components and use them in the same way as the other SFRs and SARs. From this point on, there is no further distinction between SARs and SFRs based on the CC and SARs and SFRs based on extended components.

5.2.2 How to define extended components

203 Whenever an PP/ST author defines an extended component, this has to be done in a similar manner to the existing CC components: clear, unambiguous

and evaluatable. Extended components must use similar labelling, manner of expression, and level of detail as the existing CC components.

204 The PP/ST author also has to make to sure that all applicable dependencies of a extended component are included. Examples of possible dependencies are:

a) if an extended component refers to auditing, dependencies to components of the FAU: Security audit class may have to be included;

b) if an extended component modifies or accesses user data, dependencies to components of the Access control policy (FDP_ACC) may have to be included;

c) if an extended component uses a particular design description (Functional Specification, High-Level Design, Low-Level Design, Implementation Representation), dependencies to components of the appropriate ADV family may have to be included.

205 In the case of an extended functional component, the PP/ST author also has to include any applicable audit and management information, similar to existing CC Part 2 components. In the case of an extended assurance component, the PP/ST author also has to provide suitable methodology to "perform" the component, similar to the methodology provided in the CEM.

206 Extended components may be placed in existing families, in which case the PP/ST writer has to show how these families change. If they do not fit into an existing family, they shall be placed in a new family. New families have to be defined similarly to the CC.

207 New families may be placed in existing classes in which case the PP/ST writer has to show how these classes change. If they do not fit into an existing class, they shall be placed in a new class. New classes have to be defined similarly to the CC.

5.2.3 PP evaluation results

208 The CC contains the evaluation criteria that permit an evaluator to state whether a PP is complete, consistent, and technically sound and hence suitable for use as a statement of requirements for an evaluatable TOE.

209 Evaluation of the PP shall result in a pass/fail statement. A PP for which the evaluation results in a pass statement shall be eligible for inclusion within a registry.

5.3 Requirements for a TOE

210 The CC contains the evaluation criteria that permit an evaluator to determine whether the TOE satisfies the security requirements expressed in the ST.

211 The results of a TOE evaluation shall include a statement of conformance to the CC. The use of CC terms to describe the security of a TOE permits comparison of the security characteristics of TOEs in general.

5.3.1 TOE evaluation results

212 The result of the TOE evaluation shall be a statement that describes the extent to which the TOE can be trusted to conform to the requirements.

213 Evaluation of the TOE shall result in a pass/fail statement. A TOE for which the evaluation results in a pass statement shall be eligible for inclusion within a registry. The results of evaluation shall also include a "Conformance Claim".

5.4 Conformance claim

214 The conformance claim indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance claim contains a CC conformance claim that:

a) describes to which version of the CC the TOE or PP claims conformance

b) describes the conformance to Part 2 (security functional requirements) as either:

- **Part 2 conformant** - A PP or TOE is Part 2 conformant if all SFRs are based only upon functional components in CC Part 2, or
- **Part 2 extended** - A PP or TOE is Part 2 extended if at least one SFR is not based upon functional components in CC Part 2.

c) describes the conformance to Part 3 (security assurance requirements) as either:

- **Part 3 conformant** - A PP or TOE is Part 3 conformant if all SARs are based only upon assurance components in CC Part 3, or
- **Part 3 extended** - A PP or TOE is Part 3 extended if at least one SAR is not based upon assurance components in CC Part 3.

215 Additionally, the conformance claim may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:.

- *Package name Conformant* - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

– *Package name Augmented* - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

216 Finally, the conformance claim may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) *PP Conformant* - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.

5.5 Use of TOE evaluation results

217 IT products and systems differ in respect to the use of the results of the evaluation. Figure **10** shows options for processing the results of evaluation. Products can be evaluated and catalogued at successively higher levels of aggregation until operational systems are achieved, at which time they may be subject to evaluation in connection with system accreditation.

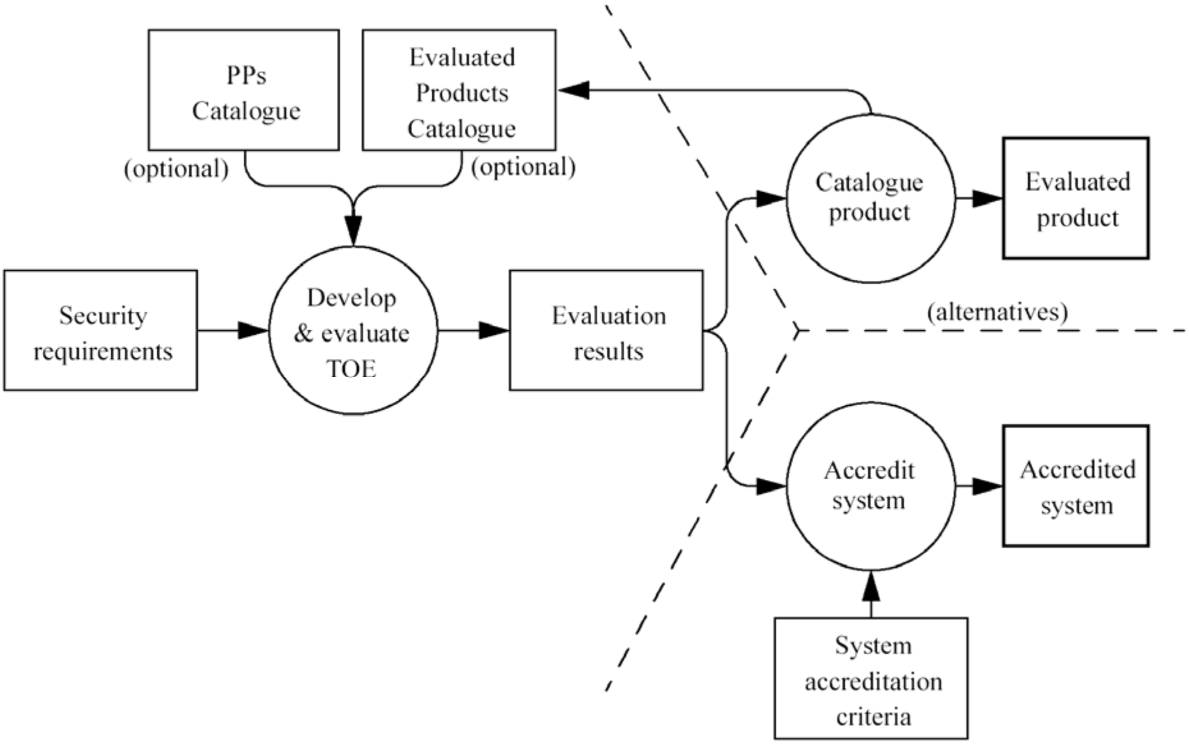

Figure 10 - Use of TOE evaluation results

218 The TOE is developed in response to requirements that may take account of the security properties of any evaluated products incorporated and PPs referenced. Subsequent evaluation of the TOE leads to a set of evaluation results documenting the findings of the evaluation.

219 Following an evaluation of an IT product intended for wider use, a summary of the evaluation findings might be entered in a catalogue of evaluated products so that it becomes available to a wider market seeking to use secure IT products.

220 Where the TOE is or will be included in an installed IT system that has been subject to evaluation, the evaluation results will be available to the system accreditor. The CC evaluation results may then be considered by the accreditor when applying organisation specific accreditation criteria that call for CC evaluation. CC evaluation results are one of the inputs to an accreditation process that leads to a decision on accepting the risk of system operation.

A Specification of Security Targets (normative)

A.1 Goal and structure of this Annex

221 The goal of this annex is to explain the ASE criteria and provide examples of their application. This annex does not define the ASE criteria, this definition can be found in CC Part 3.

222 This annex consists of three major parts:

a) *What an ST must contain*. This is summarised in Section A.2, and described in more detail in Sections A.4 - A.10. These sections describe the mandatory contents of the ST, the interrelationships between these contents, and provide examples.

b) *How an ST should be used*. This is summarised in Section A.3, and described in more detail in Section A.11. These sections describe how an ST should be used, and some of the questions that can be answered with an ST.

c) *Low Assurance STs*. Low Assurance STs are STs with strongly reduced content. They are described in detail in Section A.12.

