
**Information technology — Security
techniques — Guide for the production of
Protection Profiles and Security Targets**

*Technologies de l'information — Techniques de sécurité — Guide pour
la production de profils de protection et de cibles de sécurité*



Reference number
ISO/IEC TR 15446:2009(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2009

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	vii
Introduction.....	viii
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Abbreviations.....	1
5 Purpose and structure of this technical report	2
6 An overview of PPs and STs	3
6.1 Introduction.....	3
6.2 Audience	3
6.3 The use of PPs and STs.....	3
6.3.1 Introduction.....	3
6.3.2 Specification-based purchasing processes	4
6.3.3 Selection-based purchasing processes.....	7
6.3.4 Other uses of PPs.....	8
6.4 The PP/ST development process.....	9
6.5 Reading and understanding PPs and STs.....	9
6.5.1 Introduction.....	9
6.5.2 Reading the TOE overview	10
6.5.3 Reading the TOE description	11
6.5.4 Security objectives for the operational environment	12
6.5.5 Reading the conformance claim	12
6.5.6 Conformance to Protection Profiles.....	13

6.5.7	EALs and other assurance issues	13
6.5.8	Summary.....	14
6.5.9	Further reading	15
7	Specifying the PP/ST introduction.....	15
8	Specifying conformance claims.....	15
9	Specifying the security problem definition.....	16
9.1	Introduction	16
9.2	Identifying the informal security requirement	18
9.2.1	Introduction	18
9.2.2	Sources of information	18
9.2.3	Documenting the informal requirement	20
9.3	How to identify and specify threats	21
9.3.1	Introduction	21
9.3.2	Deciding on a threat analysis methodology	21
9.3.3	Identifying participants	22
9.3.4	Applying the chosen threat analysis methodology	26
9.3.5	Practical advice.....	27
9.4	How to identify and specify policies.....	28
9.5	How to identify and specify assumptions.....	29
9.6	Finalising the security problem definition	31
10	Specifying the security objectives.....	32
10.1	Introduction	32
10.2	Structuring the threats, policies and assumptions.....	34
10.3	Identifying the non-IT operational environment objectives	34
10.4	Identifying the IT operational environment objectives	35
10.5	Identifying the TOE objectives	36
10.6	Producing the objectives rationale.....	39

11	Specifying extended component definitions.....	40
12	Specifying the security requirements	43
12.1	Introduction.....	43
12.2	The security paradigms in ISO/IEC 15408	45
12.2.1	Explanation of the security paradigms and their usage for modelling the security functionality	45
12.2.2	Controlling access to and use of resources and objects	45
12.2.3	User management	49
12.2.4	TOE self protection	50
12.2.5	Securing communication	51
12.2.6	Security audit.....	52
12.2.7	Architectural requirements	53
12.3	How to specify security functional requirements in a PP or ST.....	54
12.3.1	How should security functional requirements be selected?	54
12.3.2	Selecting SFRs from ISO/IEC 15408-2.....	57
12.3.3	How to perform operations on security functional requirements.....	59
12.3.4	How should the audit requirements be specified?	61
12.3.5	How should management requirements be specified?.....	62
12.3.6	How should SFRs taken from a PP be specified?	63
12.3.7	How should SFRs not in a PP be specified?	63
12.3.8	How should SFRs not included in Part 2 of ISO/IEC 15408 be specified?	64
12.3.9	How should the SFRs be presented?	64
12.3.10	How to develop the security requirements rationale.....	65
12.4	How to specify assurance requirements in a PP or ST.....	66
12.4.1	How should security assurance requirements be selected?	66
12.4.2	How to perform operations on security assurance requirements	67
12.4.3	How should SARs not included in Part 3 of ISO/IEC 15408 be specified in a PP or ST?	67
12.4.4	Security assurance requirements rationale	68
13	The TOE summary specification.....	68

14 Specifying PP/STs for composed and component TOEs.....69

14.1 Composed TOEs.....69

14.2 Component TOEs 72

15 Special cases 72

15.1 Low assurance Protection Profiles and Security Targets.....72

15.2 Conforming to national interpretations.....73

15.3 Functional and assurance packages 73

16 Use of automated tools 73

Annex A (informative) Example for the definition of an extended component.....75

Bibliography.....78

Index 79

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard (“state of the art”, for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 15446, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC TR 15446:2004), which has been technically revised.

Introduction

This Technical Report is an adjunct to ISO/IEC 15408 *Information technology — Security techniques — Evaluation criteria for IT security*. ISO/IEC 15408 introduces the concepts of *Protection Profiles* (PPs) and *Security Targets* (STs). A Protection Profile is an implementation-independent statement of security needs for a type of IT product that can then be evaluated against ISO/IEC 15408, whereas a Security Target is a statement of security needs for a specific ISO/IEC 15408 target of evaluation (TOE).

Unlike previous editions, the third edition of ISO/IEC 15408 provides a comprehensive explanation of what needs to go into a PP or ST. However, the third edition of ISO/IEC 15408 still does not provide any explanation or guidance of how to go about creating a PP or ST, or how to use a PP or ST in practice when specifying, designing or implementing secure systems.

This Technical Report is intended to fill that gap. It represents the collective experience over many years from leading experts in ISO/IEC 15408 evaluation and the development of secure IT products.

Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

1 Scope

This Technical Report provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408. It is also applicable to PPs and STs compliant with Common Criteria Version 3.1 [1], a technically identical standard published by the Common Criteria Management Board, a consortium of governmental organizations involved in IT security evaluation and certification.

This Technical Report is not intended as an introduction to evaluation using ISO/IEC 15408. Readers who seek such an introduction should read Part 1 of ISO/IEC 15408.

This Technical Report does not deal with associated tasks beyond PP and ST specifications such as PP registration and the handling of protected intellectual property.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:—¹⁾, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2008, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1:—¹⁾ apply.

4 Abbreviations

For the purposes of this document, the abbreviations given in ISO/IEC 15408-1:—¹⁾ and the following apply.

COTS Commercial Off The Shelf

1) To be published. Technical revision of ISO/IEC 15408-1:2005.

CRL	Certificate Revocation List
LDAP	Lightweight Directory Access Protocol
SPD	Security Problem Definition
SSL	Secure Sockets Layer
TLS	Transport Layer Security

5 Purpose and structure of this technical report

This Technical Report is intended to help people who have to prepare Protection Profiles (PPs) or Security Targets (STs) for use in evaluation against the third edition of ISO/IEC 15408. It provides detailed guidance relating to the various parts of a PP or ST, and how they interrelate.

