PD ISO/IEC TR 15446:2017

BSI Standards Publication

Information technology — Security techniques — Guidance for the production of protection profiles and security targets

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15446:2017

National foreword

This Published Document is the UK implementation of ISO/IEC TR 15446:2017. It supersedes PD ISO/IEC TR 15446:2009, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 95758 1

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2017.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15446:2017

TECHNICAL REPORT

ISO/IEC TR 15446

Third edition
2017-10

Information technology — Security techniques — Guidance 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 15446:2017(E)

Documents
Document Sharing Hub
© ISO/IEC 2017

Full document details: PD ISO/IEC/TR 15446:2017

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC/TR 15446:2017

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Purpose and structure of this document ... **2**
6 Overview of PPs and STs ... **2**
6.1 General ... 2
6.2 Audience ... 2
6.3 Use of PPs and STs ... 3
6.3.1 General ... 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 ... 8
6.4.1 Including stakeholders in the development process ... 8
6.4.2 Method to develop a PP or ST ... 9
6.4.3 Evaluation of PPs and STs ... 9
6.5 Reading and understanding PPs and STs ... 10
6.5.1 General ... 10
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 ... 15
6.5.9 Further reading ... 15
7 Specifying the PP/ST introduction ... **15**
8 Specifying conformance claims ... **16**
9 Specifying the security problem definition ... **17**
9.1 General ... 17
9.2 Identifying the informal security requirement ... 18
9.2.1 General ... 18
9.2.2 Sources of information ... 19
9.2.3 Documenting the informal requirement ... 20
9.3 How to identify and specify threats ... 21
9.3.1 General ... 21
9.3.2 Deciding on a threat analysis methodology ... 21
9.3.3 Identifying participants ... 23
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 Finalizing the security problem definition ... 31
10 Specifying the security objectives ... **32**
10.1 General ... 32
10.2 Structuring the threats, policies and assumptions ... 33
10.3 Identifying the non-IT operational environment objectives ... 34

© ISO/IEC 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

10.4 Identifying the IT operational environment objectives ... 35
10.5 Identifying the TOE objectives ... 35
10.6 Producing the objectives rationale ... 38

11 Specifying extended component definitions ... 39

12 Specifying the security requirements ... 43
12.1 General ... 43
12.2 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 ... 48
12.2.4 TOE self protection ... 49
12.2.5 Securing communication ... 50
12.2.6 Security audit ... 52
12.2.7 Architectural requirements ... 52
12.3 How to specify security functional requirements in a PP or ST ... 53
12.3.1 How should security functional requirements be selected? ... 53
12.3.2 Selecting SFRs from ISO/IEC 15408-2:2008 ... 56
12.3.3 How to perform operations on security functional requirements ... 58
12.3.4 How should the audit requirements be specified? ... 60
12.3.5 How should management requirements be specified? ... 61
12.3.6 How should SFRs taken from a PP be specified? ... 62
12.3.7 How should SFRs not in a PP be specified? ... 62
12.3.8 How should SFRs not included in ISO/IEC 15408-2:2008 be specified? ... 62
12.3.9 How should the SFRs be presented? ... 63
12.3.10 How to develop the security requirements rationale ... 63
12.4 How to specify assurance requirements in a PP or ST ... 64
12.4.1 How should security assurance requirements be selected? ... 64
12.4.2 How to perform operations on security assurance requirements ... 65
12.4.3 How should SARs not included in ISO/IEC 15408-3:2008 be specified in a PP or ST? ... 66
12.4.4 Security assurance requirements rationale ... 66

13 The TOE summary specification ... 67

14 Specifying PP/STs for composed and component TOEs ... 67
14.1 Composed TOEs ... 67
14.2 Component TOEs ... 70

15 Special cases ... 71
15.1 Low assurance Protection Profiles and Security Targets ... 71
15.2 Conforming to national interpretations ... 71
15.3 Concepts to enhance the flexibility of Protection Profiles ... 72
15.3.1 Functional and assurance packages ... 72
15.3.2 Extended packages ... 72
15.3.3 Conditional security functional and assurance requirements ... 72
15.3.4 Optional security functional and security assurance requirements ... 73

16 Use of automated tools ... 73

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

Annex B (informative) **Example for the specification of refinements ... 77**

Bibliography ... 79

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC TR 15446:2009), which has been technically revised.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

Introduction

This document is an adjunct to ISO/IEC 15408 (all parts). 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 (all parts) 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 document 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.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

Information technology — Security techniques — Guidance for the production of protection profiles and security targets

1 Scope

This document 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 (all parts). It is also applicable to PPs and STs compliant with Common Criteria Version 3.1 Revision 4[6], a technically identical standard published by the Common Criteria Management Board, a consortium of governmental organizations involved in IT security evaluation and certification.