A.2 Mandatory contents of an ST

223 Figure **11** portrays the mandatory contents of an ST. Figure **11** may also be used as a structural outline of the ST, though alternative structures are possible. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the ST instead of in the security requirements section. The separate sections of an ST and the contents of those sections are briefly summarised below and described in much more detail in Sections A.4 to A.10. An ST normally must contain:

a) an *ST introduction* containing three narrative descriptions of the TOE on different levels of abstraction;

b) a *conformance claim*, showing whether the ST claims conformance to any PPs and/or packages, and if so, to which PPs and/or packages;

c) a *security problem definition*, showing the threats, OSPs and assumptions that must be countered, enforced and upheld by the TOE and its operational environment;

d) *security objectives*, showing how the solution to the security problem is divided between:

- the TOE;

- the development environment of the TOE;
- the operational environment of the TOE;

e) *extended components definition*, where new components (i.e. not included in CC Part 2 or CC Part 3) may be defined. These new components can then be used to define extended functional and extended assurance requirements with.

f) *security requirements*, where a well-defined translation of the security objectives for the TOE and the security objectives for the development environment is provided. This well-defined translation is in the form of SFRs (CC Part 2 requirements and extended functional requirements) and SARs (CC Part 3 requirements and extended assurance requirements);

g) a *TOE summary specification*, showing how the SFRs are implemented in the TOE.

224 There also exists low assurance STs which have reduced contents, these are described in detail in Section A.12. The rest of this Annex assumes that an ST with full contents is used.

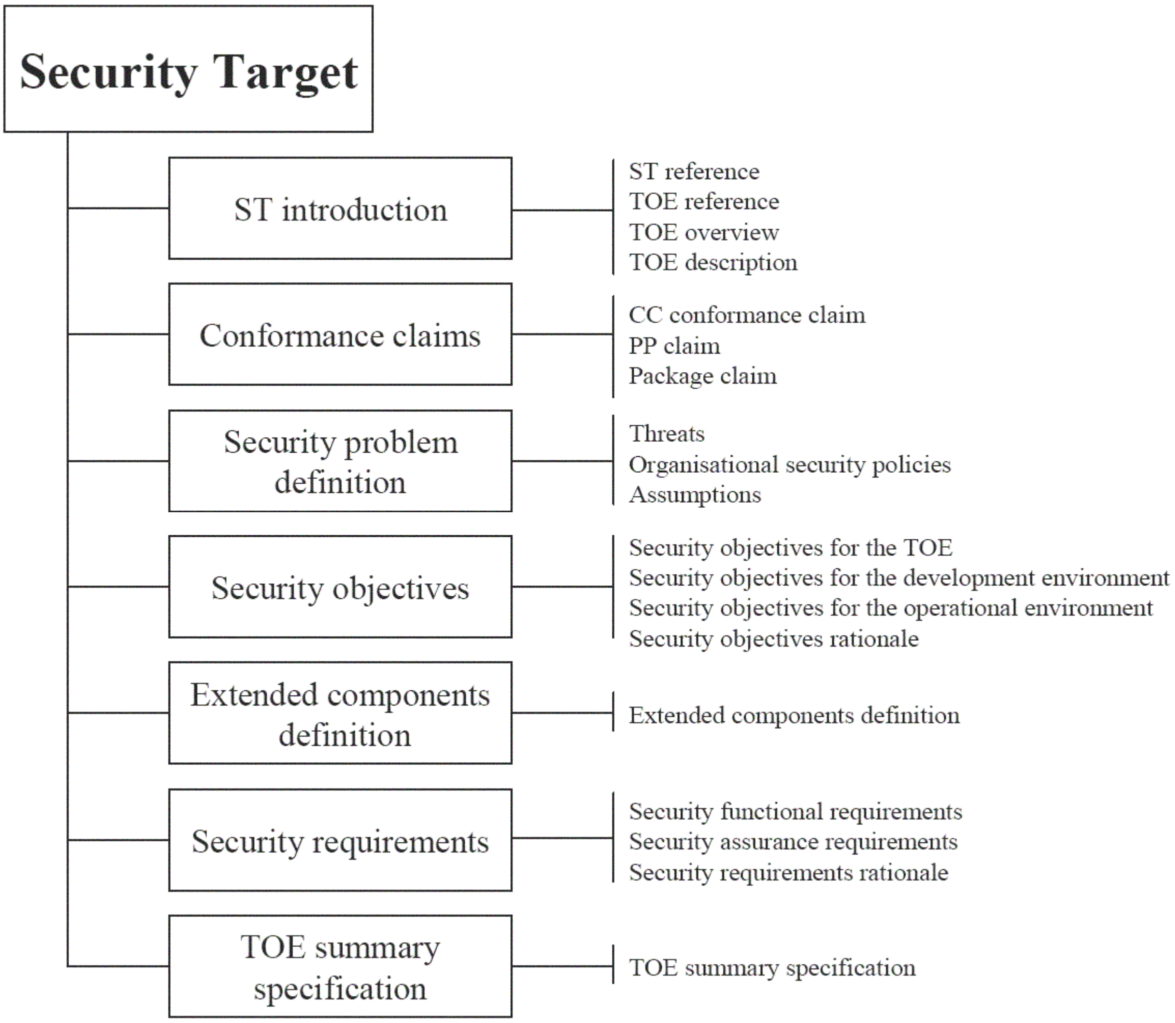
Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
CC conformance claim
PP claim
Package claim
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the development environment
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
TOE summary specification
TOE summary specification

Figure 11 - Security Target contents

A.3 Using the ST (informative)

A.3.1 How an ST should be used

225 A typical ST fulfills two roles:

- Before and during the evaluation, the ST specifies "what is to be evaluated". In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role. Section A.7 describes how the ST should be used in this role.

- After the evaluation, the ST specifies "what was evaluated". In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumer can rely on this description because the TOE has been evaluated to meet the ST. Ease of use and understandability are major issues for this role. Section A.11 describes how the ST should be used in this role.

A.3.2 How an ST should not be used

226 Two roles (among many) that an ST should not fulfill are:

- *a detailed specification*: An ST is designed to be a security specification on a relatively high level of abstraction. An ST should, in general, not contain detailed protocol specifications, detailed decriptions of algorithms and/or mechanisms, long description of detailed operations etc.

- *a complete specification*: An ST is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size and weight, required voltage etc. should not be part of an ST. This means that in general an ST may be a part of a complete specification, but is not a complete specification in itself.

A.4 ST Introduction (ASE_INT)

227 The ST introduction describes the TOE in a narrative way on three levels of abstraction:

a) the ST reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to;

b) the TOE overview, which briefly describes the TOE;

c) the TOE description, which describes the TOE in more detail.

A.4.1 ST reference and TOE reference

228 An ST contains a clear ST reference that identifies that particular ST. A typical ST reference consists of title, version, authors and publication date. An example of an ST reference is “MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 10/11/02”. The reference must be unique so that it is possible to tell different STs and different versions of the same ST apart.

229 An ST also contains a TOE reference that identifies the TOE that claims conformance to the ST. A typical TOE reference consists of developer name, TOE name and TOE version number. An example of a TOE reference is “MauveCorp MauveRAM Database v2.11”. As a single TOE may be evaluated multiple times, for instance by different consumers of that TOE, and therefore have multiple STs, this reference is not necessarily unique.

230 If the TOE is related to one or more well-known products, it is allowed to reflect this in the TOE reference. However, this should not be used to

mislead consumers: situations where only a part of a product is evaluated, yet the TOE reference does not reflect this are not allowed.

231 The ST reference and the TOE reference facilitate indexing and referencing the ST and TOE and their inclusion in summaries of lists of evaluated products.

A.4.2 TOE overview

232 The TOE overview is aimed at potential consumers of a TOE who are looking through lists of evaluated products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware. The typical length of a TOE overview is several paragraphs.

233 To this end, the TOE overview briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware/software/firmware required by the TOE.

A.4.2.1 Usage and major security features of a TOE

234 The description of the usage and major security features of the TOE is intended to give a very general idea of what the TOE is capable of, and what it can be used for in a security context.

235 An example of this is “The MauveCorp MauveRAM Database v2.11 is a multi-user database intended to be used in a networked environment. It allows 1024 users to be active simultaneously. It allows password/token and biometric authentication, protects against accidental data corruption, and can roll-back 10.000 transactions. Its audit features are very configurable, so as to allow detailed audit to be performed for some users and transactions, while protecting the privacy of other users and transactions.”

A.4.2.2 TOE type

236 The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smartcard, crypto-modem, intranet, web server, database, webserver and database, LAN, LAN with webserver and database, etc.

237 In some cases, a TOE type can mislead consumers. Examples include:

- certain functionality can be expected of the TOE because of its TOE type, but the TOE does not have this functionality. Examples include:
  - an ATM-card type TOE, which does not have any identification/authentication functionality;
  - a firewall type TOE, which does not support protocols that are almost universally used;
  - a PKI-type TOE, which has no certificate revocation functionality.

- the TOE can be expected to operate in certain operational environments because of its TOE type, but it cannot do so. Examples include:
  - a PC-operating system type TOE, which is unable to function securely unless the PC has no network connection, floppy drive, and CD/DVD-player;
  - a firewall, which is unable to function securely unless all users that can connect through that firewall are benign.

