
**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*

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.

This document is a preview generated by EVS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

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

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

Published in Switzerland

Contents

Page

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

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

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

14	Specifying PP/STs for composed and component TOEs.....	69
14.1	Composed TOEs.....	69
14.2	Component TOEs	72
15	Special cases	72
15.1	Low assurance Protection Profiles and Security Targets.....	72
15.2	Conforming to national interpretations.....	73
15.3	Functional and assurance packages	73
16	Use of automated tools	73
Annex A (informative) Example for the definition of an extended component.....		75
Bibliography		78
Index		79

Foreword

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

1 Scope

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

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

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

2 Normative references

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

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

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

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

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

3 Terms and definitions

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

4 Abbreviations

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

COTS Commercial Off The Shelf

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