NOTE This document is not intended as an introduction to evaluation using ISO/IEC 15408 (all parts). Readers who seek such an introduction can read ISO/IEC 15408-1.

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1 and the following apply.

COTS Commercial Off The Shelf

CRL Certificate Revocation List

LDAP Lightweight Directory Access Protocol

SPD Security Problem Definition

SSL Secure Sockets Layer

TLS Transport Layer Security

© ISO/IEC 2017 – All rights reserved

Documents Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

5 Purpose and structure of this document

This document 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 (all parts). It provides detailed guidance relating to the various parts of a PP or ST, and how they interrelate.

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

This document 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 document are familiar with ISO/IEC 15408-1:2009, and in particular, Annexes A and B which describe STs and PPs, respectively. PP and ST authors will need to become familiar with the other parts of ISO/IEC 15408 as described in this document, including introductory materials such as the functional requirements paradigm described in ISO/IEC 15408-2:2008, Clause 5.

This document is intended for guidance only. It should not be cited as an International Standard on the content or structure for the evaluation of PPs and STs. It is intended to be fully consistent with ISO/IEC 15408 (all parts); however, in the event of any inconsistency between this document and ISO/IEC 15408 (all parts), the latter as a normative International 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 may be used. Clause 6 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 15408-1:2009, 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 some new concepts for enhancing the flexibility and usability of Protection Profiles.

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

6 Overview of PPs and STs

6.1 General

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

6.2 Audience

This document 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 (all parts);

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

b) experts in information security with good knowledge of ISO/IEC 15408 (all parts), who are engaged in developing PPs and STs as part of their professional activities.

If the reader falls into the former category, this clause should provide the information needed to understand the purpose and structure of PPs and STs. It should also provide the background information needed to read and understand PPs and STs, and to identify their relevance and correctness with respect to the particular circumstances. Clauses 7 to 13 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 (all parts).

If the reader is an expert, she/he should already be familiar with the contents of this clause. Subsequent clauses will provide the methodologies, techniques and practical tips that can be used to prepare PPs and STs in an efficient yet consistent manner.

If the reader is not an expert in information security, and needs to produce a PP or ST, this document will help to do so. However, the reader will also need to find, read and understand published examples of PPs or STs similar to the requirements she/he has. The reader should also consider calling on the services of others who *do* have the necessary specialist knowledge and experience.

6.3 Use of PPs and STs

6.3.1 General

The main use of ISO/IEC 15408 (all parts) 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 organization, or a COTS package created by a product manufacturer for sale to many different and unrelated customers. In this document, when this document talks about IT products, or just products, the advice is intended to apply to all such entities. Where the scope of our advice is limited to a particular type of product, this document talks 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 standardized 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 recognizes 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 clause, this document will call this a specification-based purchasing process.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

— 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 clause, this document 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 6.3.2 and 6.3.3, this document shows 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 should be performed.

a) The customer has to determine his security requirements informally.

b) The customer has to transform these informal security requirements into a more formal specification suitable for use by a developer.

c) The developer has to 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 document. 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;

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

c) implicit. Some product requirements have consequences, but these consequences are not included themselves. 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; and

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 formalizing of customer requirements. For security requirements based on ISO/IEC 15408, this formalization 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 formalized, standardized way.

6.3.2.3 Using PPs as specifications

PPs are typically written as a collaborative effort by a group consisting of large organizations, groups of organizations, government departments, as consumers and a group of developers. This collaboration should ensure that the customer needs are not only addressed, but also the technical feasibility of the requirements specified is given.

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; and

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.

A PP may also contain technology-specific refinements of the "security assurance requirements", describing in detail how the correctness and effectiveness of specific security functions need to be assessed. An example would be to demand the use of a defined test suite developed for testing the correctness of the implementation of a cryptographic algorithm or cryptographic protocol.

6.3.2.4 Building a product from a PP

The customer can now give the PP, i.e. his formalized 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).

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

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 that 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; and

— the ST contains more detail than the PP. While the PP explains "what" needs to 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 (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 Role of evaluation in a specification-based purchasing process

Until now, this document has 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. If the PP requires compliance testing for some functions by using a specific test procedure as part of the assurance activities, the evaluation will ensure compliance for those functions as far as defined by the test procedure used.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

6.3.3 Selection-based purchasing processes

6.3.3.1 Overview

6.3.2 discusses a customer delivering a specification and a developer implementing that specification. This subclause discusses a 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 formalized 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 has to produce a product and a specification of this product and provide the specification to the customer, and

b) the customer has to 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 formalized 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)].