238 In these cases, the TOE overview contains additional information to ensure that potential consumers are not misled.

A.4.2.3 Required non-TOE hardware/software/firmware

239 While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify this non-TOE hardware/software/firmware.

240 It is not required to provide a complete and fully detailed identification of all this hardware/software/firmware, but the identification should be complete and detailed enough for potential consumers to determine the major hardware/software/firmware components needed to use the TOE.

241 Example hardware/software/firmware identifications are:

- a standard PC with a 1GHz or higher processor and 512MB or more RAM, running version 3.0 Update 6b, c, or 7, or version 4.0 of the Inux operating system;
- a standard PC with a 1GHz or higher processor and 512MB or more RAM, running version 3.0 Update 6d of the Inux operating system and the WonderMagic 1.0 Graphics card with the 1.0 WM Driver Set;
- a CleverCard SB2067 integrated circuit;
- a CleverCard SB2067 integrated circuit running v2.0 of the QuickOS smartcard operating system;
- the December 2002 installation of the LAN of the Director-General"s Office of the Department of Traffic.

A.4.3 TOE description

242 A TOE description is a narrative description of the TOE, likely to run to several pages.The TOE description therefore contains more detailed information than the TOE overview. The TOE description should provide evaluators and potential consumers with a general understanding of the security capabilities of the TOE, in more detail than was provided in the

TOE overview. The TOE description may also be used to describe the wider application context into which the TOE will fit.

243 The TOE description discusses the physical scope and boundaries of the TOE: the hardware, firmware and software parts that constitute the TOE at a level of detail that is sufficient to give the reader a general understanding of those parts. The TOE description should also list all guidance that is part of the TOE.

244 The TOE description should also discuss the logical scope and boundaries of the TOE: the logical security features offered by the TOE at a level of detail that is sufficient to give the reader a general understanding of those features.

245 An important property of the physical and logical descriptions is that they describe the boundaries of the TOE in such a way that there remains no doubt on whether a certain part or feature is in the TOE or whether this is outside the TOE. This is especially important when the TOE is intertwined with and cannot be easily separated from non-TOE entities.

246 Examples where the TOE is intertwined with non-TOE entities are:

- the TOE is a cryptographic co-processor of an IC, instead of the entire IC;
- the TOE is an IC, except for the cryptographic processor;
- the TOE is the Network Address Translation part of the MinuteGap Firewall v18.5.

A.5 Conformance claims (ASE_CCL)

247 This section of an ST describes how the TOE conforms with:

- the Common Criteria itself
- Protection Profiles (if any)
- Packages (if any)

in the form of a conformance claim. This conformance claim is described in detail in Section 5.4.

248 If the conformance claim refers to one or more PPs and/or packages, the ST must also be actually conformant to those PPs and/or packages. In some cases, this means that the ST must contain additional material in the form of a conformance rationale.

A.5.1 Conforming to a Protection Profile

249 The CC allows three types in which a ST can claim conformance to another PP: exact, strict and demonstrable. The type of conformance is specified in the conformance statement of the PP that is being claimed conformance to.

250 In other words, this PP effectively states “Any ST claiming conformance to me, must do so in an [exact, strict, demonstrable] manner. The ST claiming conformance to that PP simply states that it claims conformance to that PP.

251 The three types of conformance are summarised below, and described more extensively in Sections A.5.2, A.5.3 and A.5.4.

252 **Exact conformance** is expected to be used by those PP authors with the most stringent requirements that are to be expressed in a single manner. This approach to PP specification will limit the PPs/STs able to claim conformance to the PP purely on the basis of the wording used in the PP, rather than a technical ability to meet the security requirements. This may be used in Request for Development in a product acquisition process.

253 **Strict conformance** is expected to be used by those PP authors with vast experience of developing PPs, who again have requirements that must be adhered to in the manner specified. However, this completion permits the PP/ST author claiming compliance to the PP to add to those requirements, provided it is in a restrictive manner. i.e. the additional requirements cannot weaken the existing requirements, so hierarchical components can be used or additional components that build on those specified.

254 **Demonstrable conformance** allows a PP author to describe a common security problem to be solved and generic guidelines to the requirements necessary for its resolution, in the knowledge that there is likely to be more than some way of specifying a resolution.

255 Note that conformance is a binary property of a ST; either the ST conforms to the PP in question or it does not. The CC does not recognise "partial" conformance. As partial conformance is not permissible, it is the responsibility of the PP author to ensure the PP is not overly onerous, prohibiting ST authors in claiming conformance to the PP.

A.5.2 Exact conformance

256 "Exact conformance" is oriented to the PP-author who requires evidence that the requirements in the PP are met precisely and that any ST claiming conformance is an instantiation of the PP; there are to be no additions or modifications from the specification of the PP.

- The security problem definition and objectives specified in the PP are to either be duplicated in the ST or the ST is to merely reference the appropriate sections in the PP.
- Alternative security requirement claims to those in the PP cannot be used in the ST.
- No additional (functional or assurance) security requirement claims can be made in the ST.

- All remaining assignment and selection operations are to be completed.

257 The conformance rationale will be a trivial statement that the security problem definition, statement of security objectives and statement of security requirements have been included in the ST.

A.5.3 Strict conformance

258 "Strict conformance" is oriented to the PP-author who requires evidence that the requirements in the PP are met precisely and that the ST is an instantiation of the PP:

- The statements of the security problem definition and the objectives are to be consistent with those in the PP. These statements can be re-worded using terminology with which the ST consumer will be conversant. However, the conformance rationale is to demonstrate that each aspect of the statements specified in the PP has been provided in the ST.
- The objectives for the operational environment can be modified providing the statement of security objectives in the ST is more restrictive that than that of the PP. This can include reassigning an objective specified for the environment in the PP to be a TOE objective in the ST.
- The SFRs specified in the ST must be a non-strict superset of the SFRs specified in the PP; i.e. the ST must claim the SFRs specified in the PP as a minimum, and no alternative requirements can be claimed in the place of a PP SFR.
- The SARs specified in the ST must be a non-strict superset of the SARs specified in the PP; i.e. the ST must claim SARs specified in the PP as a minimum, and no alternative requirements can be claimed in the place of a PP SAR.
- The additional requirement claims made in the ST must result in the specification of the TOE being more restrictive than that of the PP.
- The completion of operations must be consistent with that in the PP; either the same completion will be used in the ST as that in the PP or one that makes the requirement more restrictive (the rules of refinement apply).

259 If the PP author does not wish objectives for the environment to be re-assigned as objectives of the TOE, he should

a) consider whether it would be more appropriate to require "exact" conformance;

b) express the objective for the environment in such a way that it cannot be reworded as a TOE objective, whilst remaining consistent with that specified in the PP.

c) consider whether it would be permissible for the TOE to meet this objective provided it could be configured. i.e. the security function in the TOE meeting the requirement can be switched off through a configuration option without adversely affecting any other security functions of the TOE.

260 The conformance rationale in an ST conforming to a PP requiring strict conformance will be a simple tracing between the statement of security requirements in the PP and the ST, and a discussion of:

- how the restatement of the security problem definition and objectives in the ST is consistent with that specified in the PP. All aspects of the statements will be considered and traced.
- the security requirements included in the ST in addition to those specified in the PP. This will include tracing these requirements to the additional aspects of the statements of security problem definition and objectives included in the ST.

A.5.4 Demonstrable conformance

261 "Demonstrable conformance" is orientated to the PP-author who requires evidence that the ST/TOE is a suitable solution to the generic security problem described in the PP. Demonstrable conformance also caters for the ST author wishing to claim conformance to multiple PPs.

- The SARs specified in the ST must be a non-strict superset of the SARs specified in the PP. i.e. the ST must claim SARs specified in the PP as a minimum, and no alternative requirements can be claimed in the place of a PP SAR.
- The ST, although ensuring all requirements specified in the PP are expressed in the ST, is able to use alternative SFRs taken from Part 2 where applicable. A rationale will be provided to explain how the set of requirements specified in the ST is consistent with that specified in the PP.
- The ST author may specify SFRs in addition to those required to meet the security problem defined in the PP, if they are necessary to meet the (extended) security problem defined in the ST.
- Any changes to the operational environment description will make the description more restrictive in the sense of refinement), or be as a result of moving an objective specified for the operational environment in the PP to become an objective for the TOE in the ST. A rationale will be provided to explain how the operational

environment described in the ST is consistent with that described in the PP.

- The completion of operations will be consistent with those in the PP; i.e the same completion is used in the ST as that in the PP or a completion that makes the requirement more restrictive (the rules of refinement apply).

  For example, if the PP author restricts the selection of four items in the component FAU_GEN.1.1b to two items in the PP. The ST can then only choose from the two in the PP, and not the other two. Nevertheless, the ST author may also add some audit events within the assignment in FAU_GEN.1.1c.