This Technical Report applies only to the third edition of ISO/IEC 15408. Earlier versions of ISO/IEC 15408 have different and incompatible technical requirements. However, the strategies proposed in this Technical Report will, in the main, also be applicable to earlier versions of ISO/IEC 15408.

This Technical Report is primarily aimed at those who are involved in the development of PPs and STs. It will also be of interest to consumers and users of PPs and STs who wish to understand the contents of PPs and STs developed by others, and wish to confirm the relevance and accuracy of the information that they contain. It is also likely to be useful to evaluators of PPs and STs and to those who are responsible for monitoring PP and ST evaluation.

It is assumed that readers of this Technical Report are familiar with ISO/IEC 15408-1, and in particular Annexes A and B which describe STs and PPs respectively. PP and ST authors will (of course) need to become familiar with the other parts of ISO/IEC 15408 as described in this Report, including introductory material such as the functional requirements paradigm described in ISO/IEC 15408-2:2008, Clause 5.

This Technical Report is intended for guidance only. It should not be cited as a Standard on the content or structure for the evaluation of PPs and STs. It is intended to be fully consistent with ISO/IEC 15408; however, in the event of any inconsistency between this Technical Report and ISO/IEC 15408, the latter as a normative Standard takes precedence.

Clauses 1 to 4 contain introductory and reference material, and are followed by this overview clause (Clause 5).

Clause 6 provides an introduction to Protection Profiles and Security Targets – what they are, when and why they might be used. This clause also discusses the relationship between PPs and STs and issues relating to the PP/ST development process.

Clauses 7 to 13 provide information on how to specify the seven mandatory parts of the contents of a PP or ST, following the order outlined in ISO/IEC 15408-1:—, clauses A.2 and B.2.

Clause 14 examines the issues specific to PPs and STs for composed TOEs, i.e. TOEs that are composed of two or more component TOEs, each of which has its own PP or ST.

Clause 15 deals with some special cases, namely low assurance reduced PP/ST contents, conforming to national restrictions and interpretations and the use of functional and assurance packages.

Clause 16 discusses the topic of use of automated tools in PP/ST development.

6 An overview of PPs and STs

6.1 Introduction

This clause provides an overview of the roles of PPs and STs in information security evaluation using ISO/IEC 15408.

6.2 Audience

This Technical Report is intended for use by two distinct audiences:

- a) IT professionals with security knowledge (e.g. security officers/architects with an understanding of a security requirement) but who are not experts in information security evaluation, and who have no prior knowledge of ISO/IEC 15408;
- b) Experts in information security with good knowledge of ISO/IEC 15408, who are engaged in developing PPs and STs as part of their professional activities.

If you fall into the former category, this clause should provide you with the information you need to understand the purpose and structure of PPs and STs. It should also provide you with the background information you will need to read and understand PPs and STs, and to identify their relevance and correctness with respect to your particular circumstances. Following clauses will explain the contents of each part of PPs and STs in detail, but are oriented towards the production of such documents and assume knowledge of ISO/IEC 15408.

If you are an expert, you should already be familiar with the contents of this clause. Subsequent clauses will provide you with methodologies, techniques and practical tips that you can use to prepare PPs and STs in an efficient yet consistent manner.

If you are not an expert in information security, and you need to produce a PP or ST, this Technical Report will help you do so. However, you will also need to find, read and understand published examples of PPs or STs similar to your requirement. You should also consider calling on the services of others who *do* have the necessary specialist knowledge and experience.

6.3 The use of PPs and STs

6.3.1 Introduction

The main use of ISO/IEC 15408 is to assess the security of IT products. The term “IT product” is never actually defined in ISO/IEC 15408; however, it can be understood to cover any type of entity built using information technology, whether a complete IT system used exclusively by one organisation, or a COTS package created by a product manufacturer for sale to many different and unrelated customers. In this Technical Report, when we talk about IT products, or just products, our advice is intended to apply to all such entities. Where the scope of our advice is limited to a particular type of product, we talk about systems, or COTS products, or some other explicitly specific wording.

As IT products may be used in many ways, and in many types of environment, the notion of security will vary with the product. The end result of an ISO/IEC 15408 evaluation is therefore never “this IT product is secure”, but is always “this IT product meets this security specification”.

ISO/IEC 15408 has standardised security specifications to (among others):

- mandate specific content needed to assess a product against the security specification;
- allow comparison of security specifications of different products.

ISO/IEC 15408 recognises two different types of security specifications: Protection Profiles (PPs) and Security Targets (STs). The difference between these two is best explained by the roles they are intended to play in a typical product purchasing process, where a customer seeks to buy a product from a developer.

The notions of customer, developer and product are deliberately kept abstract. A customer is someone who wants to buy a product. It can be a single individual, an organization, a group of organizations, a government department etc. A developer is someone who wants to sell a product. It can be a single programmer, a small company, a large company, a group of companies working together etc. Finally, a product could be anything from a small software application or a smart card to a large operating system or a complete computer system containing hundreds of distinct components.

When our customer wishes to buy a product, he has essentially two possibilities:

- The customer contacts a developer, specifies his needs, and the developer creates a product that is specifically targeted towards that customer and exactly fulfils the demands of that customer. This may be expensive but the customer gets what he wants. In the remainder of this section, we will call this a specification-based purchasing process.
- The customer selects a product from a number of existing products. This is probably cheaper, but the resulting product may or may not exactly fulfil the customer's needs. In the remainder of this section we will call this a selection-based purchasing process.

When IT security is important, these purchasing processes have an added difficulty. For the average customer it is:

- hard to define what kind of IT security he needs;
- harder to determine whether the IT security that a given product claims to have is useful or sufficient to meet his needs;
- and even harder to determine that if a product claims to have security properties, that these claims are true.

To assist a customer through a purchasing process and address the difficulties listed above, an evaluation of the product using ISO/IEC 15408 may be useful, and in this case, Protection Profiles and Security Targets play an important role. In the next two subsections, we will show how an evaluation may assist each type of process: specification-based and selection-based.

Of course, IT products do not work in isolation. The product is used by the customer in an operational environment, which may contain security measures of its own. Sometimes the product will make assumptions that certain types of security features exist within that operational environment. These assumptions will also form part of the PP or ST.

