PUBLISHED DOCUMENT

PD ISO/IEC TR 15446:2004

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

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards Documents Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

National foreword

This Published Document reproduces verbatim ISO/IEC TR 15446:2004.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT – Security techniques, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled "International Standards Correspondence Index", or by using the "Search" facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO title page, pages ii to viii, pages 1 to 125 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 15 July 2004

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 15 July 2004

ISBN 0 580 44046 X

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

TECHNICAL REPORT

ISO/IEC TR 15446

First edition
2004-07-01

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 15446:2004(E)

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

Contents

Page

Foreword vi
Introduction vii
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviations 2
5 Purpose of this Technical Report 2
6 Overview of the PP and ST 3
6.1 Introduction 3
6.2 The Protection Profile and Security Target contents 3
6.3 Relationship between the PP and ST 5
6.4 Aiming a PP or ST at its target audience 5
6.5 The PP and ST development process 6
6.6 PP families 7
7 Descriptive parts of the PP and ST 7
7.1 Introduction 7
7.2 Descriptive parts of a PP or ST 7
8 The TOE security environment 9
8.1 Introduction 9
8.2 How to identify and specify the assumptions 10
8.3 How to identify and specify the threats 10
8.4 How to identify and specify the Organisational Security Policies 15
9 The security objectives 16
9.1 Introduction 16
9.2 How to specify security objectives for the TOE 16
9.3 How to specify security objectives for the environment 18
10 Security requirements 20
10.1 Introduction 20
10.2 How to specify security functional requirements in a PP or ST 22
10.3 How to specify assurance requirements in a PP or ST 31
10.4 Security requirements on the environment 34
11 The TOE summary specification 35
11.1 Introduction 35
11.2 How to specify the IT security functions 36
11.3 How to specify security mechanisms 37
11.4 How to specify the assurance measures 37
12 PP Claims 37
12.1 Introduction 37
12.2 PP reference 38
12.3 PP tailoring 38
12.4 PP additions 38
13 PP and ST rationale 38
13.1 Introduction 38
13.2 How to present the security objectives rationale in a PP or ST 40
13.3 How to present the security requirements rationale in a PP or ST 41

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

14 PPs and STs for composite and component TOEs 46
14.1 Introduction 46
14.2 The composite TOE 47
14.3 The component TOE 49

15 Functional and assurance packages 51
15.1 Background 51
15.2 How to specify a functional package 51
15.3 How to specify an assurance package 52

Annex A (informative) Guidance checklist 54
A.1 Introduction 54
A.2 PP/ST introduction 54
A.3 TOE Description 54
A.4 Defining the statement of TOE security environment 54
A.5 Defining the security objectives 55
A.6 Specifying the IT security requirements 56
A.7 Producing the TOE summary specification 57
A.8 Constructing the PP rationale 57
A.9 Constructing the ST rationale 58

Annex B (informative) Generic examples 59
B.1 Introduction 59
B.2 Example Threats 59
B.3 Example organisational security policies 60
B.4 Example assumptions 61
B.5 Example security objectives for the TOE 61
B.6 Example security objectives for the environment 62
B.7 Example mapping of security objectives to threats 63
B.8 Example security functional requirements 71

Annex C (informative) Specifying cryptographic functionality 76
C.1 Introduction 76
C.2 Terminology 76
C.3 Overview of cryptography 80
C.4 Deriving the security requirements 81
C.5 Expressing IT security requirements 86
C.6 Guidance on applying assurance requirements 101

Annex D (informative) Worked example: Firewall PP and ST 103
D.1 Introduction 103
D.2 TOE description 103
D.3 Security environment 103
D.4 Security objectives 105
D.5 IT security requirements 105
D.6 TOE Summary Specification 107
D.7 PP claims 108
D.8 PP rationale 108
D.9 ST rationale 109

Annex E (informative) Worked example: Database PP 111
E.1 Introduction 111
E.2 TOE security environment 111
E.3 Security objectives 113
E.4 IT security requirements 113
E.5 PP rationale 115

Annex F (informative) Worked example: Trusted third party PP 117
F.1 Introduction 117
F.2 TOE security environment 118
F.3 Security objectives 119
F.4 IT security requirements 120
F.5 PP rationale 123

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

Bibliography 125

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

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.*

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

Introduction

The purpose of a Protection Profile (PP) is to state a security problem rigorously for a given collection of systems or products - known as the Target Of Evaluation (TOE) - and to specify security requirements to address that problem without dictating how these requirements will be implemented. (For this reason, a PP is said to provide an implementation-independent security description.) A PP thus includes several related kinds of security information:

a) A PP overview and a TOE description which identify, in terms appropriate for users of information technology, the statement of need or security problem to be addressed.

b) A description of the TOE security environment which refines the statement of need with respect to the intended environment of use, producing the threats to be countered and the organisational security policies to be met in light of specific assumptions.

c) Security objectives which scope the TOE evaluation based on the description of the TOE security environment, giving information about how, and to what extent, the security concerns are to be met. The purpose of a security objective is to mitigate risk and to support the security policies of the PP sponsor.

d) Security functional requirements and assurance requirements which address the problem posed by the statement of need, to the extent defined by the security objectives for the TOE and its IT environment. The security functional requirements explain what must be done by the TOE, and what must be done by its IT environment, in order to meet the security objectives. The assurance requirements explain the degree of confidence expected in the security functions of the TOE and the IT environment.

e) A rationale which demonstrates that the security functional requirements and assurance requirements suffice to meet the statement of need. The security objectives must explain what is to be done about the security concerns found in the description of the TOE security environment. The security functional requirements and assurance requirements must meet the security objectives.

A Security Target (ST) is similar to PP, except that it contains additional implementation-specific information detailing how the security requirements are realised in a particular product or system. Thus, the ST contains the following additional information not found in a PP:

a) A TOE summary specification that presents TOE-specific security functions and assurance measures.

b) An optional PP claims portion that explains which PPs the ST is claimed to be conformant with, if any.

c) Finally, the rationale contains additional evidence establishing that the TOE summary specification ensures satisfaction of the implementation-independent requirements, and that any claims about PP conformance are satisfied.

A PP may be used to define a ‘standard’ set of security requirements with which one or more products may claim compliance, or which systems used for a particular purpose within an organisation must comply. (See ISO/IEC 15408-1, 2.3 for the definition of the terms *product* and *system*, and also ISO/IEC 15408-1, 4.1.2 for a general discussion of the distinction between the two). A PP may apply to a particular type of TOE (e.g. operating system, database management system, smartcard, firewall, and so on), or it could apply to a set of products grouped together in a *composite* TOE (system or product).

Product vendors may respond to the security concerns defined by a PP by producing an ST which demonstrates how their product addresses those security concerns. However, it is not mandatory for an ST to claim conformance with a PP. A product vendor may assume a set of security concerns for their market place and produce an ST specifying how the security functions claimed by their product meets those concerns, and this forms the baseline for the product evaluation.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

A PP may also define the security requirements to be satisfied by a specific IT system. In this event, the ST is proposed in response to the PP, i.e. the ST may be written in response to an RFP (Request For Proposal) that references the PP. A PP and ST can thus be used as a means of communication among the party responsible for managing the development of a system, the stakeholders in that system, and the organisation responsible for producing the system (hereafter referred to as the developer). The content of the PP and ST may be negotiated among the players. Evaluation of the actual system against the ST - which has been confirmed as conformant with the PP - may be part of the acceptance process. (It should of course be noted that an ST may be written by a developer as part of a response to an RFP that does not reference a PP.)

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

Information technology — Security techniques — Guide 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 ISO/IEC 15408 (the 'Common Criteria').

As such, the document is primarily aimed at those who are involved in the development of PPs and STs. However, 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 may also be of interest to consumers and users of PPs and STs who wish to understand what guidance the PP/ST author used, and which parts of the PP or ST are of principal interest.

It is assumed that readers of this Technical Report are familiar with ISO/IEC 15408-1, and in particular Annexes B and C which describe PPs and STs. 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, 1.3.

This document is an informational ISO Technical Report 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.

This Technical Report does not deal with issues such as PP registration and associated tasks such as the handling of protected intellectual property (e.g. patents) in a PP. For information on PP registration procedures, see [1].

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 15408-1:1999, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:1999, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3:1999, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

ISO 2382-8:1998, *Information technology — Vocabulary — Part 8: Security*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, 2.3 apply.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

4 Abbreviations

For the purposes of this document, the abbreviations given in ISO/IEC 15408-1, 2.1 and the following apply:

DBMS Database Management System

OSP Organizational Security Policy

RFP Request for Proposal

SAR Security Assurance Requirement

SFR Security Functional Requirement

TSS TOE Summary Specification

TTP Trusted Third Party.

5 Purpose of this Technical Report

This Technical Report provides detailed guidance relating to the various parts of a PP or ST, and how they interrelate. For a summary of the key points of guidance contained in this document, presented in the form of a checklist, the interested reader should consult Annex A.

This Technical Report is structured such that the guidance to PP and ST authors is presented in the main body (i.e. the individual clauses), with a summary presented in Annex A as mentioned above. Subsequent annexes then present a variety of examples to illustrate application of the guidance.

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

Clause 6 provides an overview of the PP and ST which presents example contents lists and highlights the expected contents of, and the target audience for, the various parts of a PP or ST. This clause also discusses the relationship between the PP and the ST and issues relating to the PP/ST development process. Clause 7 examines in more depth the descriptive parts of a PP and ST, covering the PP and ST introduction and the TOE description (which tend to be more aimed at consumers and users) as well as PP application notes (which tend to be more aimed at ST authors and TOE developers).

The next five clauses of the Technical Report follow the order of the PP and ST contents as outlined in ISO/IEC 15408-1, Figures B.1 and C.1.

Clause 8 gives guidance on the definition of the TOE security environment in a PP or ST, which covers the various aspects of the ‘security concerns’ to be met by the TOE. Clause 9 then provides guidance on the definition of the intended response to the different aspects of the security concerns by the TOE and its environment, as given in the specification of security objectives in a PP or ST. Both of these clauses are of general interest, not only to PP/ST authors, but also to others such as consumers and users of PPs and STs.

Clause 10 provides guidance on the selection and specification of IT security requirements in a PP or ST. This clause goes into some detail describing how the functional and assurance components defined in ISO/IEC 15408, as well as non-ISO/IEC 15408 components, should be used to provide a clear definition of the IT security requirements. Clauses 11 and 12 then provide specific guidance relating to STs, covering the TOE summary specification and PP compliance claims respectively. These three clauses will be mainly of interest to PP/ST authors and evaluators.

Clause 13 provides guidance on the construction and presentation of the Rationale sections of a PP and ST.

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

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

Clause 15 provides guidance on the construction of functional and assurance packages, which are defined so as to be useable in different PPs and STs. A package is thus seen as potentially a very useful tool intended to promote and facilitate cost-effective construction of PPs and ST.

As described above, Annex A summarises the guidance in the form of a checklist.

Annex B presents example threats, organisational security policies, assumptions, and security objectives, and identifies appropriate ISO/IEC 15408 functional components for specifying common or generic security functional requirements. Although these examples are intended to be wide-ranging, they are in no way claimed to be exhaustive.