262 The conformance rationale is to demonstrate the following:

a) How each requirement in the PP is represented in the ST. If alternative requirements are expressed in the ST, the rationale is to contain the ST authors understanding of the relevant PP objective(s) and how the alternative requirement(s) still result in achievement of the objective(s).

b) That the statement of objectives for the operational environment in the PP is fully expressed in the ST. This may be either:

   - through equivalent or more restrictive objectives than those in the PP; or

   - through expression of a TOE requirement that has been introduced in the ST to meet an objective stated for the environment in the PP.

c) The source of each additional security requirement; how it is necessary to meet the extended objectives for the TOE, resulting from extended SPD statement in the ST.

A.5.5 Conformance to a package

263 A package is defined as a set of functional or assurance requirements that meet an identifiable subset of security objectives. It is intended to be re-usable, to be used in the construction of larger packages, PPs and STs. At present there are no criteria for the evaluation of packages, to confirm their content or to place requirements upon packages. e.g. that a package must include a statement of the type of conformance. Therefore, only the security requirements specified in a package are considered when conformance to a package is claimed.

264 The package conformance claims are <package name> conformant and <package name> augmented. These are comparative to exact and strict respectively. The ST author specifies the type of conformance to a package.

265 The completions of operations in the ST are to be consistent with that specified in the requirements package. Therefore, the same completion is used in the ST as that in the package or a completion that makes the requirement more restrictive (the rules of refinement apply).

A.5.5.1 <package name> conformant

266 A conformance claim that an ST is "<package name> conformant" is considered to fall under the categorisation of "exact" conformance used for PP conformance claims. Therefore, all requirements in the package must be included in the ST, with no substitution and no additions.

A.5.5.2 <package name> augmented

267 A conformance claim that an ST is "<package name> augmented" is considered to fall under the categorisation of "strict" conformance used for PP conformance claims. Therefore, all requirements in the package must be included in the ST, with no substitution. However, requirements in addition to those specified in the PP may be included in the ST.

A.6 Security problem definition (ASE_SPD)

A.6.1 Introduction

268 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 falls outside the scope of the CC, with two exceptions:

- the security problem definition must be correctly defined, that is: the statements must be in the form of threats, OSPs and/or assumptions, and these statements that meet the rules described in this section;
- the security problem definition must be internally consistent

269 However, it should be noted that the usefulness of the results of an evaluation strongly depends on the ST, and the usefulness of the ST strongly depends on the quality of the security problem definition. It is therefore often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good security problem definition.

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

271 Also note that where the TOE is physically distributed, it may be better to discuss the relevant threats, OSPs and assumptions separately for distinct domains of the TOE operational environment. Similarly, where the development environment of the TOE consists of multiple sites or stages, it may be better to discuss the relevant threats and OSPs separately for each distinct site or stage.

A.6.2 Threats

272 This section of the security problem definition shows the threats that are to be countered by the TOE, its development environment, its operational environment, or a combination of these three.

273 A threat consists of a threat agent, an asset (either in the operational or in the development environment) and an adverse action of that threat agent on that asset.

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

275 Examples of *assets* can be found in Section 4.1.

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

277 Examples of threats are:

– a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network;

– a worm seriously degrading the performance of a wide-area network;

– a virus sending out stored confidential email to random recipients;

– a TOE developer employee making an accidental error affecting the correctness of the low-level design of the TOE;

– a system administrator violating user privacy;

– 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.

A.6.3 Organisational security policies (OSPs)

278 This section of the security problem definition shows the OSPs that are to be enforced by the TOE, its development environment, its operational environment, or a combination of these three.

279 OSPs are rules, practices, or guidelines. These may be laid down by the organisation controlling the operational environment of the TOE, or they may stem from legislative or regulatory bodies. OSPs can apply to the TOE,

the operational environment of the TOE, and/or the development environment of the TOE.

280 Examples of OSPs are:

- All products that are used by the Government must conform to the National Standard for password generation and encryption;
- All products that are used by the branches of the Bank, must be CC-certified with the EAL 4 + ADV_IMP.2 assurance package;
- All system administrators that have access to the Department File Servers must be vetted to the level of Department Secret.

A.6.4 Assumptions

281 This section of the security problem definition shows the assumptions that the TOE makes on its operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

282 Examples of assumptions are:

- Assumptions on physical aspects of the operational environment:
    - the TOE assumes that it will be placed in a room that is designed to minimise electro-magnetic emanations;
    - the TOE assumes that its administrator consoles will be placed in a restricted access area.
- Assumptions on personnel aspects of the operational environment:
    - the TOE assumes that its users will be trained sufficiently in order to operate the TOE;
    - the TOE assumes that its users are vetted for information that is classified as National Secret;
    - the TOE assumes that its users will not write down their passwords.
- Assumptions on connectivity aspects of the operational environment:
    - the TOE assumes that it will run on a PC workstation with at least 10GB of disk space;
    - the TOE assumes that it is the only non-OS application running on this workstation;

- the TOE assumes that it will not be connected to an untrusted network.

283 Note that assumptions can only apply to the operational environment. Assumptions can never apply to the TOE and/or the development environment, as the TOE cannot assume anything about itself, or on how it is developed.

A.7 Security objectives (ASE_OBJ)

284 The security objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the security objectives is threefold:

- provide a high-level, natural language solution of the problem;
- divide this solution into three partwise solutions, that reflect that different entities each have to address a part of the problem;
- demonstrate that these partwise solutions form a complete solution to the problem.

A.7.1 High-level solution

285 The security objectives consist of a set of short and clear statements without overly much detail that together form a high-level solution to the security problem. The level of abstraction of the security objectives aims at being clear and understandable to knowledgeable potential consumers of the TOE. The security objectives are in natural language, as a more exact, well-defined description of some of the security objectives will be provided as part of the security requirements, which are described later on in this chapter.

A.7.2 Partwise solutions

286 In an ST the high-level security solution as described by the security objectives is divided into three partwise solutions. These partwise solutions are called the security objectives for the TOE, the security objectives for the development environment, and the security objectives for the operational environment. This reflects that these partwise solutions are to be provided by three different entities: the TOE, the development environment and the operational environment.

A.7.2.1 Security objectives for the TOE

287 The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This partwise solution is called the security objectives for the TOE and consists of a set of statements describing the security goals that the TOE should achieve in order to solve its part of the problem.

288 Examples of security objectives for the TOE are:

- The TOE shall keep confidential the content of all files transmitted between it and a Server;

- The TOE shall identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE;

- The TOE shall restrict user access to data according to the Data Access policy described in Annex 3 of the ST.

289 If the TOE is physically distributed, it may be better to subdivide the security objectives for the TOE into several sections to reflect this.

A.7.2.2 Security objectives for the development environment

290 The development environment of the TOE contains technical and procedural measures to provide assurance that the TOE will correctly provide its security functionality (which is defined by the security objectives for the TOE). This partwise solution is called the security objectives for the development environment and consists of a set of statements describing the security goals that should be achieved in the development environment.

291 Examples of security objectives for the development environment are:

- The development environment shall ensure that the TOE is delivered to the consumer without compromising the integrity of the TOE;

- The development environment shall ensure that the integrity of the source code of the TOE is protected;

- The development environment shall ensure that complete and clear guidance to the TOE is developed, thus minimising the probability that users will use the TOE in manner that it was not intended;

- The development environment shall conform with EAL 4 augmented with ADV_IMP.2.

292 If the development environment of the TOE consists of multiple sites or stages, it may be better to subdivide the security objectives for the development environment into several sections to reflect this.

A.7.2.3 Security objectives for the operational environment

293 The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). This partwise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment should achieve.

294 Examples of security objectives for the operational environment are:

– The operational environment shall provide a workstation with the OS Inux version 3.01b to execute the TOE on;

– The operational environment shall ensure that all human TOE users receive appropriate training before allowing them to work with the TOE;

– The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel;

– The operational environment shall ensure the confidentiality of the audit logs generated by the TOE before sending them to the central Audit Server.

295 If the operational environment of the TOE consists of multiple sites, each with different properties, it may be better to subdivide the security objectives for the operational environment into several sections to reflect this.

A.7.3 Relation between security objectives and the security problem definition

296 The ST also contains a security objectives rationale containing two sections:

– a tracing that shows which security objectives address which threats, OSPs and assumptions;

– a set of justifications that shows that all threats, OSPs, and assumptions are effectively addressed by the security objectives.

A.7.3.1 Tracing between security objectives and the security problem definition

297 The tracing shows how the security objectives trace back to the threats, OSPs and assumptions as described in the security problem definition. This tracing must obey three rules:

a) *No spurious objectives*: Each security objective traces to at least one threat, OSP or assumption.

b) *Complete w.r.t. the security problem definition*: Each threat, OSP and assumption has at least one security objective tracing to it.

c) *Correct tracing*: Since assumptions are always made by the TOE on the operational environment, security objectives for the TOE and for the development environment do not trace back to assumptions. The allowed tracings are depicted in Figure **12**.