6.3.2 Specification-based purchasing processes

6.3.2.1 Overview

In a specification-based purchasing process, a customer writes a specification, provides this specification to a developer, and the developer then creates a product based on this specification. In more detail, the following steps must be performed:

- a) The customer must determine his security requirements informally;
- b) The customer must transform these informal security requirements into a more formal specification suitable for use by a developer;
- c) The developer must build a product based on this specification.

In the end, the customer wants to know that “this product is useful for me”. Therefore the quality of each of these steps is important.

6.3.2.2 Informal security requirements

The process of determining informal security requirements, that is determining “what is my security problem, and how should I address it?” is outside the scope of ISO/IEC 15408 and therefore outside the scope of this Technical Report. However, this does not mean that this is unimportant or easy by any means.

Nevertheless, ISO/IEC 15408 assumes that the customer is capable of defining his or her informal security requirements. If this is done incorrectly, the product that is purchased in the end may not meet the true security requirements.

Customer requirements, once written down, often have a number of problems associated with them, especially in the area of security. Customer requirements are typically:

- a) Incomplete (not all the requirements are present). For example, important threats that the product should counter are missing;
- b) Not embedded: They are insufficiently tuned to the specific environment in which the product has to function, or do not describe this environment clearly enough.
- c) Implicit: Some product requirements have consequences, but these consequences are themselves not included. The developer may not take these implicit requirements into account;
- d) Not testable: The requirements are phrased ambiguously, so that it is not possible to verify whether a product meets the requirement or not;
- e) Too detailed: The implementation has in fact already been written down but not the reason why this was chosen. If, in a later stage, the requirements change it is often unclear how these changes should be made;
- f) Filled with ambiguous terms: like “the communication shall be secure” without defining what “secure” means;
- g) Inconsistent: The requirements are internally self-contradictory.

Providing these customer requirements to a developer in a raw form will generally lead to problems, as the developer may misunderstand them. Security evaluation may lead to even more problems, since evaluators may interpret requirements differently from both the customer and the developer.

For these reasons, an important step in the whole specification-based purchasing process is the formalising of customer requirements. For security requirements based on ISO/IEC 15408, this formalisation takes place using a so-called Protection Profile (PP). A PP is in essence a document that defines the customer’s security requirements in a formalised, standardised way.

6.3.2.3 Using PPs as specifications

PPs are typically written by large organizations, groups of organizations, government departments, etc. as they require a significant investment of effort.

A PP contains many sections, but as a security specification, the most important is the “security functional requirements”. Using ISO/IEC 15408, it is mandatory to write these requirements in a special language, defined within that International Standard. Use of this language ensures that the Protection Profile is:

- a) not ambiguous: the language contains well defined terms, so that a developer can understand the requirements and interpret them correctly.

- b) testable: the language is defined to contain only testable terms. Thus, it will be possible to assess in a later stage whether the product actually fulfils the PP.
- c) not too detailed: the language enforces a certain level of abstraction. This closely follows what should be the consumer requirements: the consumer wants something to be done but does not want to worry how this is accomplished.
- d) more complete: the language contains several constructions ("if this functionality is required then this other functionality is also required") to help ensure that implicit requirements are included.

6.3.2.4 Building a product from a PP

The customer can now give the PP, i.e. his formalised requirements, to one or more developers. Each developer uses this PP as a starting point for the development of a product. As a first step in this process he writes a Security Target (ST).

An ST used for this purpose is very similar to a PP, but where a PP defines the customer requirements and is in principle written by the customer, the ST is a product specification and written by the developer.

The developer can of course not deliver an arbitrary ST as a reaction to the customer's PP: his ST has to *conform* to the PP. This means that the product has to cover all the customer requirements, but:

- The ST may specify more than the PP: the product will offer more security functionality than the customer requirements (note: this extra functionality is not allowed to be incompatible with the PP), because, for example, the product will be sold to several customers, each with similar but slightly different requirements, or because the product is derived from an existing, standard product.
- The ST contains more detail than the PP: while the PP explains "what" shall be secured, the ST also explains "how": the developer points out, in general terms, how he will implement the customer requirements.

A PP may permit the ST author flexibility to offer something that is equivalent but different in terms of security functionality provided – for more details, see 6.5.6.

The ST defines for the developer the security functionality his product should deliver and serves as a "Specification of Security Requirements" for the rest of the development process.

The result of the development process should be a product that can be delivered to the customer, who in turn can install it and use it. Naturally, this product should perform as described in the ST.

6.3.2.5 The role of evaluation in a specification-based purchasing process

Until now, we have only described the role of the customer and the role of the developer in this process. Based on this process, the developer could simply say to the customer (without further evidence):

- a) my ST complies with your PP;
- b) my product complies with my ST;
- c) therefore, my product complies with your PP and meets your requirements.

If the customer accepts these statements, the process ends here.

However, if a customer requires independent verification of these statements, he can enlist a third party (an evaluation facility) to check these claims of compliance by performing an ISO/IEC 15408 security evaluation. In this process, an evaluation facility uses the PP, the ST, the product and ISO/IEC 15408 to assess two statements:

- a) the ST complies with the PP;
- b) the product complies with the ST.

Note that two issues are still left open, despite evaluation.

- a) *The translation of the customer's informal security requirements to a Protection Profile.* As said earlier, this process falls outside the scope of ISO/IEC 15408, but if this is not done correctly, the PP will not match the customer's requirements and therefore the product will likely also not match the customer's requirements.
- b) *Evaluation does not "prove" compliance.* An ISO/IEC 15408 evaluation will never provide an absolute guarantee that the product meets the PP, it can only deliver a certain degree of assurance depending on the depth and scope of evaluation as specified in the PP or ST.

6.3.3 Selection-based purchasing processes

6.3.3.1 Overview

The previous subsection discussed a customer delivering a specification and a developer implementing that specification. This subsection discusses the situation where a customer does not have the luxury of having a product made for him: he has to select from existing products. Therefore the purchase is no longer based on compliance to a formalised statement of customer requirements (i.e. a PP), but on comparison of existing products by the customer.

In a selection-based purchasing process of an IT product:

- a) a developer must produce a product and a specification of this product and provide the specification to the customer.
- b) the customer must determine from the specification (perhaps by comparing the specification to specifications from other developers) whether the specified product is the most suitable product for him to purchase.

As the customer in the end wants to know that "this product is suitable for me", the quality of each of these steps is important.