Annex C provides guidance that specifically relates to PPs and STs for TOEs which implement cryptographic functionality. Such guidance has been included to cover a wide range of such TOEs, and deal with the specific issues relating to specification of cryptographic functionality. (Future versions of the Technical Report may include similar annexes for other types of TOE.)

Annexes D to F illustrate application of the guidance in a variety of contexts, using worked examples for different types of TOE. Each of these examples is based on actual PPs and STs that have been developed (independent of this Technical Report). In Annex D, we see application of guidance to the construction of a firewall PP and ST. Annex E discusses a database management system PP, where it can be seen that the issue of dependencies on the IT environment is of particular importance. Finally, Annex F examines the issues surrounding the development of a Trusted Third Party (TTP) PP.

6 Overview of the PP and ST

6.1 Introduction

This clause provides an overview of the PP and ST, summarising the contents of both documents, discussing the relationship between the PP and ST, and the process by which the documents are developed. See also ISO/IEC 15408-1, Annexes B and C.

6.2 The Protection Profile and Security Target contents

The required content of a PP is portrayed in ISO/IEC 15408-1, Figure B.1. Table 1 following translates this into an example contents list.

The required content of an ST is portrayed in ISO/IEC 15408-1, Figure C.1. Table 2 following adds additional content to that of Table 1 to give an example contents list for an ST.

The reader of a PP or ST, as with any document, should be able to easily discern where the required content is within the PP or ST.

The *Introduction* identifies the PP or ST and TOE (including its version number) and provides a summary of the PP or ST in narrative form. The summary for a PP can be used for inclusion in a PP catalogue and register. For an ST, suitable for inclusion e.g. in a list of products that have been evaluated. This section is discussed in more detail in Clause 7 of this Technical Report.

The *TOE Description* provides general information on the TOE (or TOE type), and serves as an aid to understanding its security requirements and intended usage. For an ST, the TOE description should also include a definition of the configuration in which the TOE is to be evaluated. This section is discussed in more detail in Clause 7 of this Technical Report.

The *TOE Security Environment* provides a definition of the context in which the TOE resides, and in particular defines the ‘security concerns’ the TOE is intended to address. This description details any assumptions defining the scope of the security concerns, the scope of the intended use, the identified threats to the assets requiring protection (together with a description of those assets), and any organisational security policies with which the TOE must comply. This section is discussed in detail in Clause 8 of this Technical Report.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

Table 1 — Example Protection Profile Contents List

1	PP INTRODUCTION 1.1 Identification 1.2 Overview
2	TOE DESCRIPTION
3	TOE SECURITY ENVIRONMENT 3.1 Assumptions 3.2 Threats 3.3 Organisational Security Policies
4	SECURITY OBJECTIVES 4.1 Security Objectives for the TOE 4.2 Security Objectives for the Environment
5	IT SECURITY REQUIREMENTS 5.1 TOE Security Functional Requirements 5.2 TOE Security Assurance Requirements 5.3 Security Requirements for the IT Environment
6	PP APPLICATION NOTES
7	RATIONALE 7.1 Security Objectives Rationale 7.2 Security Requirements Rationale

Table 2 — Example Contents List for a Security Target

1	ST INTRODUCTION 1.3 ISO/IEC 15408 Conformance
6[a]	TOE SUMMARY SPECIFICATION 6.1 TOE Security Functions 6.2 Assurance Measures
7	PP CLAIMS 7.1 PP Reference 7.2 PP Tailoring 7.3 PP Additions
8	RATIONALE 8.3 TOE Summary Specification Rationale 8.4 PP Claims Rationale
[a] PP Application Notes are not included in a Security Target.	

The *Security Objectives* provide a concise statement of the intended response to the security concerns, both in terms of the security objectives to be satisfied by the TOE, and the security objectives to be satisfied by IT

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

and non-IT measures within the TOE environment. This section is discussed in detail in Clause 9 of this Technical Report.

The *IT Security Requirements* define the security functional requirements on the TOE, the security assurance requirements, and any security requirements on software, firmware and/or hardware in the IT environment for the TOE. The IT security requirements are to be defined using, where applicable, functional and assurance components from ISO/IEC 15408-2 and ISO/IEC 15408-3. This section is discussed in detail in Clause 10 of this Technical Report.

The *PP Application Notes* is an optional section in a PP providing any additional supporting information considered useful by the PP author. Note that application notes may be distributed amongst the relevant sections of the PP instead of being provided in a separate section. This is discussed in more detail in Clause 7 of this Technical Report.

The *TOE Summary Specification* is the section in an ST that defines the IT security functions provided by the TOE to meet the specified security functional requirements, and also any assurance measures claimed to satisfy the specified security assurance requirements. This is discussed in detail in Clause 11 of this Technical Report.

The *PP Claims* is an optional section of an ST which identifies any PPs with which the ST is claimed to conform, and any additions or tailoring of the PP objectives or requirements. This is discussed in detail in Clause 12 of this Technical Report.

The *Rationale* provides a demonstration that the PP or ST specifies a complete and cohesive set of IT security requirements, and that a conformant TOE would effectively address the defined security concerns, and that the IT security functions and assurance measures are suitable to meet the TOE security requirements. Note that the rationale may be distributed amongst the relevant sections of the PP or ST instead of being provided in a separate section. This is discussed in detail in Clause 13 of this Technical Report.

Note also that the Rationale section may be packaged as a separate document, as stated in ISO/IEC 15408-1, B.2.8.

6.3 Relationship between the PP and ST

It will be evident from comparison of the example contents list in Tables 1 and 2 that there is a high degree of commonality between a PP and an ST, in particular within the *TOE Security Environment, Security Objectives* and *IT Security Requirements* sections, and the parts of the *Rationale* section which address these aspects. Indeed, if an ST simply claims conformance with a PP with no additional functional or assurance requirements, then the content of these sections of the ST may be identical to that the corresponding sections in the PP. In such cases it is recommended that the ST simply references the PP content, providing detail only where it differs from the PP.

The following sections in the ST provide detail that will not be featured in a PP, reflecting the specific nature of the ST, i.e. as a definition of how the TOE will provide a solution to the defined security concerns:

a) the *TOE Summary Specification*, covering IT security functions, security mechanisms or techniques, and assurance measures;

b) the optional *PP Claims*, detailing and justifying any claims of compliance with referenced PP(s);

c) those parts of the *Rationale* in the ST which demonstrate the adequacy of the IT security functions and the assurance measures to satisfy the TOE security requirements.

6.4 Aiming a PP or ST at its target audience

One of the key challenges in writing a PP or ST is to factor the presentation so that all of the intended audiences are properly served:

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

a) Consumers (i.e. procurers and high-level decision-makers) need a general understanding of what conforming TOEs will provide in the way of security. For successful PPs, this may be the largest class of readers.

b) Developers (including implementers in the case of an ST) need an unambiguous definition of security requirements in order to build conforming TOEs.

c) TOE users (including installers, administrators, and maintainers) need information on the required TOE security environment.

d) Evaluators need information that will justify the technical soundness and effectiveness of the PP or ST.

PPs and STs are designed in such a way that different sections serve different audiences, and they need to be written accordingly.

The *PP/ST Introduction*, *TOE Description*, and *TOE Security Environment* sections should be written primarily for consumers. The *Security Objectives* section may be also written for consumers. It should, however, be remembered that TOE developers will also need to take account of information in the *TOE Security Environment* and *Security Objectives* sections.

The *IT Security Requirements* section of the PP should be written primarily for TOE developers, although the information it contains is also likely to be of interest to TOE consumers. Conversely, the *TOE Summary Specification* section of a ST should be written primarily for evaluators and consumers. If these sections are not self contained, they should explicitly indicate which other PP sections and which other documents (e.g. referenced encryption standards) are necessary for a full and accurate understanding of the presented IT security requirements. In particular, if the *TOE Summary Specification* depends for its meaning on the *IT Security Requirements* section, this fact should be explicitly pointed out.

Evaluators need to be familiar with all sections of a PP or ST. However, the *Rationale* section while of interest to each user of a PP or ST, is generally evaluation information and primarily for evaluators.

6.5 The PP and ST development process

The presentation of the requirements for PPs and STs in Annexes B and C of ISO/IEC 15408-1, and in clauses 3 to 5 of ISO/IEC 15408-3, 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 a PP) that:

a) the security concerns are first defined;

b) the security objectives are then identified to address the security concerns;

c) IT security requirements are then defined to satisfy the security objectives for the TOE.

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

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

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 environment.

It is also possible (e.g. if the TOE is a product which has already been developed) that the PP or ST author already has a clear idea of the SFRs that the TOE will meet (even if these have not yet been expressed in the way ISO/IEC 15408 requires). 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'.

6.6 PP families

A 'PP family' is (as its name suggests) a set of closely related PPs, which typically apply to the same product or system type (e.g. operating system, firewall, and so on). A PP may thus be developed as part of a wider process of developing a family of PPs. Possibilities include the development of:

a) a series of hierarchically related PPs for the same type of TOE (one PP may be said to be hierarchic to another PP in the family if it includes all IT security requirements specified in the other PP);

b) a set of PPs that apply to different components of an IT system, e.g. a smartcard family might include PPs for the integrated circuit card, operating system, application, smartcard reader, and so on.

Where a PP family applies to a particular type of TOE, it is important that there is a clear distinction between different members of the family. In other words, there should be clear differences in the TOE security requirements; and it follows from this that the PPs should at least differ in their security objectives (which drive the selection of IT security requirements), if not the statement of TOE security environment. For example, consider the case where two PPs specify the same set of SFRs, but a different set of SARs. It may be possible to justify a lower assurance requirement by an increase in the environmental security. Such differences should be reflected in the security objectives.

Where a family of PPs applies to different components of an IT system (whether in a specific or assumed environment), the relationship between the PPs should be made clear. See also Clause 14 of this Technical Report, which discusses issues relating to definition of PPs for components of an IT system.

7 Descriptive parts of the PP and ST

7.1 Introduction

This clause provides guidance on the construction of the purely descriptive parts of a PP and ST, namely:

a) the PP and ST Introduction;

b) the TOE Description in a PP or ST;

c) PP application notes.

7.2 Descriptive parts of a PP or ST

7.2.1 The Introduction

7.2.1.1 Identification

The intent of this section is to provide sufficient identification information to uniquely identify the PP or ST, possibly for the purposes of registration of a PP or for an ST to be able to include it on a list of products that have been evaluated. As a minimum this will include the PP or ST name with an identifier that is unique to that

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

version of the PP or ST, and an identifier for the TOE (e.g. name and version number). The following information may also be useful (or may be required by a PP registry or list of evaluated products):

a) key words (e.g. security features or functionality to identify or search a registry or products list);

b) an assurance package may also be specified (e.g. as an EAL if applicable).

ISO/IEC 15408 does not dictate where in the *Introduction* the EAL (if any) should be included, but it is recommended that the Assurance package or EAL used be placed here, as it plays a prominent role in international mutual recognition.

The date of the version of ISO/IEC 15408 used to develop the PP or ST needs to be included in the *Identification* for reasons of version control, although ISO/ IEC 15408 does not explicitly call for it. Similarly, details of any later criteria interpretations or supplements required by the PP or ST.

In an ST the inclusion of a CC conformance claim should also be placed in the introduction as it plays a prominent role in international mutual recognition, as enumerated in ISO/IEC 15408-1, 5.4.