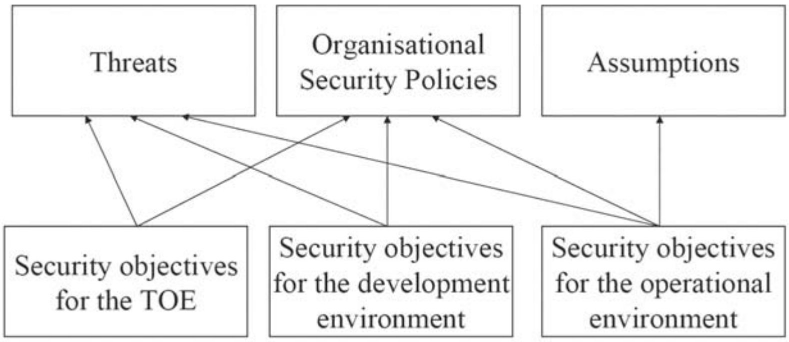
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the development environment
Security objectives for the operational environment

Figure 12 - Allowed tracings between security objectives and security problem definition

298 Multiple security objectives may trace to the same threat, indicating that the combination of those security objectives counters that threat. A similar argument holds for OSPs and assumptions.

A.7.3.2 Providing a justification for the tracing

299 The security objectives rationale also demonstrates that the tracing is effective: if all security objectives tracing to a particular threat/OSP/assumption are achieved, that threat/OSP/assumption is countered/enforced/upheld.

300 This demonstration analyses the effect of achieving the relevant security objectives on countering the threat/enforcing the OSP/upholding the assumptions and lead to the conclusion that this is indeed the case.

301 In some cases, where parts of the security problem definitions very closely resemble some security objectives, the demonstration can be very simple. An example is: a threat “T17: Threat agent X reads the Confidential Information in transit between A and B”, a security objective for the TOE: “OT12: The TOE shall ensure that all information transmitted between A and B is kept confidential”, and a demonstration “T17 is directly countered by OT12”.

A.7.3.3 On countering threats

302 Countering a threat does not necessarily mean removing that threat, it can also mean sufficiently diminishing that threat or sufficiently mitigating that threat.

303 Examples of removing a threat are:

- removing the ability to execute the adverse action from the threat agent;
- moving, changing or protecting the asset in such a way that the adverse action is no longer applicable to it;
- removing the threat agent (e.g. removing machines from a network that frequently crash that network).

304 Examples of diminishing a threat are:

- restricting the threat agent in adverse actions;
- restricting the opportunity to execute an adverse action of a threat agent;
- reducing the likelihood of an executed adverse action being successful;
- reducing the motivation to execute an adverse action of a threat agent by deterrence;
- requiring greater expertise or greater resources from the threat agent.

305 Examples of mitigating the effects of a threat are:

- making frequent back-ups of the asset;
- obtaining spare copies of an asset;
- insuring an asset;
- ensure that successful adverse actions are always timely detected, so that appropriate action can be taken.

A.7.4 Security objectives: conclusion

306 Based on the security objectives and the security objectives rationale, the following conclusion can be drawn: if all security objectives are achieved then the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

A.8 Extended Components Definition (ASE_ECD)

307 In this section of the ST all additional components needed in the ST, but not present in CC Part 2 or Part 3 are defined. For more information on this, see Section 5.2.

A.9 Security requirements (ASE_REQ)

A.9.1 Well-defined translation

308 The security requirements are a well-defined translation of the security objectives for the TOE and the security objectives for the development environment. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed). The CC requires this well-defined translation for several reasons:

– to provide an exact description of what is to be evaluated: the security functional requirements (SFRs). These are a well-defined translation of the security objectives for the TOE.

– to provide an exact description of how the TOE is to be evaluated: the security assurance requirements (SARs). These are a well-defined translation of the security objectives for the development environment.

– to allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the well-defined translations must use the same terminology and concepts. This allows easy comparison.

309 There is no well-defined translation required in the CC for the security requirements for the operational environment, because the operational environment is not evaluated in this evaluation and does therefore not require a more exact description. It may be the case that parts of the operational environment are evaluated in another evaluation, but this is out of scope for the current evaluation.

A.9.2 How the CC supports this well-defined translation

310 The CC supports this well-defined translation in four ways:

a) by providing a predefined well-defined “language” designed to describe exactly what is to be evaluated. This language is defined as a set of components defined in CC Part 2. The use of this language as a well-defined translation of the security objectives for the TOE to SFRs is mandatory, though some exceptions exist (see Section 5.2).

b) by providing a predefined well-defined “language” designed to describe exactly how the TOE is to be evaluated. This language is defined as a set of components defined in CC Part 3. The use of this language as a well-defined translation of the security objectives for the development environment to SARs is mandatory, though some exceptions exist (see Section 5.2).

c) by providing operations: mechanisms that allow the ST writer to modify the SFRs and SARs to provide a more accurate translation of the security objectives for the TOE and the development environment. The CC has four operations: assignment, selection, iteration, and refinement. These are described further in Section 4.3.1.3.2.

d) by providing dependencies: a mechanism that supports a more complete translation to SFRs and SARs. In the CC Part 2 and Part 3 languages, a security requirement can have a dependency on other security requirements. This signifies that if an ST uses that requirement, it generally needs to use those other security requirements as well. This makes it much harder for the ST writer to overlook including necessary requirements. These are described further in Section 4.3.1.3.1.

A.9.3 Relation between security requirements and security objectives

311 The ST also contains a security requirements rationale, consisting of two sections:

- a tracing that shows which security requirements address which security objectives;
- a set of justifications that shows that all security objectives for the TOE and for the development environment are effectively addressed by the security requirements.

A.9.3.1 Tracing between security requirements and the security objectives

312 The tracing shows how the SFRs and SARs trace back to the security objectives for the TOE and the security objectives for the development environment. This tracing must obey three rules:

a) *No spurious SFRs/SARs*: Each SFR/SAR traces back to at least one security objective.

b) *Complete w.r.t. the security objectives for the TOE and the development environment*: Each security objective for the TOE and each security objective for the development environment has at least one security requirement tracing to it.

c) *Correct tracing*:

   - SFRs define measurable functional properties of the TOE, and can therefore trace only to security objectives for the TOE;
   - SARs define that the TOE and certain documents with a certain content and presentation must be available and that the developer and evaluator must undertake certain actions on the TOE and on these documents. As all these actions take place in the development environment, SARs can only trace to security objectives for the development environment.

313 The allowed tracings are depicted in Figure **13**.

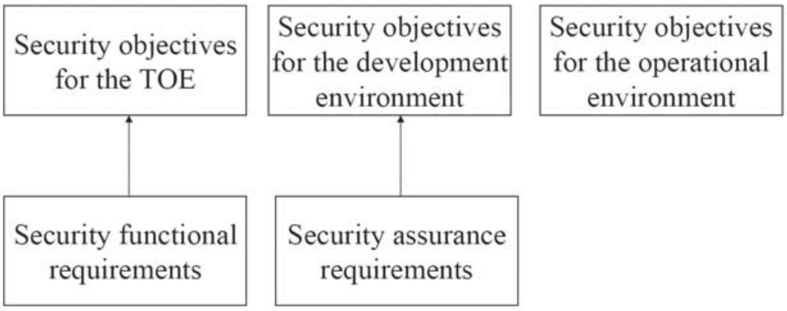
Security objectives for the TOE
Security objectives for the development environment
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure 13 - Allowed tracings between security requirements and security objectives

314 Multiple security requirements may trace to the same security objective, indicating that the combination of those security requirements meets that objective.

A.9.3.1.1 Providing a justification for the tracing

315 The security requirements rationale must also demonstrate that the tracing is effective: if all security requirements tracing to a particular security objective are satisfied, that security objective is achieved.

316 This demonstration should analyse the effect of satisfying the relevant security objectives on achieving the security objective and lead to the conclusion that this is indeed the case.

317 In some cases, where security requirements very closely resemble some security objectives, the demonstration can be very simple. An example is:

– A security objective for the development environment “OD14: The development environment shall conform to EAL3 + ADV_FSP.2”, a set of SARs consisting of EAL3 and ADV_FSP.2 and a rationale “OD14 is directly achieved by the SARs”.