6.3.3.2 Using a specification provided by the developer

In selection-based purchasing processes, the customer has to use a specification provided by the developer.

If this specification is informal, the same potential disadvantages hold as for the informal customer requirements discussed in 6.3.2.2. For this reason, this specification needs to be formalised as well. For this purpose ISO/IEC 15408 uses the Security Target (ST) as already discussed in 6.3.2.4. The ST here is identical to the ST discussed in 6.3.2.4, with one obvious difference: since it is not based on a customer's PP, it cannot claim compliance to such a PP (it may claim compliance to other types of PP – see 6.3.4 below).

Because the developer does not know a specific customer's requirements, he will have to make an estimate of what the market wants and codify this in the ST. This does therefore not necessarily match with any customer's specific requirements.

The developer builds his product according to the ST: this process is similar to that described for specification-based purchasing processes.

6.3.3.3 Comparing Security Targets by the developer

The customer can now compare the STs of a number of products and select the one that best matches his requirements (probably also considering non-security requirements such as price). This means that he will still somehow have to find out what his informal security requirements are (see 6.3.2.2) and compare these with the STs offered to him. If one or more products match his requirements, he is done. If this is not the case, he will either have to choose the “closest” product or find some other solution (i.e. change his requirements).

As already stated in 6.3.2, the process of deriving informal customer security requirements falls outside the scope of ISO/IEC 15408 and this Technical Report. Comparing requirements and an ST also falls outside the scope of ISO/IEC 15408, although guidance on this topic will be found in later clauses of this Technical Report.

6.3.3.4 The role of evaluation in a selection-based purchasing process

Similar to the specification-based purchase process, the developer could simply claim that his product meets the ST and if the customer accepts this claim, the process ends here.

However, it is customary for the developer to offer a certificate confirming that an independent third party (an evaluation facility) has validated the ST, and then performed an ISO/IEC 15408 security evaluation to confirm that the product indeed meets the ST. It is even possible for the customer to commission the evaluation if he or she believes it to be essential and the developer has not done so.

Note that using evaluated products still leaves two issues open:

- a) *Proving equivalence of the customer's informal security requirements and the Security Target.* As said earlier, this process falls outside the scope of ISO/IEC 15408, but if it is not done correctly, the ST may not match the customer's requirements, and therefore the product may not match the customer's requirements either.
- b) *Evaluation does not “prove” compliance.* A ISO/IEC 15408 evaluation will never provide a perfect guarantee that the product meets the ST, it can only deliver a certain degree of assurance depending on the depth and scope of evaluation as specified in the ST.

6.3.4 Other uses of PPs

Protection Profiles have other uses. For example, standards bodies or vendor associations may specify PPs as best practice minimum security standards for specific types of applications. Governments and trade associations may mandate their use. Where these exist, both customers and developers are likely to require compliance with such PPs, as well as requiring or offering additional security functionality to meet their own specific needs.

Organisations specifying or mandating PPs for such purposes have an onerous responsibility to ensure that such PPs are minimal (they ask for no more than is absolutely necessary) and realistic (they do not ask for functionality or assurances that are not achievable by developers).

A PP may also be developed to express the need for a certain type of security product, even though it is recognised that at the time of publication, no such products (yet) exist. If you are a product developer, treat such PPs with caution. By the time you have developed a suitable product, the requirement may be obsolete or the sponsors of the PP may no longer want to buy your product because they have found other ways to meet their requirements.

Finally, PPs are *security* requirement specifications. Beware of their attempted misuse to specify other types of requirements which, if made more explicitly, would be rejected.

6.4 The PP/ST development process

The order of presentation of the requirements for PPs and STs in Annexes A and B of ISO/IEC 15408-1, and in earlier parts of this clause, might suggest that it is expected that PPs and STs are always developed in a logical 'top-down' manner, e.g. (in the case of an ST) that:

- a) the security problem is first defined;
- b) the security objectives are then identified to address the security problem;
- c) security requirements are then defined to satisfy the security objectives for the TOE;
- d) actual security functions are then selected to satisfy the security requirements.

Whilst such a possibility is not ruled out, it is more likely that an iterative process will be required. For example, definition of security requirements may highlight clarifications needed to the definition of the security objectives, or even the security problem. In general, a number of iterations may be required in which the relationships between threats, organisational security policies, security objectives and security requirements and functions are examined closely, particularly when rationales are being constructed. Only when all identified gaps in the rationales are filled may it be assumed that the PP or ST is complete.

During an iterative process of PP or ST development new information might surface, within the scope of the current security problem, that may lead changes to the document that reflect changes in external circumstances, for example:

- a) new threats may be identified;
- b) organisational security policies may change;
- c) cost and time constraints may impose changes in division of responsibility between what the TOE is expected to do, and what is expected of the TOE environment;
- d) changes in intended attack potential may impact on the TOE security problem definition.

It is also possible (particularly if the TOE is a product which has already been developed) that the PP or ST author already has a clear idea of the security functionality the TOE will provide (even if this has not yet been expressed as ISO/IEC 15408 security functional requirements). In such cases the definition of the security concerns and security objectives will unavoidably be influenced by the knowledge of the form of the security solution the TOE provides. The PP/ST development process will in those cases be, to some extent, 'bottom-up'.

6.5 Reading and understanding PPs and STs

6.5.1 Introduction

This section is *not* intended for experts with prior knowledge of ISO/IEC 15408. It is intended for that part of the audience for this Technical Report that know very little about PPs or STs but who need to read one or more PPs or STs in order to understand the security capabilities of the related products. It is intended to highlight where potential omissions or deficiencies may be concealed, particularly in the scope of evaluation.

For detailed understanding of the contents of PPs and STs there is no substitute for reading ISO/IEC 15408-1, in particular Annexes A and B which provide details concerning Security Targets and Protection Profiles respectively. It is also a good idea to look at other PPs and STs that have been published and are in general use. There are a number of *registries* from which you can download these. The Common Criteria Portal includes the largest [2]. This register is recognised by the ISO and IEC councils as the official JTC 1 register

for Protection Profiles and packages constructed in accordance with ISO/IEC 15408. It is operated in accordance with the relevant International Standard, ISO/IEC 15292 [3].

