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)

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

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

Published in Switzerland

Contents

Page

Foreword

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.*

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.

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.)

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.

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.

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.

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 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:

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;

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