A.9.3.2 Security requirements: conclusion

318 In ASE_SPD the security problem is defined as consisting of threats, OSPs and assumptions. In ASE_OBJ the solution is provided in the form of three sub-solutions:

– security objectives for the TOE

– security objectives for the development environment

– security objectives for the operational environment

319 Additionally, a security objectives rationale is provided showing that if all security objectives are achieved, the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

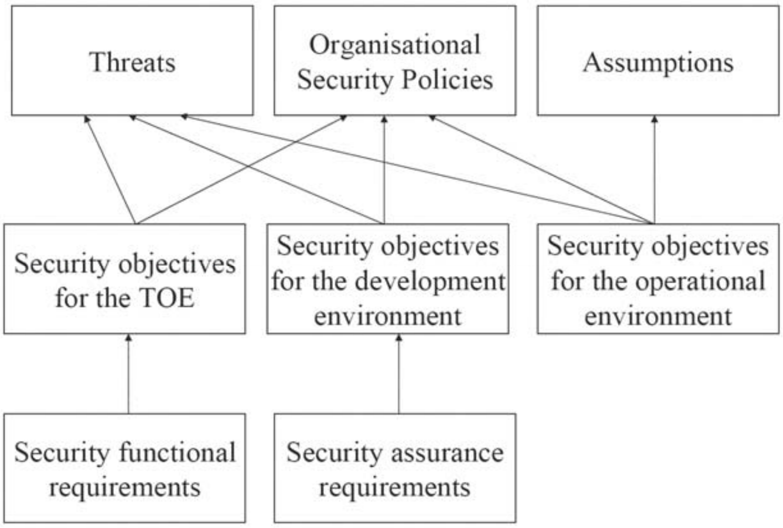
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the development environment
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure 14 - Relation between ASE_SPD, ASE_OBJ and ASE_REQ

320 In ASE_REQ a well-defined translation is provided of two of the sub-solutions from ASE_OBJ:

- the security objectives for the TOE are translated to SFRs
- the security objectives for the development environment are translated to SARs

321 Additionally, a security requirements rationale is provided showing that if all SFRs are satisfied, all security objectives for the TOE are achieved and if all SARs are satisfied, all security objectives for the development are achieved.

322 This can be combined into a single statement: If all SFRs and SARs are satisfied and all security objectives for the operational environment are achieved, then the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld. This is illustrated in Figure **14**.

A.9.3.3 Notes on tracing and rationales

323 Figure **14** shows that (through the security objectives) every SFR and SAR must be traced back through the security objectives into individual statements in the security problem definition. This tracing can be coarse or detailed depending on the chosen level of granularity in the security problem definition and the security objectives.

324 For example, if the SARs consist of EAL 4 + ADV_IMP.2, some possible options are:

- A single OSP “The TOE shall be evaluated at EAL 4 + ADV_IMP.2” leading to a single security objective for the development environment “The development environment shall comply with

EAL4 + ADV_IMP.2" and trace all SARs back to that single security objective.

- An OSP "The TOE shall be developed according to good commercial development practices applied rigorously", a threat "Threat Agent X obtains the source code by theft or reverse engineering, subverts the TOE and thereby is able to read the Confidential Data Asset", leading to two security objectives for the development environment "The development shall comply with EAL 4" and "The development environment shall have a thorough and complete source code level analysis performed" and tracing the EAL4 SARs to the EAL4 security objective and the ADV_IMP.2 SAR to the source code security objective.

- An extensive set of OSPs and threats relating to the development environment, leading to an extensive set of security objectives for the development environment and a detailed tracing of the SARs to these security objectives.

325 Similar examples apply to tracing of SFRs.

326 The choice of granularity is made by the ST author.

A.10 TOE summary specification (ASE_TSS)

327 The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies its SFRs. The TOE summary specification should provide the general technical mechanisms that the TOE uses for this purpose. The level of detail of this description should be enough to enable potential consumers to understand the general form and implementation of the TOE.

328 For instance if the TOE is an Internet PC and the SFRs contain FIA_UAU.2 User authentication before any action to specify authentication, the TOE summary specification should indicate how this authentication is done: password, token, iris scanning etc. More information, like applicable standards that the TOE uses to meet SFRs, or more detailed descriptions may also be provided.

329 The TOE summary specification may use the TOE description (to be provided as part of the ST introduction) as a general description of the TOE, and add specific descriptions of how each SFR is met to this general description. These specific descriptions may be separated from the TOE description, so as to ensure the readability and clarity of the TOE description.

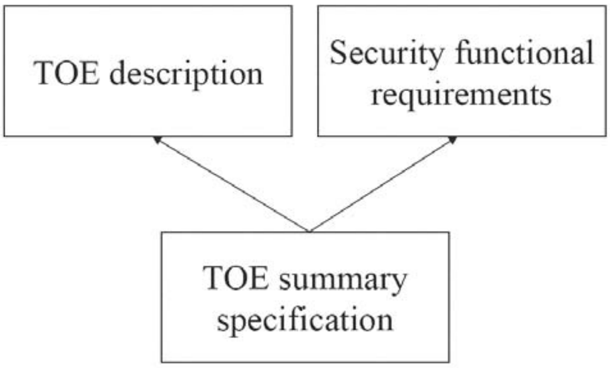

Figure 15 - Relation between ASE_INT, ASE_REQ and ASE_TSS

A.11 Questions that can be answered with an ST (informative)

330 After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST can therefore answer the following questions (and more):

a) *How can I find the ST/TOE that I need given the multitude of existing STs/TOEs?* This question is adressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

b) *Does this TOE fit in with my existing IT-infrastructure?* This question is addressed by the TOE overview, which identifies the major hardware/firmware/software elements needed to run the TOE;

c) *Does this TOE fit in with my existing operational environment?* This question is addressed by the security objectives for the operational environment, which identifies all constraints the TOE places on the operational environment in order to function;

d) *What does the TOE do (interested reader)?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

e) *What does the TOE do (potential consumer)?* This question is addressed by the TOE description, which gives a less brief (several pages) summary of the TOE;

f) *What does the TOE do (technical)?* This question is addressed by the TOE summary specification which provides a high-level description of the mechanisms the TOE uses;

g) *What does the TOE do (expert)?* This question is addressed by the SFRs which provide an abstract highly technical description, and the TOE summary specification which provide additional detail;

h) *Does the TOE address the problem as defined by my government/organisation?* If your government/organisation has defined packages and/or PPs to defines this solution, then the answer can be found in the Conformance Claims section of the ST, which lists all packages and PPs that the ST conforms to.

i) *Does the TOE address my security problem (expert)?* What are the threats countered by the TOE? What organisational security policies does it enforce? What assumptions does it make about the operational environment? These questions are addressed by the security problem definition;

j) *How much trust can I place in the TOE?* This can be found in the SARs, which provide the assurance level that was used to evaluate the TOE, and hence the trust that the evaluation provides in the correct functioning of the TOE.

A.12 Low assurance Security Targets

331 Writing an ST is not a trivial task, and may, especially in low assurance evaluations, be a major part of the total effort expended by developer and evaluator in the whole of the evaluation. For this reason, it is also possible to write a low assurance ST. There are two important difference between a “full” ST and a low assurance ST:

– Reduced content: a low assurance ST does not have to contain a security problem definition, a statement of security objectives, a security objectives rationale and a security requirements rationale;

– Reduced completeness: the SFRs and SARs in a low assurance ST do not have to meet their dependencies.

A.12.1 Reduced content

332 A low assurance ST has a strongly reduced content:

– there is no need to describe the threats, OSPs and assumptions that the TOE must counter, enforce and uphold

– there is no need to describe the security objectives for the TOE, the security objectives for the development environment and/or the security objectives for the operational environment

– there is no need to describe the rationale how the security objectives counter the threats, enforce the OSPs, and uphold the assumptions, as none of these entities are present in the ST

– there is no need to describe the rationale how the SFRs meet the security objectives for the TOE nor how the SARs meet the security objectives for the development environment, since the security objectives are not present in the ST.

333 All that remains are:

a) the references to TOE and ST

b) the conformance claim

c) the various narrative descriptions

1) the TOE overview

2) the TOE description

3) the TOE summary specification

d) the SFRs and the SARs (including the extended components definition).