Unfortunately, a PP or ST cannot be summarised into a single number or a set of simple properties: PPs and STs describe a complex set of security properties that, if not carefully read, may lead to surprises when purchasing or using the product. On the other hand, some sections in a PP or ST (notably the security functional requirements) are equally or more important, but almost impossible to understand without an in-depth knowledge of ISO/IEC 15408. In the following subsections, we therefore identify the key sections of a PP or ST for the novice reader: sections that are relatively easy to understand, but that contain key information to understanding the security properties of a requirement expressed as a PP or a product described by an ST.

These relevant and readable sections are:

- a) the TOE overview;
- b) the TOE description;
- c) the security objectives for the operational environment;
- d) the conformance claim.

In the subsections following we will discuss each of these in more detail.

6.5.2 Reading the TOE overview

The TOE overview is in general the first thing you should read in a PP or ST, as it “is aimed at potential consumers of a TOE who are looking through lists of evaluated TOEs/Products to find TOEs that may meet their security needs, and are supported by their hardware, software and firmware” (ISO/IEC 15408-1:—, subclause A.4.2). The TOE overview contains three sections of interest:

- a) Usage and major security features of the TOE;
- b) The TOE type;
- c) Required non-TOE hardware/software/firmware.

We will now discuss each of these in turn. You will find some simple examples of each in ISO/IEC 15408-1:—, subclause A.4.2.

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 in terms of security, and what it can be used for in a security context.

This section should be fairly short (several paragraphs) so it should not require much effort to read and understand. And, as it should be aimed at consumers, it should not be highly technical. It is intended to be general, so it will not be exhaustive.

The TOE type is a description of the general category of IT products the TOE belongs to (e.g. firewall, smart cards, intranet, LAN etc.). ISO/IEC 15408 mandates that the TOE overview lists any reasonable expectations that a reader may have from this TOE type but that are not supported by the TOE. Specifically:

- a) If the TOE-type would lead you to believe that the TOE has certain security functionality and it does not have this functionality, the TOE overview must list this missing functionality.
- b) If the TOE-type would lead you to believe that the TOE could be used in a certain environment and it can not be used in such an environment, the TOE overview must list this.

Note that this is the only place in a PP or ST where these warnings are required to appear. The writer of the PP or ST may repeat this information in appropriate places later on by means of notes, but is not required to do so.

If these warnings are provided and possibly impact upon your intended use, you should seriously consider whether you can still use this TOE with these limitations.

The TOE, especially when it is a software type TOE, will sometimes have to rely on hardware and possibly firmware and other software components just to be able to execute. If this is the case, the TOE overview is required to identify this non-TOE hardware/software/firmware.

The PP or ST does not have to provide a complete and fully detailed identification of all this hardware/software/firmware, but the identification should be complete and detailed enough for you to determine the major external hardware/software/firmware components needed to use the TOE.

You should carefully assess whether there are any non-standard components on which the TOE relies and whether these components fit in with your existing infrastructure, budgets, company policies etc.

6.5.3 Reading the TOE description

An important thing to understand about ISO/IEC 15408 evaluations, is that if you read that well-known product XYZ has been evaluated, this does not mean that all security features (or even a majority of security features) of this product have been evaluated. It may well be the case that only some of its security functional features have actually been looked at and the remaining ones were not considered part of the evaluated security functionality. ISO/IEC 15408-1:—, subclause A.4.1 prohibits misleading TOE references, but developers can always get around this by just using a product name. You need to check that the evaluated functionality meets your needs. If some of the security functionality you intend to use was excluded, you need to ask yourself why.

One of the most important roles of the TOE description is to allow the ST reader to find this out. To this end the TOE description discusses the physical and logical scope of the TOE in detail.

Starting with the physical scope, ISO/IEC 15408 tells us that “The TOE description discusses the physical scope of the TOE: a list of all hardware, firmware, software and guidance parts that constitute the TOE. This list should be described at a level of detail that is sufficient to give the reader a general understanding of those parts” (quotation from ISO/IEC 15408-1:—, subclause A.4.3).

You should briefly examine this list to see if you see anything odd in it that you would not expect, or whether some parts of the product that you might expect to find present are missing. If something is not in this list, then the evaluation has completely ignored it and assumed it did not exist. If you intend to use that part, then you can draw no conclusions about its security capabilities from the evaluation.

With regards to logical scope, ISO/IEC 15408 tells us that “The TOE description should also discuss the logical scope 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. This description is expected to be in more detail than the major security features described in the TOE overview” (quotation from ISO/IEC 15408-1:—, subclause A.4.3).

Whereas the physical scope tells us the list of parts of the TOE, the logical scope should tell us what the TOE does. This was already briefly discussed in the Usage and Major Security features section (see 6.5.2) but where that discussion was only a few paragraphs, this discussion is more likely to be a few pages. The most important feature of this section is that if you expect the product to have a certain feature such as remote management (e.g. because an advertisement of the product in a trade magazine describes that feature) but the logical scope does not mention remote management, it may well be that remote management was not evaluated, and hence, remote management should not be turned on if you want to use the product in its evaluated configuration.

It is therefore important to scrutinise this section to determine whether all security-related features that you require were actually evaluated. If they are not, you will have no assurance in the operation of that feature from evaluation.

6.5.4 Security objectives for the operational environment

The operational environment is the general location that the TOE will be placed in. In order for the TOE to work correctly, this operational environment must meet certain constraints. For example, if a TOE is a high-availability server, this TOE needs to be protected against people accessing it with a screwdriver. This protection could be provided by the TOE (although tamper-proof servers are pretty rare), so in general the operational environment should address this, by specifying a requirement for a locked secure server room.

These and similar requirements for the operational environment are described in a PP or ST in the security objectives for the operational environment section. These objectives describe the things that must be achieved by everything except the TOE in order for the TOE to meet its security requirements. You will find a number of example of security objectives for the operational environment in ISO/IEC 15408-1:—, subclause A.7.2.2.

It is of vital importance to realize that these are not guidelines, but necessary conditions for the TOE to operate as stated. All of these objectives must be fully met and addressed by you or your organisation: the TOE will not do it for you. If a single one of these objectives is not met, the TOE might not function securely. It is therefore imperative that you determine whether they are achievable in your organisation, and if one of them is not achievable, the TOE may not be suitable for you.