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, therefore, does 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 document. 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 document.

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.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

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*. An 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.

Organizations specifying or mandating PPs for such purposes have an onerous responsibility to ensure that such PPs are minimal (they ask for no more than what 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 recognized that at the time of publication, no such products exist yet. If the reader is a product developer, treat such PPs with caution. By the time a suitable product has been developed, the requirements defined in the PP may be obsolete or the sponsors of the PP may no longer want to buy the 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

6.4.1 Including stakeholders in the development process

When a PP or ST is developed, it is crucial that the relevant stakeholders are represented in the development team. The development team should include experts in the product-type technology, the security functionality that will be included in the PP or ST, as well as experts familiar with the application of ISO/IEC 15408.

Although out of scope for this document, it is also important that the developer of the ST or PP has a thorough understanding of any applicable regulations and policies with regard to the proposed assurance consumer.

When developing an ST that is expected to be conformant to a PP, the team should include someone familiar with the application of that PP.

When developing a PP that several product developers may try to meet in the future, it is recommended that stakeholders from the developer community are included. This will help ensure that the requirements of the PP can be met in the future, and that the requirements given do not inadvertently preclude products provided by certain vendors. Especially for a PP intended for use in a specification-based purchasing process, those stakeholders should also include representatives from the proposed end-user community.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

With such a large variety of stakeholders represented, it can be expected that developing a PP can take some time, usually in the order of months, and that the development process requires collaboration and negotiation skills.

As an example, the concept of a collaborative Protection Profile (cPP), a construct of the Common Criteria Recognition Arrangement (CCRA), seeks to ensure that all the relevant stakeholders are involved in the development of a cPP through the establishment of technical communities or an international Technical Community (iTC) recognized by the CCDB, and ensuring that the needs of the specification-based purchasing processes of the proposed assurance consumers are met.

The process for the development of a cPP by an iTC is defined by the CCDB. Details of this process can be found on the website maintained by the CCDB.

6.4.2 Method to develop a PP or ST

The order of presentation of the requirements for PPs and STs in ISO/IEC 15408-1:2009, Annexes A and B and in the earlier parts of this clause may 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, and

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, organizational 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 may surface, within the scope of the current security problem, that may lead changes to the document which reflect changes in external circumstances, for example,

a) new threats may be identified,

b) organizational 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, and

d) changes in intended attack potential may impact 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".

6.4.3 Evaluation of PPs and STs

ISO/IEC 15408 describes the evaluation of both PPs and STs. The goal of evaluating these documents is to determine whether it is complete, consistent, and technically sound. ISO/IEC 15408-3:2008 contains the evaluation criteria that an evaluator is obliged to consult in order to determine this. These criteria, and the evaluation methodology associated with Protection Profile Evaluation (APE class) and with

© ISO/IEC 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

Security Target evaluation (ASE class) evaluation may, of course, also be used by the developer of the PP or ST as a check before a formal evaluation occurs.

Once a PP has been evaluated and found to meet these criteria, a validation certificate may be published or the PP may be added to a catalogue. This is so that prospective users of the PP can have confidence that it is complete, consistent, and technically sound. This, of course, does not imply that a PP will meet other objectives of the assurance consumer that were described in 6.3.

6.5 Reading and understanding PPs and STs

6.5.1 General

6.5 is *not* intended for experts with prior knowledge of ISO/IEC 15408. It is intended for the part of the audience for this document who know very little about PPs or STs and 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 15408-1:2009, 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 they can be downloaded. The Common Criteria Portal includes the largest[4]. This register is recognized by the ISO and IEC councils as the official JTC 1 register for Protection Profiles and packages constructed in accordance with ISO/IEC 15408.

Unfortunately, a PP or ST cannot be summarized 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 6.5.2 to 6.5.7, this document therefore identifies 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, and

d) the conformance claim.

In 6.5.2 to 6.5.6, this document will discuss each of these in more detail.

6.5.2 Reading the TOE overview

The TOE overview is, in general, the first thing one 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 15408-1:2009, 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.

This document now discusses each of these in turn. Some simple examples of each can be found in ISO/IEC 15408-1:2009, A.4.2.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

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 description 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 the reader to believe that the TOE has certain security functionality and it does not have this functionality, the TOE overview should list this missing functionality, and

b) if the TOE-type would lead the reader to believe that the TOE could be used in a certain environment and it cannot be used in such an environment, the TOE overview should 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 the intended use, the reader should seriously consider whether she/he 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 the reader to determine the major external hardware/software/firmware components needed to use the TOE.