334 The reduced content of a low assurance ST is shown in Figure **16**.

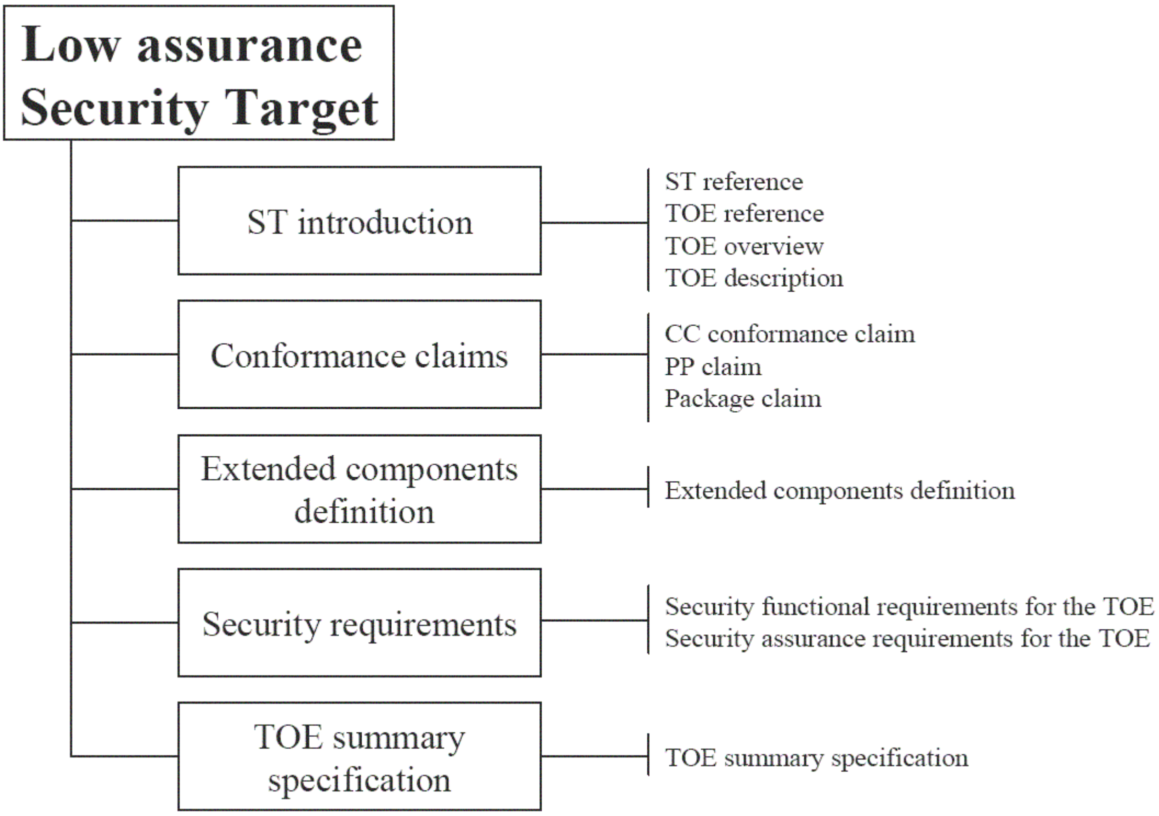
Low assurance Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
CC conformance claim
PP claim
Package claim
Extended components definition
Extended components definition
Security requirements
Security functional requirements for the TOE
Security assurance requirements for the TOE
TOE summary specification
TOE summary specification

Figure 16 - Low assurance ST contents

A.12.2 Reduced completeness

335 A low assurance ST has reduced requirements for completeness: it is no longer required to provide a rationale for not meeting a dependency. However, a low assurance ST writer may consider the dependencies while writing the ST to provide a good set of SFRs and SARs.

B Specification of Protection Profiles (normative)

B.1 Goal and structure of this Annex

336 The goal of this Annex is to explain the APE criteria and provide examples of their application. This Annex does not define the APE criteria, this definition can be found in CC Part 3.

337 As Protection Profiles and Security Targets have a significant overlap, this Annex focuses on the differences between Protection Profiles and Security Targets. The material that is identical between Security Targets and Protection Profiles is described in Annex A.

338 This annex consists of two major parts:

a) *What a PP must contain*. This is summarised in Section B.2, and described in more detail in clauses B.4-B.9. These sections describe the mandatory contents of the PP, the interrelationships between these contents, and provide examples.

b) *How a PP should be used*. This is summarised in Section B.3.

c) *Low Assurance PPs*. Low Assurance PPs are PPs with strongly reduced content. They are described in detail in Section B.11.

B.2 Mandatory contents of a PP

339 Figure **17** portrays the mandatory content for a PP. Figure **17** may also be used as a structural outline of the PP, though alternative structures are possible. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the PP instead of in the security requirements section. The separate sections of a PP and the contents of those sections are briefly summarised below and described in much more detail in Sections B.4 - B.9. A PP must contain:

a) a PP *introduction* containing a narrative description of the TOE;

b) a *conformance claim*, showing whether the PP claims conformance to any PPs and/or packages, and if so, to which PPs and/or packages;

c) a *security problem definition*, showing the threats, OSPs and assumptions that must be countered, enforced and upheld by the TOE and its operational environment;

d) *security objectives*, showing how the solution to the security problem is divided between:

- the TOE;

- the development environment of the TOE;
- the operational environment of the TOE;

e) *extended components definition*, where new components (i.e. not included in CC Part 2 or CC Part 3) may be defined. These new components can then be used to define extended functional and extended assurance requirements with.

f) *security requirements*, where a well-defined translation of the security objectives for the TOE and the security objectives for the development environment is provided. This well-defined translation is in the form of CC Part 2 requirements, CC Part 3 requirements and extended security requirements.

340 There also exists low assurance PPs which have reduced contents, these are described in detail in Section B.11. The rest of this Annex assumes that a PP with full contents is used.

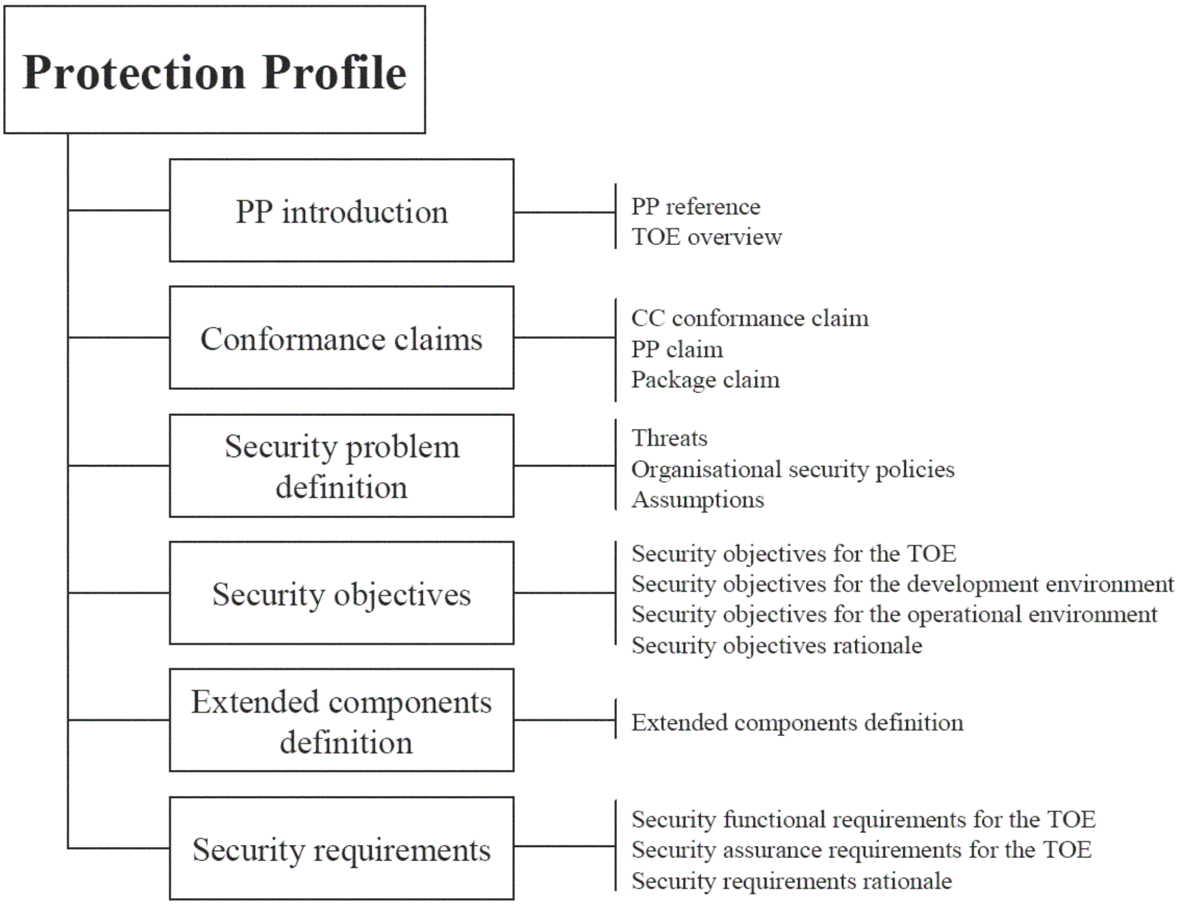
Protection Profile
PP introduction
PP reference
TOE overview
Conformance claims
CC conformance claim
PP claim
Package claim
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the development environment
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements for the TOE
Security assurance requirements for the TOE
Security requirements rationale

Figure 17 - Protection Profile contents

B.3 Using the PP (informative)

B.3.1 How a PP should be used

341 A PP is typically a statement of need where a user community, a regulatory entity, or a group of developers define a common set of security needs. A PP gives consumers a means of referring to this set, and facilitates future evaluation against this need.