6.5.5 Reading the conformance claim

The conformance claim is usually found in a prominent place in the PP or ST, usually somewhere up front. It usually consists of a single sentence of the form:

This Protection Profile/Security Target claims conformance to:

- the third edition of ISO/IEC 15408. This part of the claim represents the version of ISO/IEC 15408 that is used. If this is not the third edition or higher (or the Common Criteria equivalent V3.1 or higher), the PP/ST will not match the specifications in this Technical Report, and this Technical Report is not directly applicable. Although not all parts of the third edition of ISO/IEC 15408 were published in 2008, it will often, if incorrectly, be referred to as "ISO/IEC 15408:2008".
- Part 2 extended or Part 2 conformant. This part of the claim defines how security functional requirements are constructed, and from a consumer point of view, both are acceptable.
- Part 3 extended or Part 3 conformant. This part of the claim defines how security assurance requirements are constructed. If the answer is "Part 3 extended", the developer of the PP and ST has designed their own assurance tests, and from a consumer point of view, you should question why this was necessary.
- a list of packages that the TOE claims conformance with. Usually there is only one such package and it is named EAL1, EAL2, ..., EAL7, often followed by "augmented". These EALs are discussed further in 6.5.7. It is rare to find any other type of package specified and from a consumer point of view, you should again question why this was necessary.
- a list of Protection Profiles that the PP or ST claims conformance with. This is discussed further in 6.5.6 below.

6.5.6 Conformance to Protection Profiles

As already described in 6.3.2.4, STs can claim conformance to PPs (but do not have to do so). Also, PPs can claim conformance to other PPs. If they do claim conformance, this is listed here. ISO/IEC 15408 does not allow any form of partial conformance, so if a PP is listed here, the PP or ST must fully conform to the referenced PP or PPs.

Conformance to a PP means that the PP or ST (and if an ST is of an evaluated product, the product as well) meets all requirements of that PP.

If you are reading a PP, you will also find a statement that STs and other PPs must conform in a way that is either “strict conformance” or “demonstrable conformance”. Published PPs will normally require demonstrable conformance. This means that STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP. “Equivalent but more restrictive” is defined at length within ISO/IEC 15408, but in principle it means that the PP and ST may contain entirely different statements that discuss different entities, use different concepts etc., provided that overall the ST levies the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

Strict conformance is only used where no differences are permitted between PP and ST, e.g. in selection based purchasing (see 6.3.3 above). Of course, an ST can still introduce additional restrictions if it wishes to do so. If a PP demands strict conformance, and you or your organisation did not write it, it is highly unlikely to be suitable for your use.

6.5.7 EALs and other assurance issues

The TOE overview and TOE description will tell you what the TOE is capable of doing, i.e. the functionality that is provided by the TOE. However, functionality does not say everything about a IT product. Products with the same general functionality can be used in different settings. For example, the same smart card design can be used as:

- a bus ticket with a small amount of “travel budget” on it;
- a credit card with a €10.000 credit limit;
- an access control measure for access to a top secret military facility.

In the first case, one is happy with a “low-quality” smart card. If a hacker manages to break the bus ticket, he may be able to get free bus rides until the card parameters change. The loss of potential revenue (provided that other cards are not hacked in the same way) is not significant to the bus company.

In the second case, and certainly in the third case, we need much more confidence in the correct implementation of the card functionality, as the consequences of breaking even one card may be significant.

In ISO/IEC 15408, this quality is called “assurance”. ISO/IEC 15408 measures assurance by examining many aspects of the development of the product, such as the development and production process, the designs, the manuals, the amount of testing done by the developer of the product etc.

ISO/IEC 15408 formalises assurance into 27 categories (the so-called assurance families). In each category, ISO/IEC 15408 specifies different levels of conformance, where meeting a higher level is better.

As an example, a product could score in the category developer test coverage:

- 0: it is not known whether the developer has performed tests on the product;
- 1: the developer has performed some tests on some interfaces of the product;

- 2: the developer has performed some tests on all interfaces of the product;
- 3: the developer has performed a very large amount of tests on all interfaces of the product.

It can be seen from that this example that the degree of effort expended increases with each level, and the degree of uncertainty decreases.

Unfortunately it is almost impossible for a non-expert to interpret a scorecard consisting of individual ratings for all 27 subcategories. To allow non-experts to assess assurance, ISO/IEC 15408 has 7 predefined ratings, called Evaluation Assurance Levels (EALs). These are called EAL 1 to EAL 7, with EAL 1 the lowest and EAL 7 the highest.

Each EAL can be thought of as a set of 27 numbers, one for each subcategory. For instance, EAL1 assigns a rating of 1 to 13 of the subcategories, and 0 to the other 14 subcategories, while EAL2 assigns the rating 2 to 7 subcategories, the rating 1 to 11 subcategories, and 0 to the other 9.

The EALs are strictly hierarchical, so that if EAL n assigns a certain rating to a certain subcategory, then EAL $n+1$ will assign the same or a higher rating to that subcategory. So EAL $n+1$ provides strictly more assurance than EAL n overall.

The drawback of higher assurance is of course cost. In the test coverage area described earlier, a rating of 0 will mean no cost, but for each higher rating, the developer will have to perform and document the tests that are being done, the evaluator will have to determine if the developer did this correctly and document this, etc. More assurance almost always means more cost. Of course, more assurance also reduces the risk that the claimed functionality does not work correctly or contains exploitable vulnerabilities.

A listing of each EAL, together with a description of that EAL and a characterisation of the assurance that that EAL provides can be found in ISO/IEC 15408-3:2008, Clause 8.

EALs are a broad-brush mechanism, and are more suitable for assessing some types of product than others. Nevertheless, the EALs are currently the only widely accepted way to provide a characterisation of ISO/IEC 15408 assurance that a relative layman can understand.

6.5.8 Summary

In summary, this section was intended to convey two things:

- (obviously) that an ST can be reasonably understood from reading a number of sections; but also
- (less obviously) that these sections may contain important caveats and are therefore vital to understanding the limitations of the evaluation.

In the past there have been cases where consumers have stated that they wanted an EAL4 firewall or whatever. Hopefully, this section has conveyed that a ISO/IEC 15408-certified EAL4 firewall may have limitations that make it totally unusable for you, and may not provide all the relevant security you need.

For example, suppose you need both packet routing and HTTP/FTP proxy services from your firewall. A router may have a TOE type of firewall, and have been evaluated at EAL4. But as a router, it will only offer packet routing controls. Worse, if you find an evaluated firewall that offers proxy services but the logical scope is limited to packet routing, you must ask yourself why.