7.2.1.2 Overview

According to ISO/IEC 15408, the *Overview* should be a summary of the PP or ST in narrative form, usable as a stand-alone abstract for use in PP catalogues and registers or ST in a list of evaluated products. A top-level overview of the security problem being solved with the PP or ST may be included and be sufficient for a potential consumer to determine whether the PP or ST is of interest. This overview has to be consistent with the technical content of the PP or ST.

7.2.2 TOE Description

The TOE Description should contain the following kinds of information (the first two are mandated by ISO/IEC 15408, the latter is suggested):

a) product or system type;

b) general TOE functionality;

c) TOE boundary (optional for PP).

The general TOE functional description is just that. It is not simply a description of TOE security features, unless the TOE is a special-purpose security product.

In a PP, the optional description of the TOE boundary tells the reader what is in the TOE and what is not. For an ST, the definition of the TOE boundary must be provided, both in a physical way (hardware and/or software components/modules) and in a logical way (IT and security features offered by the TOE).

You should ensure that the TOE description does not present an inaccurate or misleading picture of the intended usage of the TOE or its security functionality, e.g. describes security features or configurations that are not within the scope of the intended evaluation of the TOE.

7.2.3 Application notes

Application Notes are optional in a PP, and may either be included in a separate section, or they may be interspersed throughout the document, for example to accompany individual TOE security requirements. Application notes should be used to provide any supporting information that you consider relevant or useful for the construction, evaluation, or use of the TOE. A typical use of application notes is to provide clarifications of how particular security requirements are to be interpreted in the context of the TOE, or to provide advice to ST authors as to how operations on functional components might be completed in the ST.

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

If the application notes are integrated into text throughout the PP, it is recommended that individual application notes are clearly identified as such, so that the reader clearly understands that the text is informative and is not, for example, a refinement of an SFR or SAR.

8 The TOE security environment

8.1 Introduction

This clause provides guidance on the specification of the *TOE Security Environment* section of a PP or ST. ISO/IEC 15408-1 defines the requirements for the content of this part of a PP or ST in ISO/IEC 15408-1, B.2.4 and C.2.4. The wording of these two sections is identical, which can be taken as an indication that the expected content of the *TOE Security Environment* section does not differ greatly between a PP and an ST.

The purpose of the *TOE Security Environment* section is to define the nature and scope of the definition of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed, i.e. the 'security concerns', to be addressed by the TOE. This is illustrated in Figure 1 below.

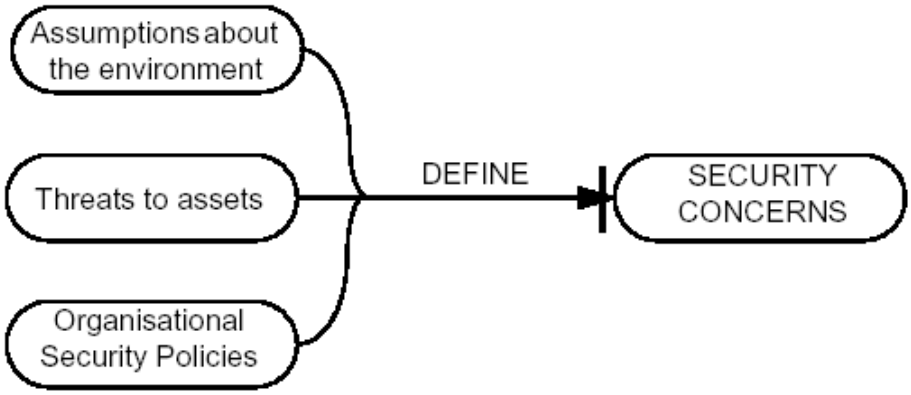

Figure 1 — Definition of the Security Concerns

This section will therefore involve a discussion of:

a) assumptions made regarding the TOE security environment, thereby defining the scope of the security concerns;

b) the assets requiring protection (typically information or resources within the IT environment or the TOE itself), the identified threat agents, and the threats they pose to the assets;

c) any organisational security policies or rules with which the TOE must comply in addressing the security concerns.

Subsequent sections of the PP and ST show how the security concerns will be addressed by the TOE, in combination with its operating environment. It is therefore important to ensure that the security concerns are clearly and concisely defined - otherwise you may end up with a PP and ST that addresses the wrong concerns.

As a general principle, the definition of the security concerns should avoid, where possible, any discussion of the form of the TOE's response to meeting the security concerns, 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 concerns. Discussion of how the security concerns are to be satisfied by the TOE should be left to the later parts of the PP or ST.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

8.2 How to identify and specify the assumptions

ISO/IEC 15408 requires the *TOE Security Environment* section of a PP or ST to contain a list of assumptions about the TOE security environment or the intended usage of the TOE. To compile such a list, you first need to ask the following question:

What assumptions am I making about the TOE security environment and the scope of the security concerns?

For example, it may be necessary to make some assumptions in order to ensure that a potential threat to an asset is not, in practice, relevant in the TOE security environment.

The following types of assumption should be included:

a) aspects relating to the intended usage of the TOE;

b) environmental (e.g. physical) protection of any part of the TOE;

c) connectivity aspects (e.g. a firewall being configured as the only network connection between a private network and a hostile network);

d) personnel aspects (e.g. the types of user roles anticipated, their general responsibilities, and the degree of trust assumed to be placed in those users).

Other assumptions may be included where these have had a material effect on the PP or ST content, for example assumptions which led to the choice of the assurance requirement. However, it must be remembered that ISO/IEC 15408 requires that the formally identified assumptions have to be shown to be upheld by the security objectives. General assumptions which cannot be traced to security objectives may nonetheless be usefully included within the descriptive (informative) text in the PP or ST.

It is unlikely that you will be able to completely identify all the assumptions you are making in a single attempt. Rather, you should expect to be identifying additional assumptions throughout the development of the PP or ST. In particular, when constructing the PP or ST rationale (e.g. demonstrating that the security objectives are suitable to counter the identified threats), you should consider whether you are making any assumptions that have not been stated in the PP or ST.

When adopting this iterative approach to identifying assumptions, it is important (in line with the general principle stated above) to carefully consider the inclusion of any ‘assumptions’ relating to the effective use of specific TOE security functions that you identify in the process of constructing the rationale. Such detail might be included as security requirements for the non-IT environment (see 10.4.2). It is, however, reasonable to state as a ‘personnel’ assumption that (for example) the TOE has one or more administrators who are assigned responsibility for ensuring the TOE security functions are configured and used appropriately.

For ease of reference, it is recommended that each assumption is numbered or otherwise uniquely labelled.

Example assumptions are presented in Annex B of this Technical Report.

8.3 How to identify and specify the threats

8.3.1 Overview

ISO/IEC 15408 requires that the PP or ST contains a description of *any threats to the assets against which protection will be required* (ISO/IEC 15408-1, B.2.4). However, ISO/ IEC 15408 goes on to say that the statement of threats may be omitted if the security objectives are derived solely from the organisational security policies (OSPs) and assumptions: in other words, where the ‘security concerns’ are defined in full by the OSPs and assumptions. This might be the case, for example, where an ST is being written in response to an RFP which defines those OSPs.

In practice, it is recommended that a statement of threats be included in the PP or ST as these generally provide a better understanding of the security concerns than a corresponding set of OSPs. Moreover, there is

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

a danger in relying on the OSPs alone, since they may not be up-to-date and accurately reflect the current threat. If you already have a comprehensive set of OSPs you are nonetheless encouraged to extrapolate the threats that they address in order to facilitate maximum reuse of the PP, as well as to convey a more thorough understanding of the security concerns.

The importance of risk analysis, to correctly identify the assets and the threats to those assets, should not be underestimated since if it is not done properly:

a) the TOE may provide inadequate protection, as a result of which the organisation's assets may be exposed to an unacceptable level of risk;

b) the threats may be over estimated, raising the cost of implementation and the assurance required in the implementation, and limiting potential solutions.

It should, however, be noted that ISO/IEC 15408 does not provide a framework for risk analysis or the specification of threats at an organisational level. Similarly, a detailed discussion of the process by which the threats to the assets are identified (which is one of the hardest parts of an organisation's risk analysis) is outside the scope of this Technical Report. However, for completeness, the general principles involved are stated below; see also ISO/IEC 15408-1, Clause 4. The reader is referred to standards such as [2] for more detailed guidance on this topic.

8.3.2 How should threats be identified?

8.3.2.1 What is a threat?

A 'threat' (as described in ISO/IEC 15408-1, 4.1.1) is simply an undesirable event, which is characterised in terms of *a threat agent, a presumed attack method, any vulnerabilities that are the foundation for the attack, and identification of the asset under attack* (ISO/IEC 15408-1, 4.3.1).

In order to identify what the threats are, you therefore need to answer the following questions:

a) what are the assets that require protection?

b) who or what are the threat agents?

c) what attack methods or undesirable events do the assets need to be protected from?

8.3.2.2 Identifying the assets

ISO/IEC 15408 defines *assets* as *information or resources to be protected by the countermeasures of a TOE* (ISO/IEC 15408-1, 2.3). They are so named because they have some intrinsic value to those who own those assets (whether individuals or organisations). By the same token, they are often of value to threat agents who may seek to compromise the assets of those assets, contrary to the wishes and interests of the owner, for example by causing loss of confidentiality, integrity, reliability, authenticity, accountability or availability of the assets.

The *assets* of concern to the PP or ST author may be a representation of the primary assets of the organisation (e.g. monetary value, or an organisation's personnel, customers, or reputation). In the context of the description provided in ISO/IEC 15408-1, 4.1.1, the *owners* of the assets should be understood as referring to those who are responsible for safeguarding the assets within the IT system (in which the TOE is deployed). In practice, the primary assets they represent may have multiple owners who differ from the owner of the TOE and of the information that the TOE contains. It may be helpful to the reader of a PP or ST to identify such primary owners when describing the assets. For example:

a) in a Trusted Third Party (TTP), different keys will have different owners, i.e. TTP subscribers as well as the owner of the TTP itself (see the worked example in Annex F and also [3] for additional information);

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

b) in the case of medical systems, it is commonly held that the TOE's information has no single owner, but rather consists of all those having an interest, due to the complex rules and considerations guiding its use and control.

ISO/IEC 15408 indicates that assets typically take the form of information which is stored, processed and transmitted by IT systems (ISO/IEC 15408-1, 4.1.2). It should be emphasised that the assets may be *external* to the TOE (but within the IT environment), as is the case with information and resources protected by firewalls or intrusion detection systems.

ISO/IEC 15408 suggests that the identified assets may also include such things as authorisation credentials and the IT implementation, which are indirectly subject to security requirements (ISO/IEC 15408-1, 4.3.1). Such 'assets' might be identified as part of the process of identifying the countermeasures needed to protect the primary assets (or their representation). Although permitted by ISO/IEC 15408, it is not (in general) recommended that you identify explicitly as assets information and resources that are introduced by the presence of the TOE itself, and which are only indirectly related to the primary assets. This is because the inclusion of such detail may:

a) obscure the primary purpose of the TOE (which is to protect the primary assets or their representation within the IT environment);

b) lead to the introduction of implementation detail (i.e. the solution to the defined security concerns) at too early a stage in the PP or ST, which will then be promulgated through to the threats and security objectives.