The reader should carefully assess whether there are any non-standard components on which the TOE relies and whether these components fit in with the 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 a 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 15408-1:2009, A.4.1 prohibits misleading TOE references, but developers can always get around this by just using a product name. The ST reader needs to check that the evaluated functionality meets the needs. If some of the security functionality intended to be used was excluded, the reader needs to ask 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 15408-1:2009, A.4.3).

The ST reader should briefly examine this list to see if there is anything odd or unexpected, or whether some parts of the product that are expected to be present are missing. If something is not in this list, then the evaluation has completely ignored it and assumed it did not exist. If such parts are intended to be used, then one can draw no conclusions about its security capabilities from the evaluation.

© ISO/IEC 2017 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

With regards to logical scope, ISO/IEC 15408-1:2009 states 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 15408-1:2009, A.4.3).

Whereas the physical scope specifies the list of parts of the TOE, the logical scope should define what the TOE does. This was already briefly discussed in the *Usage and Major Security features* section of the TOE overview (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 the TOE description is that if the product is expected 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 one wants to use the product in its evaluated configuration.

It is therefore important to scrutinize the TOE description to determine whether all security-related features that the reader of the ST requires were actually evaluated. If they are not, there will be no assurance in the operation of those features from the 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 has to 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 have to be achieved by everything except the TOE in order for the TOE to meet its security requirements. There are a number of examples of security objectives for the operational environment in ISO/IEC 15408-1:2009, 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 have to be fully met and addressed by the operational environment; the TOE itself will not meet them. If a single one of these objectives is not met, the TOE may not function securely. It is therefore imperative to determine whether they are achievable in the organization using the TOE, and if one of them is not achievable, the TOE may not be suitable for the organization.

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 document, and this document 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

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

designed their own assurance tests, and from a consumer point of view, one should question why this was necessary;

— a list of packages that the TOE claims conformance with. These can be packages consisting of security functional requirements only, packages consisting of security assurance requirements only or packages consisting of a mixture of both security functional requirements and security assurance requirements. ISO/IEC 15408 defines only a set of assurance packages named “evaluation assurance levels (EAL)”. A set of 7 packages (EAL1, EAL2, ..., EAL7) is defined. These EALs are discussed further in 6.5.7;

— a list of Protection Profiles that the PP or ST claims conformance with. This is discussed further in 6.5.6.

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 has to 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.

When reading a PP, one will also find a statement that STs and other PPs has to 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 have to 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 the 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). Of course, an ST can still introduce additional restrictions if it wishes to do so. If a PP demands strict conformance and the organization that wants to use it was not part of the development of the PP, it is highly unlikely to be suitable for use within the organization.

Some national schemes and cPPs have also introduced the terms "exact compliance" and "exact conformance", both of which require that a conformant Security Target includes only Security Functional Requirements and Security Assurance Requirements that are defined in the PP. While exact compliance may be useful when assurance requirements have been refined specific for the security functions listed in the PP, one also has to take into account that such a restriction disallows a vendor to specify those additional security functions where he believes he provides more than his competitors. Customers may find that the specific security functions they are interested in have not been subject to the evaluation. To address security functionality that is not common to all products the PP intents to address, the use of extended packages, optional requirements and conditional requirements is strongly suggested for a PP that requires "exact conformance" or "exact compliance". Clause 15 describes those concepts.

6.5.7 EALs and other assurance issues

The TOE overview and TOE description will specify what the TOE is capable of doing, i.e. the functionality that is provided by the TOE. However, functionality does not say everything about an 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; or

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

— 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, one needs 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 formalizes 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 requires evaluation using enhanced or additional activities on the same set or a superset of evaluation deliverables.

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 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 characterization 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, and/or conformance to a technology-specific and widely adopted Protection Profile, are currently the only widely accepted ways to provide a characterization of ISO/IEC 15408 assurance that a relative layman can understand.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

A better way to adapt the assurance activities to the needs of system integrators and users of evaluated products is the definition of technology-specific refinements of the generic assurance requirements as defined in ISO/IEC 15408-2:2008. Protection Profiles are the best place to define such technology-specific refinements of assurance requirements. When it is foreseeable that those assurance requirements need to be adapted more often than changes to the Protection Profile itself are intended, it is wise to publish those technology-specific refinements in a "supporting document", where the PP itself references this document and makes the use of the latest version of it mandatory for an evaluation claiming compliance to the PP.

When developing a PP, there may be good reasons to not use one of the predefined evaluation assurance levels, but select a package of assurance components that better suit the type of product described in the PP and its intended way of operation.