Even a big standard like ISO/IEC 15408 is not a substitute for thinking, and complex matters like IT security cannot be reduced to one sentence descriptions, no matter how hard you try.

6.5.9 Further reading

The sections of the PP or ST described above are the most basic sections of the PP and ST, and the most useful to be read by relative laymen. If you want to know more about the product, you could also try reading the TOE summary specification, which is intended to provide more detail on how the TOE is implemented. This section does not have to be easily readable. It may be filled with unexplained abbreviations like FIA_UID.2.1. However, many developers will take great pride in producing a TOE summary specification that meets the requirements of the evaluators but can still be readily understood by users of the product.

If you need to understand other sections of a PP or ST, then the following clauses of this Technical Report may help you. Whilst they are designed to be used by experts to specify PPs and STs, the information should also help you to understand the relevant contents.

7 Specifying the PP/ST introduction

This clause provides guidance on the specification of the PP/ST introduction section of a PP or ST. These are described at length in ISO/IEC 15408-1:—, clauses A.4 and B.4, and therefore little additional guidance is necessary in this Technical Report.

The introduction of a PP consists of the following elements:

- a PP reference;
- a TOE overview.

The introduction of an ST consists of the following elements:

- ST and TOE references
- a TOE overview;
- a TOE description.

The only non-obvious part is the “usage and major security features of the TOE” section of the TOE overview. Usage is often best derived by summarising the security problem definition section of the PP or ST (see Clause 9 for details), whilst the major security features are best described by summarising the security objectives for the TOE. This will ensure that the introduction is consistent with the more detailed parts of the PP or ST.

As with most introductions, you will probably find it easiest if you leave it until the rest of the PP or ST is complete and write it last!

8 Specifying conformance claims

This clause provides guidance on the specification of the conformance claims section of a PP or ST. ST conformance claims are described in ISO/IEC 15408-1:—, Clause A.5, and the differences applicable to conformance claims in PP in ISO/IEC 15408-1:—, Clause B.5.

The Conformance Claims section of a PP or ST describes how the PP or ST conforms to:

- a) *ISO/IEC 15408*. This consists of listing the exact version of ISO/IEC 15408 that was used to write (and presumably also to evaluate) the PP or ST. If an unofficial translation of ISO/IEC 15408 into some language other than English was used, this should also be indicated. If any corrigenda, or CC interpretations or supporting documents were used, these should be listed as well.

- b) *Protection Profiles*. This consists of listing any Protection Profiles that this PP or ST claims conformance to. A simple list is sufficient: no extra information is needed in this section.
- c) *Packages*. This consists of listing any packages that are referenced by the PP or ST. It is normal to claim conformance to one of the assurance packages (EALs) defined in ISO/IEC 15408-3, possibly with augmentations. Use of packages is discussed further in 15.3. Again: a simple list suffices: no extra information is needed in this section.

Of course, this conformance also applies to any TOE based on that PP or ST.

If you are specifying a PP, you must define how other PPs and STs conform to your PP. There are two choices for this:

- a) *Strict*. Conceptually, this means that conforming PPs/STs must contain everything in this PP. See ISO/IEC 15408-1:—, subclause 8.3 for the precise requirements.
- b) *Demonstrable*. Conceptually, this means that conforming PPs/STs must be “equivalent” to this PP. Again, please see ISO/IEC 15408-1:—, subclause 8.3 for the precise requirements.

As a guideline, if you are writing a PP as the precise and complete specification for a product you will be buying or building for your own private use, you should require “strict” conformance. If you are specifying a PP for any other purpose, use “demonstrable”.

If you claim conformance to a functional package or another PP, your own security problem definition, security objectives and security requirements must be compatible with that package or PP.

If you are writing a PP or ST and add additional requirements to those found in a referenced PP, be very careful that you do not create inconsistencies such that no TOE can implement all of the requirements, all at the same time.

9 Specifying the security problem definition

9.1 Introduction

This clause provides guidance on the specification of the *security problem definition* (SPD) section of a PP or ST. ISO/IEC 15408-1:—, clauses A.6 and B.6 describe PP and ST SPDs respectively. ISO/IEC 15408-1:—, Clause B.6, which deals with PPs, is simply a pointer to A.6, which can be taken as a confirmation that the expected content of the security problem definition section does not differ between a PP and an ST. Indeed, the wording of the relevant validation criteria in ISO/IEC 15408-3 is identical.

The purpose of the security problem definition is to define in a formal manner the nature and scope of the security problem which the TOE is intended to address. This is illustrated in Figure 1 following.

Although not all Protection Profiles and Security Targets contain a security problem definition (see clause 15), where it is present it is probably the most important part of the PP or ST, and the most dangerous to delegate to external contractors to prepare. To quote from ISO/IEC 15408:

“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”, (ISO/IEC 15408-1:—, subclause A.6.1).

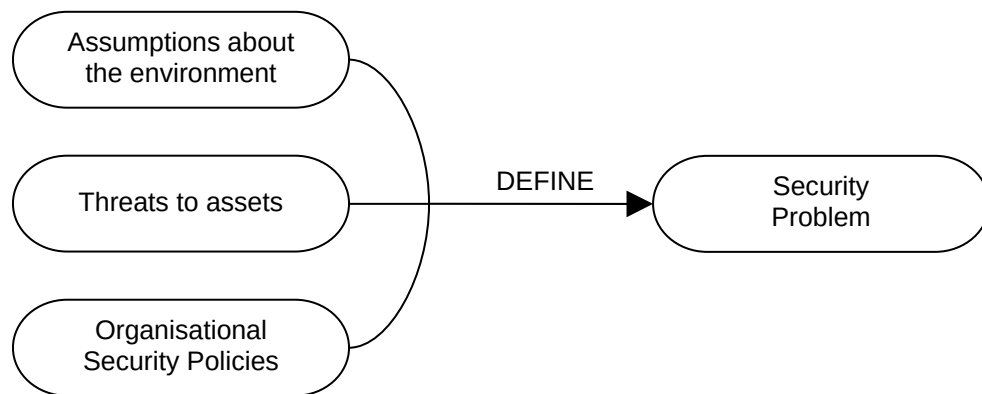


Figure 1 — Security problem definition

If the problem specified is the wrong problem, or if it is ambiguously described, then the remainder of the PP or ST will also be wrong. Worse, the wrong product may be selected or purchased on the basis of a valid but inapplicable specification. This clause is therefore one of the largest and most detailed in this Technical Report, although the criteria that it describes in ISO/IEC 15408 occupy only two or three pages of text. Regardless of whether you are a developer or a customer, and regardless of whether your PP or ST will be used in a specification or selection based process, it is of paramount importance *to get the security problem definition right*.