8.3.2.3 Identifying the threat agents

As described above, *threat agents* may either be human or non-human, although (as pointed out by ISO/IEC 15408-1, 4.1.1) in the domain of security greater attention is usually given to those threats that are related to malicious or other human activities.

In identifying who the human *threat agents* are, you should consider:

a) who might consider it worth their while to attempt to compromise the identified assets, for whatever reasons;

b) who would be in a position to attempt to compromise those assets - in other words, who could gain access to the IT systems which store, process or transmit the asset;

c) what is likely to be their level of technical expertise, opportunities, available resources (e.g. automated tools for hacking and probing networks) and motivation.

Non-human sources of threats, as well as threats *unintentionally* arising from human sources (i.e. by accident), should also be considered where these could lead to compromise of assets.

8.3.2.4 Identifying the attack methods

Having identified the assets to be protected and the threat agents, the next step is to identify the possible attack methods which could lead to a compromise of the assets. This will be based on what is known regarding the TOE security environment, for example:

a) potential vulnerabilities to the assets which a threat agent could exploit;

b) the capabilities of attackers who have access to the TOE security environment.

Potential vulnerabilities to an organisation's assets may be identified by a vulnerability analysis of the TOE security environment (note however that such an analysis is not within the scope of ISO/IEC 15408), taking into account the identified environmental assumptions. However, you should note that such an analysis may not identify all vulnerabilities, and should not therefore underestimate the possibility of new and undiscovered threats.

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

8.3.2.5 The role of risk analysis in threat identification

Risk analysis methods may be helpful in the process of threat identification, but such methods are not defined in ISO/IEC 15408. The risk analysis process is also likely to have a bearing on the identification of the security objectives for the TOE and its environment (see Clause 8), and the required level of assurance in the countermeasures proposed to address the threats (see Clause 9). Such methods may consider:

a) the probability and consequences of compromise of the assets, taking into account:

- the possible attack methods identified,
- the likelihood of the attack proving to be successful, and
- the consequences of any damage that may be caused (including the expected magnitude of tangible loss arising from a successful attack);

b) other constraints such as legal requirements and cost.

8.3.3 How should threats be specified?

Having identified the threats to be addressed by the TOE or its environment, the next step is to specify them in the PP or ST. As noted above, the *TOE Security Environment* section should be a clear and concise statement of the security concerns, and a clear and concise specification of threats is an essential part of this.

In order to provide a *clear* specification of a threat, you should include the following details (identified as described in 8.3.2 above):

a) the threat agent (e.g. an authorised user of the TOE);

b) the assets subject to the attack (e.g. sensitive data);

c) the attack method employed (e.g. impersonation of an authorised user of the TOE).

For example:

An attacker may gain unauthorised access to information or resources by impersonating an authorised user of the TOE.

An authorised user of the TOE may gain unauthorised access to information or resources by impersonating another authorised user.

It will help the reader to understand the threat if the threat description is accompanied by an explanation of any terms used within the description of the threat, and the scope of the threat in terms of the assets at risk of compromise and specific attack methods that the threat agent might use. For example, in the case of the threats above it may be usefully clarified that the assets at risk are the information and resources which the (impersonated) user has the right to access; or (from a number of different approaches) how impersonation might be achieved.

In order to help ensure you have a *concise* statement of threats, as far as possible the threat descriptions should be *disjoint*. In other words, there should be minimal overlap between different threats. This will help avoid potential confusion on the part of the reader of the PP or ST as well as helping to simplify the PP or ST rationale by avoiding needless repetition.

Overlap between threats can be more easily avoided if you specify all threats at the same level of detail. For example, don't specify a threat describing a detailed attack method against a specific asset if this is a specific attack scenario that is already associated with a more general threat stated elsewhere in the PP or ST.

Each threat should be uniquely labelled for ease of reference (for example, in those parts of PP rationale which show how the specified security objectives address the threats). Possible options are:

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

a) sequential numbering of threats (e.g. T1, T2, T3, and so on);

b) a unique label providing a brief but meaningful 'name' for the threat (e.g. as used in the example threats given in annex B).

The advantage of the first option is that a simple number is generally short and easy to use for reference purposes. The advantage of the second option is that the label is more likely to be meaningful and memorable as a standalone identifier. However, when using the second option it may not be possible (due to practical constraints limiting the number of characters in the label) to assign a fully defined label in all cases, however, the label should accurately reflect the intent.

The threat descriptions should only refer to potential events which could *directly* compromise the assets requiring protection. It is therefore recommended that you do not include 'threats' of the form *There may be security flaws in the TOE.* Such a 'threat' does not help the reader to understand what the security need is, especially since it applies to any TOE. Moreover, it is not an event that can actually be addressed by the TOE or by any non-technical measures that can be taken within the TOE security environment; rather, it can only be addressed by actions taken by those who develop and evaluate the TOE.

The introduction of countermeasures to the threats may introduce detailed attacks that may lead indirectly to compromise of the assets, for example bypassing or tampering attacks against the TOE security functions. Caution is advised when considering such *indirect* threats to the assets; in particular you should ensure that any such threats:

a) will not, as a result of their inclusion in the *TOE Security Environment* section, confuse the reader by anticipating details of the TOE implementation;

b) do not already fall within the scope of an existing threat.

For example, if threat X could compromise asset Y, then it follows that any attempt to bypass the countermeasure to threat X may also lead to compromise of asset Y. Therefore, bypass of the countermeasure to threat X may be an attack method that is already implicitly within the scope of threat X, and hence (for the sake of brevity in the statement of TOE security environment) does not need to be stated explicitly as a separate threat.

(It should also be noted that you will need to consider attacks against the countermeasures of the TOE, such as bypassing and tampering, when you come to select the IT security requirements, which ISO/IEC 15408 requires to be mutually supportive: see 13.3.4. Any feasible attacks against the TOE security functions should also be discovered during the evaluation of the TOE.)

Example threats are presented in Annex B of this Technical Report.

8.3.4 Completing the statement of threats

ISO/IEC 15408 requires the *TOE Security Environment* section to include all threats to the assets that are relevant for secure TOE operation (ISO/IEC 15408-1, B.2.4). The threats that are of principal interest are those that will be countered by the TOE (which will often be in association with procedural or other non-technical countermeasures). However, for completeness, the PP or ST may need to include some threats that are not at all addressed by the TOE, for example because of attack methods or threat agents against which the TOE offers no protection.

Examples of threats that are relevant to secure operation of the TOE, but which might not be addressed by the TOE, might include:

a) physical attack against the TOE;

b) abuse of trust by highly privileged users;

c) improper administration and operation of the TOE by careless or improperly trained administrators.

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

The decision as to which threats are to be addressed by the TOE, and which (if any) are only addressed by the environment, will not (of course) be made until the security objectives are finalised.

It should be noted that the identified environmental assumptions may preclude certain threats that would otherwise have been considered relevant to the secure operation of the TOE. It follows from this that the PP or ST author has a certain amount of freedom in deciding whether such aspects are dealt with in the environmental assumptions or in the statement of threats to be countered by the operating environment. Either approach is acceptable since both assumptions and threats have to be mapped onto the security objectives which uphold or address them. The choice between these two alternatives should therefore be made on the basis of which approach best helps the reader to understand the security concerns. As a general rule, specific attacks should be handled as threats, whilst more general forms of attack may be best handled as assumptions. Whichever approach is adopted, however, it is important that the issue is only stated once.

8.4 How to identify and specify the Organisational Security Policies

ISO/IEC 15408 requires the *TOE Security Environment* section to contain a description of any OSPs with which the TOE must comply (ISO/IEC 15408-1, B.2.4). However, ISO/ IEC 15408 goes on to say that the statement of OSPs may be omitted if the security objectives are derived solely from the threats and assumptions: in other words, where the 'security concerns' are defined in full by the threats and assumptions.

As indicated in 8.3 above, a PP and ST author should review any OSPs against the existing and relevant threats to the assets before including them in the PP or ST.

An OSP is defined as one or more rules, procedures and practices imposed by an organisation (ISO/IEC 15408-1, 2.3). An OSP may need to be applied by the TOE or its environment, or by some combination of the two.

If your PP or ST specifies OSPs as well as threats, you should remember the requirement that the *TOE Security Environment* section provide a concise statement of the security concerns: little useful purpose is served by including an OSP which is simply a restatement of a threat in a different form (unless of course you have no choice in the matter because the relevant organisation mandates an OSP which is a restatement of an existing threat).

For example, if you have identified a threat which states 'An unauthorised person may gain logical access to the TOE' then there is little to be gained from including an OSP which states 'Legitimate users of the TOE must be identified before TOE access can be granted'.

This OSP does not only (in effect) restate the threat in a different form, it also pre-empts the definition of security objectives which provide the intended response to the security concerns. Your PP or ST will be easier to follow if you only state the problem once.

As a general rule, it will be appropriate to specify OSPs where the TOE is intended for use by a specific organisation or a type of organisation, or where there is a need for the TOE to implement a set of rules that cannot be sensibly included within or implied by a threat description. Examples include:

a) identification of information flow control rules to be applied;

b) identification of access control rules to be applied;

c) definition of an organisation's security policy with respect to security audit;

d) solution techniques mandated by the organisation, e.g. use of specified approved cryptographic algorithms, or conformance with identified standards.

As with the threats, each OSP should be uniquely labelled for ease of reference.

Example OSPs are presented in Annex B of this Technical Report.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

9 The security objectives

9.1 Introduction

This clause provides guidance on the identification and specification of security objectives in a PP or ST, the requirements for which are described in ISO/IEC 15408-1, B.2.5 and C.2.5.

The *security objectives* provide a *concise statement of the intended response to the security problem* (ISO/IEC 15408-3, 4.4). In other words, having stated (in the *TOE Security Environment* section) what the security concerns are, you now need to give an indication of the extent to which they will be addressed by the TOE and its environment, in the form of a statement of security objectives. This is illustrated in Figure 2 below.

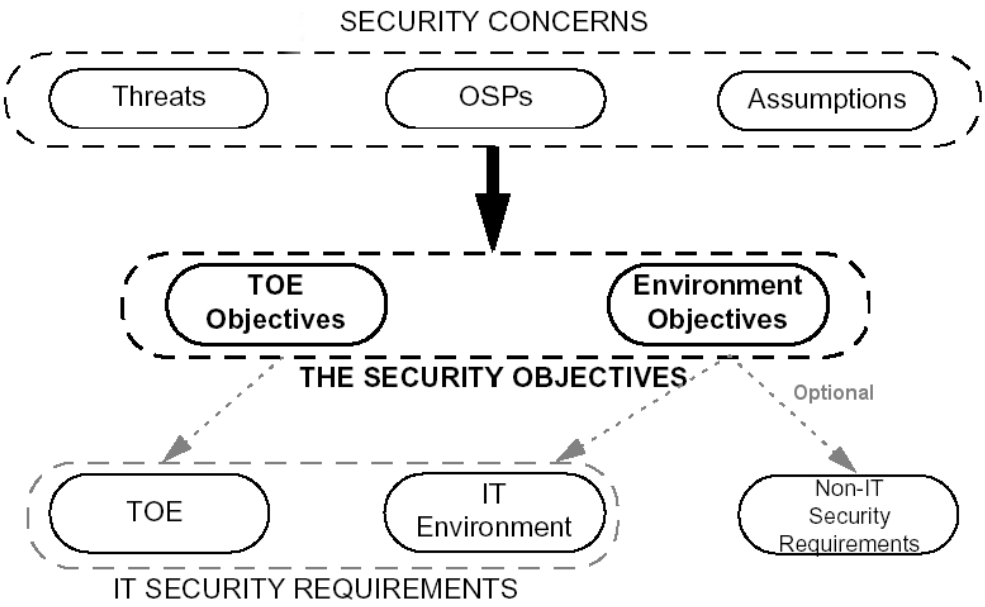

Figure 2 — Role of the security objectives

Figure 2 illustrates the two types of security objectives which ISO/IEC 15408 requires to be clearly distinguished in a PP or ST:

a) Security objectives for the TOE, which will be satisfied by technical (IT) countermeasures implemented by the TOE;

b) Security objectives for the environment, which are to be satisfied by either technical measures implemented by the IT environment, or by non-IT (e.g. procedural) measures.