342 Protection Profiles are therefore typically used as:

- part of a requirement specification for a specific consumer or group of consumers, who will only consider buying a specific type of IT if it meets the PP;
- part of a regulation from a specific regulatory entity, who will only allow a specific type of IT to be used it it meets the PP
- a baseline defined by a group of IT developers, who then agree that all IT that they produce of this type will meet this baseline.

though this does not preclude other uses.

B.3.2 How a PP should not be used

343 Three roles (among many) that a PP should not fulfill are:

- *a detailed specification*: A PP is designed to be a security specification on a relatively high level of abstraction. A PP should, in general, not contain detailed protocol specifications, detailed decriptions of algorithms and/or mechanisms, long description of detailed operations etc.
- *a complete specification*: A PP is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size and weight, required voltage etc. should not be part of a PP. This means that in general a PP is a part of a complete specification, but not a complete specification itself.
- *a specification of a single product*: A PP is designed to describe a certain type of IT, and not a single product. When only a single product is described, it is better to use a Security Target for this purpose.

B.4 PP introduction (APE_INT)

344 Where an ST introduction describes the TOE in a narrative way on three levels of abstraction:

a) the ST reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to;

b) the TOE overview, which briefly describes the TOE;

c) the TOE description, which describes the TOE in more detail.

345 a PP introduction consists of only

a) the PP reference;

b) the TOE overview.

B.4.1 PP reference

346 A PP contains a clear PP reference that identifies that particular PP. A typical PP reference consists of title, version, authors and publication date. An example of a PP reference is “Atlantean Navy CablePhone Encryptor PP, version 2b, Atlantean Navy Procurement Office, 4/7/03”. The reference must be unique so that it is possible to tell different PPs and different versions of the same PP apart.

347 The PP reference facilitates indexing and referencing the PP and its inclusion in lists of Protection Profile.

B.4.2 TOE overview

348 The TOE overview is aimed at potential consumers of a TOE who are looking through lists of evaluated products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware. The typical length of a TOE overview is several paragraphs.

349 To this end, the TOE overview briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware/software/firmware available to the TOE.

B.4.2.1 Usage and major security features of a TOE

350 The description of the usage and major security features of the TOE is intended to give a very general idea of what the TOE should be capable of, and what it can be used for.

351 An example of this is “The Atlantean Navy CablePhone Encryptor is an encryption device that should allow confidential communication between ships across the Atlantean Navy CablePhone system. To this end it should allow at least 32 different users and support at least 100Mb encryption speed. It should allow both bilateral communication between ships and broadcast across the entire network.”

B.4.2.2 TOE Type

352 The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smartcard, crypto-modem, intranet, web server, database, webserver and database, LAN, LAN with webserver and database, etc.

B.4.2.3 Available non-TOE hardware/software/firmware

353 While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify this non-TOE hardware/software/firmware.

354 It is not required to provide a complete and fully detailed identification of all this hardware/software/firmware, but the identification should be complete and detailed enough for potential consumers to determine the major hardware/software/firmware components needed to use the TOE.

355 Example hardware/software/firmware identifications are:

- a standard PC with a 1GHz or higher processor and 512MB or more RAM, running version 3.0 Update 6b, c, or 7, or version 4.0 of the Inux operating system;
- a standard PC with a 1GHz or higher processor and 512MB or more RAM, running version 3.0 Update 6d of the Inux operating system and the WonderMagic 1.0 Graphics card with the 1.0 WM Driver Set;
- a CleverCard SB2067 IC;
- a CleverCard SB2067 IC running v2.0 of the QuickOS smartcard operating system;
- the December 2002 installation of the LAN of the Director-General"s Office of the Department of Traffic.

B.5 Conformance claims (APE_CCL)

356 This section of a PP describes how the PP conforms with other PPs and with packages. It is identical to the conformance claims section for an ST (see Section A.5), with one exception: the conformance statement.

357 The conformance statement in the PP states how STs and/or other PPs must conform to that PP. The PP author can select whether "exact", "strict" or "demonstrable" conformance is required.

358 The authors of PP/STs that subsequently claim conformance must then comply with the PP according to that conformance statement.

B.6 Security problem definition (APE_SPD)

359 This section is identical to the security problem definition section of an ST as described in Section A.6.

B.7 Security objectives (APE_OBJ)

360 This section is identical to the security objectives section of an ST as described in Section A.7.

B.8 Extended components definition (APE_ECD)

361 This section is identical to the extended components section of an ST as described in Section A.8.

B.9 Security requirements (APE_REQ)

362 This section is identical to the security requirements section of an ST as described in Section A.9. Note however that the rules for completing operations in a PP are slightly different from the rules for completing operations in an ST. This is described in more detail in Section 4.3.1.3.2.

B.10 TOE summary specification

363 A PP has no TOE summary specification.

B.11 Low assurance Protection Profiles

364 A low assurance PP has the same relation to a regular PP, as a low assurance ST to a regular ST. This means that a low-assurance PP consists of

a) a PP introduction, consisting of a PP reference and a TOE overview, as per Section B.4

b) a conformance claim, as per Section B.5.

c) the SFRs and the SARs (including the extended components definition), as per Sections B.8 and B.9.

365 The reduced content of a PP for low assurance is shown in Figure **18**.

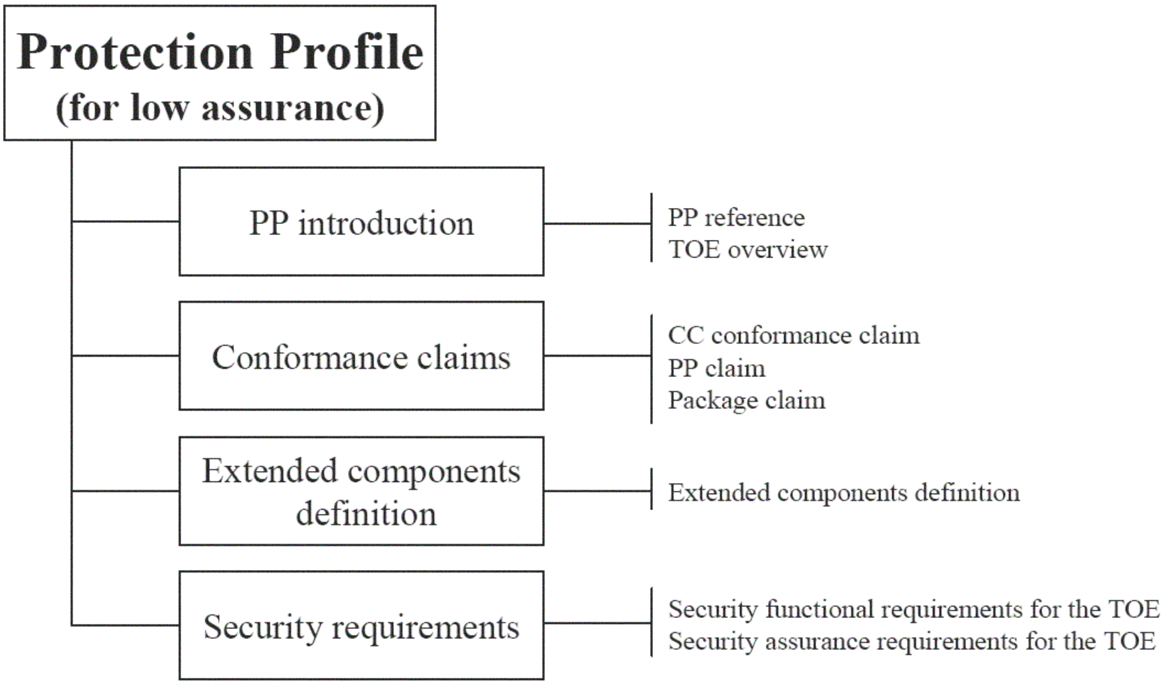

Figure 18 - Protection Profile for low assurance contents

366 A low assurance PP has similar reduced requirements for completeness as a low assurance ST (see Section A.12.2).

C Bibliography (informative)

BL Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

BIBA Biba, K. J., Integrity Considerations for Secure Computer Systems, ESD-TR-372, ESD/AFSC, Hanscom AFB, Bedford MA., April 1977.

CTCPEC Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993.

FC Federal Criteria for Information Technology Security, Draft Version 1.0, (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993.

GOGU1 Goguen, J. A. and Meseguer, J., “Security Policies and Security Models,” 1982 Symposium on Security and Privacy, pp.11-20, IEEE, April 1982.

GOGU2 Goguen, J. A. and Meseguer, J., “Unwinding and Inference Control,” 1984 Symposium on Security and Privacy, pp.75-85, IEEE, May 1984.

ITSEC Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991.

OSI ISO/IEC 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture.

TCSEC Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985.