Subsequent sections of the PP and ST show how the security problem will be addressed by the TOE, in combination with its operating environment. It is therefore important to ensure that the security problem definition is clear, concise and consistent.

ISO/IEC 15408 does not assume or mandate any particular process or methodology for preparing the security problem definition; you can use any method you like. Of course, if you are new to the process of developing PPs and STs this is not helpful. This clause therefore includes a detailed description of a simple methodology that has been tried and tested in practice and found to work in a variety of organisations and environments. It is based upon a series of steps, performed in sequence:

- a) Identifying and confirming the informal security requirement;
- b) Identifying and specifying the applicable threats by performing formal threat analysis;
- c) Documenting the applicable policies;
- d) Documenting the applicable assumptions;
- e) Finalising and checking the complete SPD specification.

Regardless of the methodology employed, this Technical Report assumes that the security problem definition represents a formalised description of an existing informal security requirement. Of course, in practice, there may not be a straightforward single document that represents that informal requirement, it may not even be written down! The first step in the recommended methodology is therefore to identify and confirm the informal requirement, even though it does not appear within the PP or ST. The informal requirement may be obvious and well defined. In other cases, a large part of the work in developing the SPD may simply be identifying the informal requirement, and obtaining confirmation from management and other stakeholders that it is a correct and complete representation of their security needs.

The methodology also has two other aspects that are not *required* by ISO/IEC 15408, but which have been found in practice to save time overall, by avoiding confusion and queries in later stages of PP/ST development. These are:

- a) Documenting discounted threats;
- b) Producing a rationale to link the SPD back to the informal security requirement.

Both of these are explained in more detail at appropriate points in the methodology, but in brief, discounted threats are threats that may or may not apply to the product, but which, if applicable, would be countered by security functionality included in the TOE for other reasons. If these are not documented in the SPD, they are likely to be raised as queries when the PP/ST is reviewed. More seriously, if the requirement changes, functionality might be removed without considering its value in also covering discounted threats.

Evaluation treats the SPD as axiomatic; no attempt is made to trace it back to actual security needs. If no SPD rationale is created, there is always a risk that parts of the informal requirement may be lost in the process of creating the SPD, and that this is not discovered until the product is used and found not to be fit for purpose. A rationale therefore provides an important consistency and completeness check.

As a general principle, the security problem definition should avoid, where possible, any discussion of the form of the TOE's response to meeting the its requirements, e.g. details relating to the TOE security functions. By following this principle, you will help to focus the reader's attention on what are the important aspects of the security problem. Discussion of how the security problem will be satisfied by the TOE should be left to the later parts of the PP or ST. Of course, where a particular solution is mandated as part of the informal security requirement, that solution will have to be stated as part of the SPD, both to ensure it is documented and as justification for constraining later design decisions.

9.2 Identifying the informal security requirement

9.2.1 Introduction

There are always many things about a security problem – and its intended solution – that are already fixed and known before security problem definition begins. These requirements and constraints form the informal security requirement. The difficulty is always to identify and document them. This therefore becomes the first step in our recommended methodology.

9.2.2 Sources of information

9.2.2.1 Overview

There are many ways that aspects of the informal security requirement can be identified. The subsections following discuss some of them. In a particular organisation, there may be others that a generic methodology as described in this Technical Report cannot identify. You will have to think about your security needs carefully and thoroughly. However, the possible sources of information suggested in this subsection should help.

9.2.2.2 Required functionality

Security functionality may be part of the purpose of the product under consideration. This particularly applies to COTS products, where security services to be available to the purchaser through Application Program Interfaces (APIs) or Human Computer Interfaces (HCIs) may be an essential part of the product specification.

If security functionality is part of a documented user requirement, providing it is part of the problem addressed in the SPD.

9.2.2.3 Risk assessment

A security risk assessment may have already been performed covering a proposed system, and even a COTS product, and identified risks that need to be reduced by IT security controls. These risks represent part of the security problem.

There are many methodologies for performing risk assessments. However, these methodologies generally accept that for a risk to exist, there must be three things: an asset with a value that can be damaged in some way, a threat, something or someone who can damage the asset, and a vulnerability, a way that the asset can be damaged. If any one of these three does not exist, there can be no risk. This form of model is assumed by ISO/IEC 15408; if the actual risk assessment used an incompatible model of risk, there might be problems mapping its results into a suitable form for use in the SPD.

9.2.2.4 Threat assessment

A threat assessment is a weakened form of risk assessment where it is assumed that if a threat exists, assets can be damaged and thus a risk will exist. In this case, the identified threats represent part of the security problem.

Threat assessment is particularly appropriate where the person trying to identify and specify a security problem is not the owner of the assets that will be protected, and thus not in a position to perform risk assessment or determine the value of assets.

9.2.2.5 Management policy

A security requirement can result from a policy decision by management, for example that all systems in a particular organisation will contain certain standard IT security controls. This process is sometimes known as “minimum standards” or “risk avoidance”. The policy may be arbitrary, for example, following what similar organisations do, or it may have a logical basis, for example to meet legal requirements or contractual conditions imposed by customers.

Of course, even where a policy has a logical basis in law or contract, the mandated security controls may not be appropriate for a particular system or organisation, or may only be applicable in part.

9.2.2.6 Presentational policy

A security requirement may arise from a wish to demonstrate that an organisation or a COTS product implements certain IT security controls. This policy may arise due to marketing needs, or from a wish to be seen to follow best practice.

Security problems of this type are well suited to ISO/IEC 15408 evaluation, as successful evaluation using an approved evaluation facility will permit an official certificate to be issued, providing independent verification that the controls exist. Published PPs can be used to identify suitable controls.

The drawback to policies of this type is that they are based on achieving certification or demonstration of compliance, not in selecting security controls that are relevant to the product in question. This can cause problems finding reasons to put in the SPD that justify the need for the controls. They may have to be treated as policy decisions, which the originator may be reluctant to acknowledge is the true reason for their selection.

9.2.2.7 Evaluation policy

An organisation may have a policy that IT products are evaluated using an evaluation scheme based on ISO/IEC 15408 or the Common Criteria, regardless of the security controls they implement.