Thus the statement of security objectives serves to outline what the TOE will and will not do within the context of the TOE security environment. By clearly dividing responsibility for meeting the security concerns between the TOE and its environment, the risk to the assets requiring protection can be mitigated. Furthermore, in defining this division of responsibility, the statement of security objectives will scope the evaluation of the TOE; this is because the security objectives for the TOE drive both the selection of security functional requirements that are needed to fulfil the TOE's responsibilities in meeting the security concerns, and also the determination of the level of assurance needed in the security functions required of the TOE.

9.2 How to specify security objectives for the TOE

The security objectives for the TOE states what the responsibility of the TOE is in countering the threats and in supporting the OSPs. As illustrated in Figure 2, the security objectives for the TOE may be viewed as

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

providing the reader with a 'stepping stone' (or bridge) from the identified security concerns to the IT security requirements, and this should always be borne in mind when specifying the security objectives for the TOE.

Because of the pivotal role played by the security objectives in the PP or ST, the question of what level of detail is appropriate in a statement of security objectives is important. ISO/IEC 15408 gives a strong hint by saying (as pointed out above) that security objectives are intended to be *concise.* In practice, you need to strike a balance between the following two considerations:

a) The security objectives should help the reader to understand the extent to which the security concerns are to be addressed by the TOE, without delving into implementation detail; ideally, the security objectives for the TOE should be implementation-independent. The focus is thus on *what* the solution intends to achieve rather than *how* it is achieved.

b) At the same time, you should ensure that the defined security objectives do not just repeat the information contained within the threats and OSPs (albeit in a slightly different form).

The test of whether you have pitched your security objectives at the right level of detail will ultimately come when you construct the rationale for the security objectives and the IT security requirements. If one step in the rationale is trivial whilst the other is comparatively difficult, it is likely that your security objectives are either too detailed or too abstract, depending on which step is the easier.

As will become clear in the next clause of this Technical Report, a well-defined set of security objectives for the TOE will help ensure that the IT security requirements selected to meet them are not excessive - either in terms of the security functional requirements (see 10.2.1) or the security assurance requirements (see 10.3.1). This in turn will serve to minimise the cost and timescales of the TOE evaluation.

Broadly speaking, three types of security objective can be identified to address the identified threats:

a) *preventive* objectives, which prevent a threat from being carried out, or limit the ways in which it can be carried out;

b) *Detective* objectives, which provide the means to detect and monitor the occurrence of events relevant to the secure operation of the TOE;

c) *Corrective* objectives, which require the TOE to take action in response to potential security violations or other undesirable events, in order to preserve or return to a secure state and/or limit any damage caused.

An example of a *preventive* security objective is the following, which identifies the need for identification and authentication of users of the TOE:

The TOE will ensure that each user is uniquely identified, and that the claimed identity is authenticated, before the user is granted access to the TOE facilities.

Access control and information flow control security objectives also fall into the *preventive* category. Where the security concerns indicate that the TOE should enforce more than one access control or information flow control policy, it is recommended that you identify distinct security objectives for each policy. Such an approach will help simplify the security requirements rationale.

An example of a *detective* security objective is the following, which identifies the need for the TOE to provide a non-repudiation of origin capability:

The TOE will provide the means by which a recipient of information can generate evidence which can be used as proof of the origin of that information.

An example of a *corrective* security objective is the following, which identifies the need for the TOE to respond to detected intrusions:

The TOE will, upon detection of events that are indicative of an imminent security violation, take appropriate steps to curtail the attack with a minimum of disruption to the service provided to other TOE users.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

Where possible, the security objectives should aim to informally quantify the minimal effectiveness expected, thus leaving little doubt as to what level of effectiveness must be justified in the PP or ST rationale. Quantities may be stated:

a) in relative terms, e.g. to environmental conditions or to a previous situation;

b) in absolute numeric terms.

Clearly, specifying absolute numeric values is the most precise option, but is also the most difficult to assess in terms of effectiveness.

If your PP or ST is being written where the SFRs are already known, a useful starting point may be to define one security objective for the TOE corresponding to each of the major groupings of security functional requirements that will be specified in the PP or ST. One benefit of this approach will be to simplify the construction of the security requirements rationale. If this approach is adopted, you still ensure that the defined security objectives comply with the guidance in this section. In particular, you should ensure that the security objectives do not contain unnecessary implementation detail.

Examples of security objectives are provided in Annex B of this Technical Report.

ISO/IEC 15408 requires that security objectives for the TOE are clearly traced to the relevant threats and OSPs (ISO/IEC 15408-1, B.2.5). Therefore, you need to ensure that:

a) each identified threat to be countered in full or in part by the TOE is addressed by at least one security objective for the TOE;

b) each identified OSP to be met in full or in part by the TOE is addressed by at least one security objective for the TOE.

This traceability may be provided (for example) by means of textual cross-references or by mappings in tabular form. Whilst the information required may be provided in the rationale (see Clause 13), it may be more helpful to the reader of the PP or ST if the mappings are provided in the security objectives section. Where a security objective is included to comply with an OSP, it may be appropriate to reference the OSP rather than repeat in full the rules to be implemented (e.g. as with O.DAC in the examples in Annex B).

As with threats and OSPs, the security objectives for the TOE should be uniquely labelled for ease of reference. Again, the labelling convention may be based on sequential numbering (e.g. O1, O2, O3, and so on) or the use of brief but meaningful names (e.g. as in the examples presented in Annex B).

9.3 How to specify security objectives for the environment

The *security objectives for the environment* include any security objectives that are to be satisfied by the IT environment, as well as by procedural or other non-technical measures to be implemented within the operating environment of the TOE. In other words, security objectives for the environment can either be IT or non-IT.

Security objectives for the environment will have to be identified to address those aspects of the security concerns that the TOE will not (or cannot) be expected to do. In particular, security objectives for the environment will be needed to:

a) counter threats (or aspects of threats) that are not countered by the TOE;

b) help satisfy OSPs that are not fully satisfied by the TOE;

c) support the identified security objectives for the TOE by helping to counter the threats or satisfy the OSPs;

d) ensure that identified environmental assumptions are satisfied.

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

An appropriate starting point to the identification process might therefore be to compile a list of security objectives by taking each threat, OSP and assumption that is not to be fully addressed by the TOE in turn, and for each such aspect of the TOE security environment to either:

a) add a new security objective to the list to address that aspect; or

b) map an existing security objective to that aspect if an appropriate one has already been identified (possibly rewording the security objective to extend its scope).

This list should then be refined when you formulate the security objectives rationale, since this may lead to the identification of additional security objectives that are needed to ensure that the security concerns are suitably met (in terms of the threats to be countered and the OSPs and assumptions to be covered).

The identification process should be carried out in conjunction with the identification of security objectives for the TOE. The statement of security objectives as a whole should then be reviewed to ensure that the division of responsibilities between the TOE and its environment is appropriate, i.e. such that:

a) the security objectives for the TOE will not lead to a set of IT security requirements for which the cost of implementation and evaluation is disproportionate to the value of the assets being protected;

b) the security objectives for the environment will not lead to a set of procedural or other non-IT security requirements that will be impractical to implement, or will be unduly restrictive to the TOE users.

Typical examples of (non-IT) security objectives for the environment include:

a) establishment and implementation of procedures to ensure that the TOE will be used in a secure manner (and in particular in accordance with the environmental assumptions);

b) objectives for education and training of administrators and users in sound security practices.

The statement of security objectives for the environment should therefore include any security objectives relating to management activities needed to ensure that the security services to be provided by the TOE are effective. In some cases, the required management activity is obvious, and can be conveniently expressed in the form of a (non-IT) security objective for the environment (e.g. regarding the need for proper management of the audit functions). In other cases the required management activity may depend on the detailed security requirements used to implement the TOE security objectives. For example, the 'identification and authentication' security objective of 9.2 above might be implemented by user passwords. This would imply a requirement for users to ensure their passwords are not disclosed to other individuals, which would properly be expressed as a security requirement for the non-IT environment (see 10.4.2) which refines the security objective for the environment.

ISO/IEC 15408 states that when a threat or OSP is to be covered partly by the TOE and partly by its environment, the related security objective is to be repeated in each category (ISO/IEC 15408-1, B.2.5). This might be appropriate in the case of the identification and authentication security objective identified above, where the relevant threat can only be countered by the TOE with appropriate support from management activity within the environment, e.g. management of authentication data such as passwords. Thus the security objective might be stated in the following terms:

The TOE, with support from its environment, will ensure that each user is uniquely identified, and that the claimed identity is authenticated, before the user is granted access to the TOE facilities.

In cases where it is possible to clearly divide responsibility between the TOE and its environment, such repetition of security objectives in both categories will clearly not be necessary. An example would be the identification of security objectives for security audit, where the TOE is assigned responsibility for generating and collecting the data, and the environment is assigned responsibility for the supporting management activity, e.g. analysis of the data generated.

A typical example of an IT security objective for the environment is a security objective for an underlying operating system to identify and authenticate TOE users. (Such dependencies on the IT environment will be

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

refined in the IT security requirements for the environment: see 10.4.1). As with the security objectives for the TOE, it is recommended that the security objectives for the environment are uniquely labelled for ease of reference. It may be helpful if you adopt a labelling convention which clearly distinguishes security objectives for the environment from the security objectives for the TOE. If a numbering convention is used, there should be separate numbering for the two types of security objective (for example, security objectives for the environment could be numbered OE1, OE2, OE3, and so on).

Example environmental security objectives are presented in Annex B of this Technical Report.

10 Security requirements

10.1 Introduction

This clause provides guidance on the specification of IT security requirements in a PP or ST. This guidance applies to both TOE security requirements and to security requirements for the IT environment. Security requirements for the non-IT environment (not required to be a formal part of a PP or ST) are also briefly discussed.

The following types of IT security requirements are specified in a PP or ST:

a) Security Functional Requirements (SFRs) on the TOE. These identify the requirements for security functions which the TOE must provide to ensure that the security objectives for the TOE are achieved.

b) Security Assurance Requirements (SARs) on the TOE. These identify the required level of assurance in the implementation of the SFRs.

c) Security Requirements on the IT environment. (These are optional in PP or ST.) These define any functional and assurance requirements to be satisfied by the IT environment (i.e. by hardware, firmware and/or software external to the TOE), which are needed in order to ensure that the security objectives for the TOE are achieved.