6.5.8 Summary

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

a) (obviously) that an ST can be reasonably understood from reading a number of sections of the ST; but also

b) (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 clause has conveyed that an ISO/IEC 15408-certified EAL4 firewall may have limitations that make it totally unusable for use within some specific environments, and may not provide all the relevant security needed.

For example, suppose there is a need for both packet routing and HTTP/FTP proxy services from the 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 one finds an evaluated firewall that offers proxy services but the logical scope is limited to packet routing, one should ask 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 one tries.

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 one wants to know more about the product, one could also try reading the TOE summary specification, which is intended to provide more detail on how the TOE is implemented. The TOE summary specification 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 one needs to understand other sections of a PP or ST, then Clauses 7 to 13 may help. Whilst they are designed to be used by experts to specify PPs and STs, the information should also help 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 15408-1:2009, A.4 and B.4, and therefore little additional guidance is necessary in this document.

The introduction of a PP consists of the following elements:

— a PP reference;

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

— 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 summarizing the security problem definition section of the PP or ST (see Clause 9), whilst the major security features are best described by summarizing 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, one will probably find it easiest to leave it until the rest of the PP or ST is complete and writes 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 15408-1:2009, A.5, and the differences applicable to conformance claims in PP in ISO/IEC 15408-1:2009, 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 of a PP or ST;

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 15408-3:2008, 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 a PP or ST.

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

When specifying a PP, one has to define how other PPs and STs conform to the new PP. There are two choices for this:

a) Strict. Conceptually, this means that conforming PPs/STs has to contain everything in this PP. See ISO/IEC 15408-1:2009, 8.3 for the precise requirements.

b) Demonstrable. Conceptually, this means that conforming PPs/STs has to be "equivalent" to this PP. Again, see ISO/IEC 15408-1:2009, 8.3 for the precise requirements.

As a guideline, when writing a PP as the precise and complete specification for a product intended to be bought or built for one's own use, "strict" conformance should be required. When specifying a PP for any other purpose, "demonstrable" conformance should be required.

When claiming conformance to a functional package or another PP, the security problem definition, security objectives and security requirements of the PP developed has to be compatible with that package or PP.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

When writing a PP or ST and one adds additional requirements to those found in a referenced PP, one has to be very careful to 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 General

This clause provides guidance on the specification of the *security problem definition* (SPD) section of a PP or ST. ISO/IEC 15408-1:2009, A.6 and B.6 describe PP and ST SPDs, respectively. ISO/IEC 15408-1:2009, B.6, which deals with PPs, is simply a pointer to A.6 of that document, 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 15408-3:2008 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.

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 15408-1:2009, A.6.1).

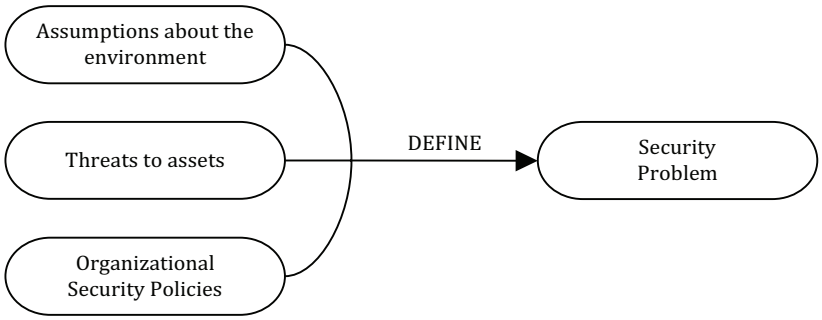

Figure 1 — Security problem definition

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 document, although the criteria that it describes in ISO/IEC 15408-1:2009 occupy only two or three pages of text. Regardless of whether the ST or PP author is a developer or a customer, and regardless of whether the 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; one can use any method. Of course, if someone is new to the process of developing PPs and STs, this is not helpful. This clause therefore includes a detailed description

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

of a simple methodology that has been tried and tested in practice and found to work in a variety of organizations 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) finalizing and checking the complete SPD specification.

Regardless of the methodology employed, this document assumes that the security problem definition represents a formalized 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, and

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 may 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 requirements, e.g. details relating to the TOE security functions. By following this principle, one 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 General

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.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC/TR 15446:2017

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. This subclause discusses some of them. In a particular organization, there may be others that a generic methodology as described in this document cannot identify. The PP or ST author will have to think about the security needs carefully and thoroughly. However, the sources of information suggested in this subclause 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 assessement

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 should 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 or 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 may 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 organization 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 organizations 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 organization, 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 organization 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 the best practice.

Documents
Document Sharing Hub

© ISO/IEC 2017 – All rights reserved

Full document details: PD ISO/IEC/TR 15446:2017