This is illustrated in Figure 3 below.

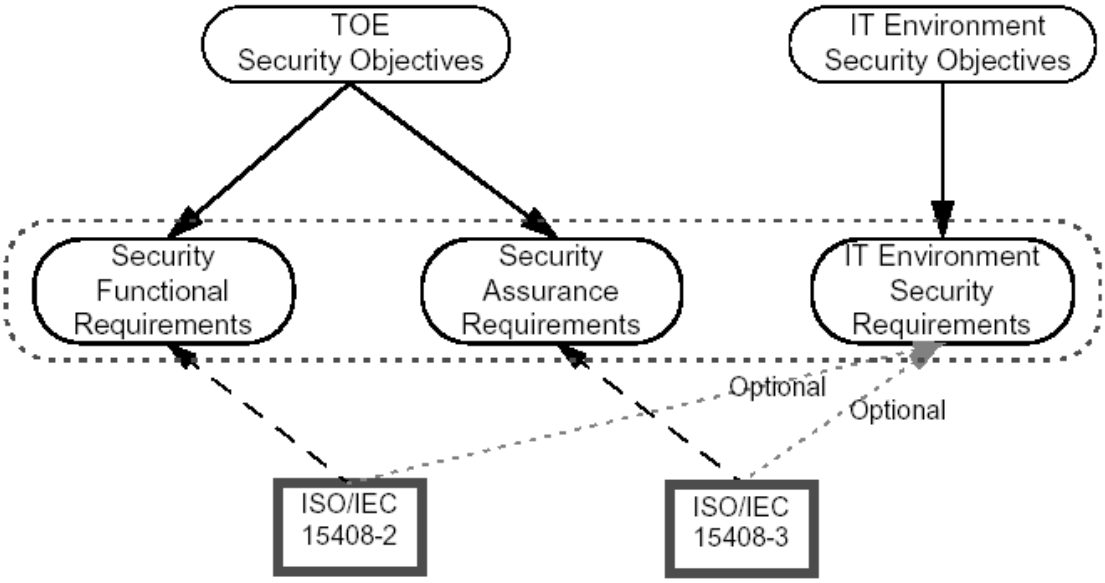

Figure 3 — Derivation of IT security requirements

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

In addition to functional and assurance requirements, the IT security requirements section of a PP or ST is required (where appropriate) to specify a minimum strength of TOE security function level, with explicit strength claims where relevant (see ISO/IEC 15408-1, B.2.5 and C.2.5).

As Figure 3 shows, a significant characteristic of the IT security requirements is that they are intended to be constructed, where possible, using the catalogue of functional components defined in ISO/IEC 15408-2 and the catalogue of assurance components defined in ISO/IEC 15408-3, as appropriate. The intent of ISO/IEC 15408 here is to ensure a degree of standardisation in the way the IT security requirements are presented. The use of this 'common language' for expressing IT security requirements is thus intended to facilitate comparison between PPs and STs.

However, ISO/IEC 15408 recognises that there may be cases where there is no appropriate functional or assurance component in ISO/IEC 15408-2 or ISO/IEC 15408-3. In this case, the IT security requirements may be stated explicitly without reference to ISO/IEC 15408; however, such IT security requirements must be unambiguous, evaluatable, and expressed in a similar style to existing ISO/IEC 15408 components. 10.2.8 provides guidance where no appropriate functional components can be identified in ISO/IEC 15408-2; 10.3.3 provides similar guidance in respect of assurance components.

ISO/IEC 15408 permits a degree of flexibility in the way the SFRs and SARs are specified by allowing a set of *operations* to be performed on them to tailor the security requirement appropriately - namely assignment, iteration, selection and refinement. 10.2.2 below provides guidance on the use of operations on ISO/IEC 15408 functional components. 10.3.2 does the same for ISO/IEC 15408 assurance components.

Each security component in ISO/IEC 15408-2 and ISO/IEC 15408-3 is assigned its own unique reference in ISO/IEC 15408, based on a defined taxonomy.

a) in ISO/IEC 15408-2, for example, component FAU_GEN.1.2 has the following meaning:

- 'F' indicates it is a *functional* requirement;
- 'AU' indicates it belongs to the *security audit* class of SFRs;
- 'GEN' indicates it belongs to the *security audit data generation* family within that class;
- '1' indicates it is the *audit data generation* component within that family;
- '2' indicates it is the second *element* within that component.

b) the components in ISO/IEC 15408-3 use a similar taxonomy, but additionally identifies each *element* as belonging to one of three sets of *assurance elements*, by appending a letter:

- the letter 'D' indicates it belongs to the set of *developer action elements,* the activities performed by the developer;
- the letter 'C' indicates it belongs to the set of *content and presentation elements,* the information the evidence is meant to convey;
- the letter 'E' indicates it belongs to the set of *evaluator action elements*, the activities performed by the evaluator.

c) in ISO/IEC 15408-3, for example, component ADV_HLD.1.2C has the following meaning:

- 'A' indicates it is an *assurance* requirement;
- 'DV' indicates it belongs to the *development* class of SARs;
- 'HLD' indicates it belongs to the *high level design* family within that class;
- '1' indicates it is the *descriptive high-level design* component within that family;

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

- '2' indicates it is the second *element* in a set of *assurance elements*;

- 'C' indicates it is an *element* in the set of *content and presentation elements* within that component.

SFRs and SARs are selected at the *component* level: all defined elements within that component have to be included in the PP or ST if the component is to be included. There are two types of *relationships* between components which you need to be aware of, as these have a bearing on the process of selecting the IT security requirements:

a) Components within a family may have an *hierarchic* relationship, indicating that one component includes all requirement elements specified in another component in that family. For example, FAU_STG.4 is hierarchic to FAU_STG.3 because all functional elements defined in the latter are also included in the former. However, FAU_STG.4 is not hierarchic to FAU_STG.1, and it is therefore possible to include both components in the same PP or ST.

b) Components may have defined *dependencies* on any component in any other family. For example, FIA_UAU.1 (which requires authentication of any user's claimed identity) has a dependency on FIA_UID.1 (which requires users to be identified). These components must also be included in a PP or ST, unless the dependencies can be shown not to be relevant to the threats and security objectives.

10.2 How to specify security functional requirements in a PP or ST

10.2.1 How should security functional requirements be selected?

Having defined the security objectives for the TOE in response to the identified security concerns, you now need to elaborate on how these security objectives are to be met. This is done by selecting an appropriate set of SFRs which, as stated above, is done at the *component* level. Of course, the SFR selection process will be significantly easier if pre-defined functional packages are available that are relevant to the security objectives for the TOE (see Clause 15).

There are several stages to the process of selecting the SFRs for a PP or ST. In considering the selection process, it is helpful to distinguish between the following two types of SFR:

a) *principal* SFRs, which *directly* satisfy the identified security objectives for the TOE;

b) *supporting* SFRs, which do not *directly* satisfy the security objectives for the TOE, but which nonetheless provide support to the *principal* SFRs, and hence *indirectly* help satisfy the relevant security objectives for the TOE.

Whilst ISO/IEC 15408 does not *explicitly* distinguish between these two types of SFRs, such a distinction is *implicit* in the consideration of such things as dependencies between functional components, and the demonstration of mutual support between SFRs. Therefore, whilst there is no need for you to explicitly categorise the SFRs as *principal* or *supporting* in the PP or ST, recognising that there are these two types of SFR will be of significant benefit when you come to write the PP or ST Rationale.

The first stage in the SFR selection process is thus, for each security objective for the TOE, to identify the *principal* SFRs which directly satisfy them. Once a complete set of *principal* SFRs has been established, there then follows an iterative process whereby the complete set of *supporting* SFRs are identified. As described above, all SFRs (whether *principal* or *supporting*) should, where possible, be expressed using appropriate functional components from ISO/IEC 15408-2. Annex B provides guidance identifying which functional components should be used to express common security functional requirements. When selecting functional components from ISO/IEC 15408-2, you should also consult the guidance contained in the annexes to ISO/IEC 15408-2 as to whether the component would be appropriate, and how it should be interpreted.

The relationship between these two types of SFR is illustrated in Figure 4. It may be noted that this relationship is relevant to the PP or ST rationale, which, *inter alia*, is required to demonstrate mutual support between the SFRs (see 13.3.4). This will involve providing an explanation of the nature of the support provided by *supporting* SFRs in helping to ensure that the security objectives for the TOE are met.

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

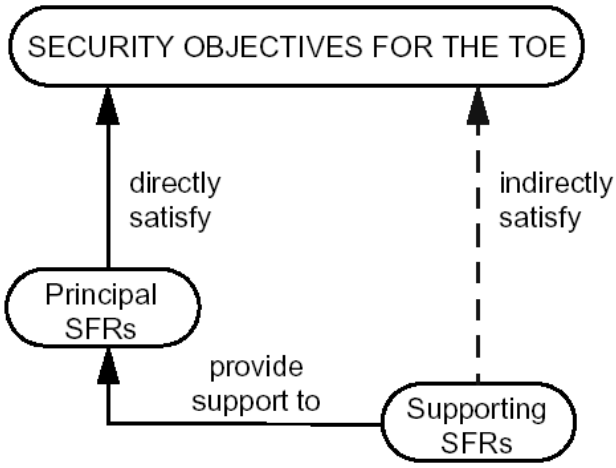

Figure 4 — Role of principal and supporting SFRs

There are three stages involved in identifying the complete set of *supporting* SFRs:

a) Identify the additional SFRs needed to satisfy (where you consider it appropriate) the dependencies (as defined in ISO/IEC 15408-2 for the relevant functional components) of all *principal* SFRs. This includes any dependencies of the *supporting* SFRs identified during this stage.

b) Identify any additional SFRs that are necessary to ensure that the security objectives for the TOE are achieved. This will include SFRs needed to defend the *principal SFRs* against composite attacks that first defeat the function, then mount the threat the function is intended to counter.

c) Identify the additional SFRs needed to satisfy (where you consider it appropriate) the dependencies of those *supporting* SFRs selected during the second and third stages.

The identification of *supporting* SFRs to satisfy the dependencies as identified in ISO/IEC 15408-2 is likely to be an iterative process, for example:

a) Suppose that the PP or ST includes a security objective requiring the TOE to provide specific responses to the detection of events indicative of an imminent security violation. This leads to the inclusion of a *principal* SFR based on the FAU_ARP.1 (Security Alarms) component.

b) According to ISO/IEC 15408-2, FAU_ARP.1 has a dependency on FAU_SAA.1 (Potential Violation Analysis) which should also be included as a *supporting* SFR.

c) FAU_SAA.1 has a dependency on FAU_GEN.1 (Audit Data Generation).

d) FAU_GEN.1 has a dependency on FPT_STM.1 (Reliable Time Stamps).

e) FPT_STM.1 introduces no requirements for additional functional components.

It should be noted that ISO/IEC 15408 permits you to leave some dependencies ‘unsatisfied’, provided you explain why the relevant SFRs are not required to satisfy the security objectives (and hence address the security concerns).

Dependencies should be applied in a consistent manner. For example, in the case of FAU_ARP.1, consistency is ensured by the nature of the requirements (FAU_ARP.1 depends on the expectation of a potential security violation that is defined by application of FAU_SAA.1.2).

For other components, consistency may be more problematic. For example, in the case of FDP_ACC.1, the PP or ST will identify the particular access control SFP to which it relates. In satisfying the dependency of

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

FDP_ACC.1 on FDP_ACF.1, it must be ensured that FDP_ACF.1 is applied to the same access control SFP that was used for FDP_ACC.1. If the iteration operation is applied to FDP_ACC.1 for different access control SFPs, the dependency on FDP_ACF.1 will need to be satisfied in respect of each such access control SFP.

The identification of additional *supporting* SFRs (i.e. those that are not identified as dependencies in ISO/IEC 15408-2) involves identifying any other SFRs which you consider to be necessary to support the achievement of the security objectives for the TOE. Such SFRs will typically provide support by reducing the options or opportunities available to an attacker, or by increasing the level of expertise or resources an attacker must have to mount a successful attack. The following should be considered in the light of the security concerns and the security objectives:

a) SFRs based on relevant components from the same class in ISO/IEC 15408-2. For example if the component FAU_GEN.1 (Audit Data Generation) is included then this may imply a need to create and maintain a secure audit trail to store the data generated (requiring one or more functional components from the FAU_STG family) and a need for tools to review the generated audit data (requiring one or more functional components from the FAU_SAR family). Alternatively, the generated data may be exported to another system for review.

b) SFRs based on relevant components from the FPT (Protection of the TOE Security Functions) class. Such SFRs will typically protect the integrity and/or availability of the TSF or TSF data on which the other SFRs rely, although they may protect its confidentiality as well. Examples include FPT_AMT.1 (Abstract Machine Testing) and components from the FPT_SEP (Domain Separation) family, which may be required to support the security objectives where there is an identified need to protect the TSF against such things as TSF failure, corruption, or modification (possibly by malicious means).

c) SFRs based on relevant components from the FMT (Security Management) class. These components will be used to specify any necessary supporting security management SFRs. An example of this would be FMT_REV.1 which addresses the revocation of security attributes, and may be considered relevant where SFRs are included that deal with security attributes (e.g. access control).

The selection of these *supporting* SFRs should always be done in light of the security objectives, in particular taking into account the need to end up with a set of SFRs which form a mutually supportive and integrated and effective whole. The process of constructing the PP or ST rationale may therefore have a significant influence on this selection process. You are strongly advised to avoid including *supporting* SFRs that are not needed to achieve the security objectives, because this will only serve to limit the acceptability of the PP or ST given that:

a) some TOEs may not be able to meet such SFRs;

b) increasing the number of SFRs will increase the cost and maintenance of unneeded requirements in evaluation.

If the PP or ST is being constructed using a related PP as a basis, the process for selection of SFRs should be simplified considerably. The PP or ST being constructed should include different SFRs, where appropriate, taking into account any differences between the TOE security environment and/or security objectives.

10.2.2 How to perform operations on security functional requirements

10.2.2.1 Permitted operations

As stated in 10.1 above (see also ISO/IEC 15408-2, 2.1.4), some functional components include permitted operations which may require the PP or ST author to tailor the security requirement as appropriate for the PP or ST. These operations are:

a) *assignment*, allowing the specification of an identified parameter;

b) *iteration*, allowing multiple use of the same functional component to express different requirements;

c) *selection*, allowing the specification of one or more elements from a given list;

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

d) *refinement*, allowing the addition of details to the security requirement, thereby restricting the set of acceptable solutions without introducing any new dependencies on other SFRs.

10.2.2.2 Iteration

The *iteration* operation is often needed to express SFRs using components in the FMT (Security Management) class, which are called up as dependencies by many different functional components in ISO/IEC 15408-2. In order to satisfy such dependencies, it will typically be necessary to use the same component, with the assignment and selection operations completed differently. For example, FMT_MSA.1 may be iterated a number of times to define distinct SFRs relating to the management of different types of security attributes. Similarly, it may be desirable to make multiple use of components from the FDP_ACC and FDP_ACF families in the case where a TOE is required to enforce different access control policies, e.g. Discretionary Access Control (DAC) and Role Based Access Control (RBAC).

You are encouraged to use the iteration operation where the clarity of the PP or ST can be enhanced, e.g. to break down a complex and unwieldy SFR into distinct and manageable functional requirements. Use of the iteration operation does, however, pose other potential problems when presenting the SFRs in the PP or ST, as will be seen in 10.2.9 below.

For each SFR you have included in the PP or ST, you need to make a judgement as to whether to:

a) complete any *assignments* or *selections* included in the functional component used to express the SFR;

b) specify any *refinement* of the SFR.

10.2.2.3 Assignment and selection

In assignment there is the possibility that the value of the parameter may be null, whereas with a selection there is always at least one value of the parameter identified. By completing an assignment or selection operation in a PP removes any decision by the ST author as to how the functional component is to be tailored to meet the security objectives (other than the possibility of refinement). In other words, there are no aspects (insofar as the operation is concerned) that are ‘to be defined’ by the ST author.

Generally individual *assignments* or *selections* will require completion by the PP or ST author. Over-qualification through completion of operations, or too much detail, may unduly restrict the number of TOEs that might be able to claim conformance with the PP or ST. The balance of completing operations is based on the need for a PP to be:

a) a complete set of the requirements of the author;

b) *implementation-independent*;

c) sufficiently detailed to demonstrate that the objectives are met.

Therefore, it is necessary to complete assignment and selection operations to the extent needed to meet the security objectives. A critical test will come when you construct the security requirements rationale: the arguments you present to demonstrate the suitability of the IT security requirements to meet the security objectives should not rely on details that have not been specified in the SFRs. For example, in the case of an access control SFR based on FDP_ACF.1, you may consider it appropriate to leave the specification of access control rules entirely in the hands of the ST author if such rules are already defined in an OSP which the relevant (access control) security objective is intended to meet.

One technique that you may use in order to solve the above problem is that of *partially* completing the operations. By adopting this approach you can give maximum flexibility to the ST author, whilst at the same time precluding potential choices for assignments or selections that would not be consistent with the security objectives for the TOE.

For example, in the following SFR (based on FAU_STG.4.1), the selection operation has been partially completed by precluding selection of the option ‘ignore auditable events’, which the PP author has judged to

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

be inconsistent with the security objectives for the TOE. The SFR therefore presents the ST author with a choice of two (rather than three) acceptable options:

*The TSF shall [selection: **'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'**] and [assignment: **other actions to be taken in case of audit storage failure**] if the audit trail is full.*

With assignments, the PP author may wish to limit the choices an ST author can make to a set of options acceptable for the environment. In this case, the PP author may wish to complete the assignment operation by turning it into a selection operation containing the valid choices, which in turn can be completed by the ST author.

As a general principle, a *partially* completed selection is valid if the set of options it presents is a subset of the options that are permitted by the original functional component. Similarly, a *partially* completed assignment is valid if the permitted values to complete the assignment are also valid assignments with respect to the original functional component. If for any reason these conditions are not met, then you have ended up with an extended functional component with a different assignment or selection operation.

Completing the operations of assignment and selection is reasonably straightforward. In the case of assignment, you simply need to ensure that the parameter is specified unambiguously. In the case of selection, you simply need to select the appropriate item(s), based on consideration of the security objectives for the TOE. You should, however, consult the guidance given in the annexes to ISO/IEC 15408-2 if in doubt.

Where assignment or selection has been performed in a PP, it is mandatory that you highlight the text that has been specified (this is helpful to the reader, and especially to the PP evaluator checking conformance to ISO/IEC 15408). The customary way of highlighting is by using italics, but bolding or a different character set can also be used.

For example, FMT_SAE.1.1 could be presented as:

*The TSF shall restrict the capability to specify an expiration time for **user passwords to the authorised administrator**.*

In this case bold has been used for highlighting, since, being an example, the text is already in italics.

If an operation is left uncompleted, it is mandatory for the ST author to complete the operation.

Any uncompleted (or partially completed) operations should, where appropriate, be accompanied by an explanation, targeted at the ST author, of how the operation should be completed (for example, in the form of an application note). It may be helpful to make it clear that the onus is on the ST author to specify the details. For example, FDP_RIP.1.1 could be specified in a PP as:

*The TSF shall ensure that any previous information content of a resource is made unavailable upon the **allocation of the resource to** the following objects [assignment: **list of objects specified by the ST author**].*

10.2.2.4 Refinement

The operation of refinement may be performed on any functional component element, and involves specifying additional technical details which do not levy any new requirements to those specified in the text, but rather restrict the set of acceptable implementations. A refinement is acceptable if meeting the refined requirement also means meeting the unrefined requirement. Use of refinement may be appropriate in the following circumstances:

a) where the PP is being written by an organisation which has additional technical details, such as organisation policy information, not included in the appropriate ISO/IEC 15408-2 component;

b) where the selected functional component would permit implementations which would not make sense, or would otherwise be inappropriate, for the type of TOE considered, unless it is refined so as to exclude that possibility e.g. on the grounds of interoperability;

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

c) where the readability of the SFR may be improved: see 10.2.9.

As with assignment and selection operations, it is recommended that you highlight the text that has been refined to assist the reader (and the PP evaluator in particular).

An example of the use of the refinement operation is as follows (based on FMT_MTD.3.1):

The TSF shall ensure that only secure values are accepted for TSF data. ***Refinement: the TSF shall ensure that the minimum password length enforced by the TOE is configured to a value of at least 6 characters.***

The use of the refinement operation to help clarify SFRs is discussed in 10.2.9 below.

10.2.3 How should the audit requirements be specified?

If the PP or ST includes auditing requirements (i.e. based on FAU_GEN.1) then ISO/IEC 15408 requires that the minimum set of events which must be auditable, and the minimum information which must be recorded, is specified through the consideration of all other functional requirements included in the PP or ST.

This selection will depend on a number of factors, including:

a) any security policy requirements on security audit, as defined in an OSP;

b) the importance of auditing in achieving the security objectives;

c) the relevance of potential events, and their characteristics, to the security objectives;

d) cost/benefit analysis.

For example, if the TOE is intended to defend against the actions of malicious users or hackers, it is likely that events such as login or access control violations will need to be auditable where the PP or ST includes such SFRs. However, events relating to the use of administrative functions may not need to be auditable, depending on the extent to which an administrator is (or has to be) trusted. The trustworthiness of the administrator would be stated as an assumption.

The question of cost/benefit analysis may rest on such issues as:

a) is the benefit of collecting the information worth the impact on performance?

b) if the information is collected, will the administrator have sufficient resources (e.g. tool support) to effectively analyse the data?

c) what are the likely costs of managing or archiving the data collected?

ISO/IEC 15408 identifies three pre-defined levels of auditing, namely *minimum*, *basic*, or *detailed* (see ISO/IEC 15408-2, 2.1.2.5): for each such level, ISO/IEC 15408-2 tells you which events should be auditable (as a minimum), together with the minimum information to be recorded, based on the functional components included in the PP or ST (see also ISO/IEC 15408-2, C.2). These three levels can be broadly characterised as follows:

a) The *minimum* level typically requires only some defined subset of operations or events associated with a given functional component to be auditable. This subset is generally defined to be the most interesting or significant type of event.

b) The *basic* level typically requires all operations or events associated with a given functional component to be auditable, e.g. successful and unsuccessful login attempts.

c) The *detailed* level generally differs from the *basic* level by requiring additional information of interest to be recorded. This level is only likely to be appropriate where the amount of audit data generated is

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

anticipated to be small, or if the data will be subject to analysis by sophisticated audit analysis tools or intrusion detection facilities.

If none of these levels is appropriate, you should select the *not specified* level, and list all required auditable events explicitly in FAU_GEN.1.1c. For example, you might use the *minimum* level for guidance, but choose to deviate from the *minimum* requirements in specific cases because a different subset of operations or events is more relevant to the security objectives, e.g. if FDP_ACF.1 is included in the PP or ST, you may consider that unsuccessful access attempts should be auditable rather than *successful* attempts (which is what ISO/IEC 15408-2 requires for the *minimum* level).

You will need to compile a list of auditable events by going through each functional component used in turn; in the case of the pre-defined levels of *minimum, basic* or *detailed,* these are explicitly identified in the *Audit* section included for each family of components. It is recommended that you construct a table, identifying the events and (where appropriate) the additional information to be recorded, which can be referenced by FAU_GEN.1.1 and FAU_GEN.1.2 as appropriate.

10.2.4 How should management requirements be specified?

ISO/IEC 15408-2 identifies, in the *Management* section included for each family of components, a list of management activities which should be considered for the component. This may suggest the need to include particular components from the FMT (Security Management) class. However, it is important to note that this section is intended to be *informative*. There is therefore no need to justify any decision not to include particular management components in the PP or ST (unless, of course, they are explicitly identified in the *Dependencies* section within ISO/IEC 15408-2).

Generally speaking, possible management activities are identified where a functional component refers to, or implies the existence of, configurable TSF data which may need to be managed and controlled. For example, the security objectives for the TOE might be undermined if the ability to modify such data was not restricted to administrators of the TOE. Therefore FMT components are often included in order to define *supporting* SFRs, in order to ensure that the security objectives for the TOE are met, and that the SFRs as a whole are mutually supportive (see 13.3.1 and 13.3.4).

You should consult the guidance on the FMT class given in ISO/IEC 15408-2, Annex H when choosing functional components from this class.

10.2.5 How should SOF be specified?

ISO/IEC 15408-3 identifies three pre-defined levels of SOF (Strength Of Function), namely *basic, medium or high* for all IT security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function) identified in the PP or ST (see also ISO/IEC 15408-1, C.2). The levels are characterised as follows:

a) the function provides adequate protection against casual breaches of TOE security by attackers possessing a low attack potential;

b) the function provides adequate protection against straightforward or intentional breaches of TOE security by attackers possessing a moderate attack potential;

c) the function provides adequate protection against deliberately planned or organised breaches of TOE security by attackers possessing a high attack potential.

The level to choose is based on a number of factors related to the threat agent(s):

a) Elapsed time;

b) Expertise;

c) Knowledge of the TOE;

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

d) Access to the TOE;

e) Equipment.

The value for these factors are derived from the breakdown of the attack potential for the threat agents identified in the threat statements. A characterisation of these factors should be derived during a full threat risk assessment.

For some probabilistic or permutational mechanisms an optional explicit metric could be provided, rather than the more general statement of *basic, medium or high*.

10.2.6 How should SFRs taken from a PP be specified?

Where an ST claims compliance with one or more PPs, it is likely that the SFRs will be specified either completely or mostly by the PP. In such cases, the ST author must decide whether to specify the PP functional requirements in full (in order to ensure all the text is in one place), or whether to simply reference the PP and specify SFRs where these differ from the PP.

In general, the latter approach is recommended since this will simplify the ST. The reader of an ST is more likely to be interested in the IT security functions than in the SFRs. This includes the evaluator of the TOE (since the content of evaluation evidence - such as design, test documentation and guidance documents - is likely to be more easily related to the IT security functions in the TOE summary specification than to the SFRs). The main purpose of specifying SFRs in an ST is to be able to demonstrate traceability back to relevant PPs, and to the SFRs as defined in ISO/IEC 15408-2. There is indeed a case for relegating the statement of SFRs to an annex so as not to confuse the reader by having two specifications of security functionality in the ST.

It should, however, be noted that some SFRs in the PP may have operations (such as assignment or selection) that are left to the ST author. In such cases it is recommended that the SFR is specified in full, with the completed operations emphasised by suitable typesetting (e.g. using italics). Any necessary explanations should be added using the same typesetting. Such an approach will make it easier for the reader of the ST (and the ST evaluator in particular) to see which operations have been performed, and in which manner. It will also facilitate the construction of the ST rationale (see 13.3.6).

10.2.7 How should SFRs not in a PP be specified?

In some cases it will be necessary to specify SFRs in an ST where these are not in a corresponding PP. This may be necessary where:

a) there is no appropriate PP available for the TOE to claim compliance with;

b) the sponsor considers that the benefit to be gained by having functional or assurance requirements, that are in addition to what is required by the PP, is sufficient to justify the additional cost that would be incurred.

In such cases, the approach to the specification of SFRs is the same as described in the preceding clause. Where SFRs are specified in addition to those required by a PP, the ST author must ensure that these do not conflict with SFRs in the PP (the ST rationale will need to demonstrate that such conflict does not occur: see Clause 13).

10.2.8 How should SFRs not included in Part 2 of ISO/IEC 15408 be specified?

ISO/IEC 15408 requires that if the PP or ST author wishes to include a functional requirement for which there is no appropriate functional component defined in ISO/IEC 15408-2, the resultant SFR should be specified using Part 2 components as a model for presentation.

The decision as to whether there is an appropriate functional component in ISO/IEC 15408-2 to use can be a difficult one to make, since this requires a high degree of familiarity with its content. It is recommended that you consult the guidance in Annex B which identifies the appropriate functional components to express

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004

common security functional requirements. It is often the case that the desired SFR can be obtained through appropriate application of the refinement operation, or of permitted assignment or selection operations. However, it is recommended that you do not attempt to 'shoehorn' an SFR into a functional component if this does not readily lead to the SFR you want, i.e. it results in an SFR whose meaning or intent cannot be readily discerned by the reader, or which (through the use of an inappropriate component) introduces inappropriate dependencies that need to be argued away.

Specifying a new SFR using ISO/IEC 15408-2 functional components as a model for presentation will involve:

a) defining the SFR at a similar level of abstraction as Part 2 components;

b) using a similar style and phraseology to Part 2 components;

c) using the topology and nomenclature approach for components as in ISO/IEC 15408-2.

Knowing that a new SFR is of a similar nature to others in an existing class or family helps bound its degree of newness and also may help with specific wording for common concepts that occur throughout that class or family.

Particular characteristics of the style of presentation of functional components in ISO/IEC 15408-2 include:

a) most functional requirements begin with the phrase *The TSF shall* or *The TSF shall be able to*, followed by a verb such as *allow, detect, enforce, ensure, limit, monitor, permit, prevent, protect, provide* or *restrict*;

b) the use of standard terms such as *security attribute* or *authorised user*;

c) each element tends to stand on its own and can be understood without reference to previous elements;

d) each security requirement must be evaluatable, i.e. it must be possible to determine whether the requirement has been met by a TOE.

In constructing an explicitly stated SFR, you should also consider whether the SFR:

a) should incorporate any assignment or selection operations to be completed by the ST author;

b) implies any dependencies on other SFRs which must be included in the PP or ST;

c) describes any events which should be auditable, and if so what information should be recorded for the event;

d) has any implications for security management, e.g. relies on security attributes that need to be managed.

If you believe you have a well-constructed SFR that is not included in ISO/IEC 15408-2, and is significantly different from, and would significantly enhance, the existing set of functional components in ISO/IEC 15408, you are advised to submit the SFR for inclusion in the next iteration of that International Standard.

ISO/IEC 15408 permits the ST author to explicitly state SFRs in an ST without reference to ISO/IEC 15408-2. The guidance given in 10.2.8 applies. However, it should be noted that it may not be necessary to specify ISO/IEC 15408 operations such as assignment or selection for SFRs constructed in this way if the SFR is only intended for use in the ST, i.e. there is no intent to reuse the component in other PPs, STs, or functional packages.

Naming for an SFR not included in ISO/IEC 15408-2 should use the topology and naming conventions of Part 2, to be in the same style as the standard. Extended components should use 'F' for function, followed by the appropriate class, and family designations followed by a component number. An extended component based on the existing classes can then be inserted at the appropriate place. Where an extended component is unrelated to existing classes it is acceptable for naming to make it clear that the extended security requirement is new by, for example making the class of the component 'EX', or appending 'EX' to the end of

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 15446:2004

the component name. How the extended component is denoted should be explained in the application notes for the PP or ST. Care should be taken that the naming convention used does not conflict with ISO/IEC 15408-2.

10.2.9 How should the SFRs be presented?

Writing a set of SFRs that are demonstrably compliant with the requirements of ISO/IEC 15408 is not (of course) the *only* aim of the PP or ST author. You should also consider how best to present and express the SFRs such that the general reader can understand what the security requirements mean. There are a number of steps you can take to enhance readability, without compromising compliance with ISO/IEC 15408.

Firstly, group the SFRs under headings which are appropriate for your PP or ST: do not feel constrained to adopt the class, family or component headings used in ISO/IEC 15408-2.

Secondly, do not feel constrained to adopt the functional element labelling system used in ISO/IEC 15408-2 for labelling the SFRs in your PP or ST. It is perfectly acceptable to adopt your own labelling system (which may feature more meaningful labels), provided the mapping of SFRs onto the relevant functional component from ISO/IEC 15408-2 is demonstrated (e.g. in an annex). Indeed, such an approach is likely to be highly desirable where the PP or ST includes functional components which are invoked several times. This is because the alternative is to have SFRs that do not have unique labels: the lack of unique labels for SFRs presents significant problems when constructing the security requirements rationale.

Thirdly, judicious use of the refinement operation may improve the readability of the SFR by substituting generic terms (such as *security attributes*) with more specific terminology relevant to the type of TOE or security functionality being described. For example, the following SFR is based on FMT_MSA.3.1:

*The TSF shall enforce the **DAC policy** to provide **restrictive** default values for **object permissions**.*

In this example, refinement has been used to replace the generic ‘security attributes that are used to enforce the SFP’ with the policy-specific ‘object permissions’.

Any such use of the refinement operation should be clearly highlighted and explained in the PP or ST Rationale (to support evaluation of the PP or ST).

The worked example presented in Annex F illustrates the application of this approach.

10.3 How to specify assurance requirements in a PP or ST

10.3.1 How should security assurance requirements be selected?

The selection of the assurance requirements will require the balancing of several factors including:

a) the value of the assets to be protected and the perceived risk of compromise of those assets;

b) technical feasibility;

c) likely development and evaluation costs;

d) required timescales for development and evaluation of the TOE;

e) perceived market requirement (in the case of products);

f) any identified dependencies of functional components on assurance components.

The greater the value of the assets to be protected, and the greater the risk to those assets, the higher the level of assurance that will be required in the security functions used to protect those assets. This should be reflected in the statement of security objectives. Organisations may define their own policies and rules to determine the level of assurance that is needed to ensure that the risks to their assets are reduced to an

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 15446:2004