TECHNICAL REPORT

ISO/IEC TR 15446

Third edition
2017-10

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

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

Reference number
ISO/IEC TR 15446:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

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

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

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **1**
5 Purpose and structure of this document **2**
6 Overview of PPs and STs **2**
6.1 General 2
6.2 Audience 2
6.3 Use of PPs and STs 3
6.3.1 General 3
6.3.2 Specification-based purchasing processes 4
6.3.3 Selection-based purchasing processes 7
6.3.4 Other uses of PPs 8
6.4 The PP/ST development process 8
6.4.1 Including stakeholders in the development process 8
6.4.2 Method to develop a PP or ST 9
6.4.3 Evaluation of PPs and STs 9
6.5 Reading and understanding PPs and STs 10
6.5.1 General 10
6.5.2 Reading the TOE overview 10
6.5.3 Reading the TOE description 11
6.5.4 Security objectives for the operational environment 12
6.5.5 Reading the conformance claim 12
6.5.6 Conformance to Protection Profiles 13
6.5.7 EALs and other assurance issues 13
6.5.8 Summary 15
6.5.9 Further reading 15
7 Specifying the PP/ST introduction **15**
8 Specifying conformance claims **16**
9 Specifying the security problem definition **17**
9.1 General 17
9.2 Identifying the informal security requirement 18
9.2.1 General 18
9.2.2 Sources of information 19
9.2.3 Documenting the informal requirement 20
9.3 How to identify and specify threats 21
9.3.1 General 21
9.3.2 Deciding on a threat analysis methodology 21
9.3.3 Identifying participants 23
9.3.4 Applying the chosen threat analysis methodology 26
9.3.5 Practical advice 27
9.4 How to identify and specify policies 28
9.5 How to identify and specify assumptions 29
9.6 Finalizing the security problem definition 31
10 Specifying the security objectives **32**
10.1 General 32
10.2 Structuring the threats, policies and assumptions 33
10.3 Identifying the non-IT operational environment objectives 34

© ISO/IEC 2017 – All rights reserved

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

11 Specifying extended component definitions ... 39

12 Specifying the security requirements ... 43
12.1 General ... 43
12.2 Security paradigms in ISO/IEC 15408 ... 45
12.2.1 Explanation of the security paradigms and their usage for modelling the security functionality ... 45
12.2.2 Controlling access to and use of resources and objects ... 45
12.2.3 User management ... 48
12.2.4 TOE self protection ... 49
12.2.5 Securing communication ... 50
12.2.6 Security audit ... 52
12.2.7 Architectural requirements ... 52
12.3 How to specify security functional requirements in a PP or ST ... 53
12.3.1 How should security functional requirements be selected? ... 53
12.3.2 Selecting SFRs from ISO/IEC 15408-2:2008 ... 56
12.3.3 How to perform operations on security functional requirements ... 58
12.3.4 How should the audit requirements be specified? ... 60
12.3.5 How should management requirements be specified? ... 61
12.3.6 How should SFRs taken from a PP be specified? ... 62
12.3.7 How should SFRs not in a PP be specified? ... 62
12.3.8 How should SFRs not included in ISO/IEC 15408-2:2008 be specified? ... 62
12.3.9 How should the SFRs be presented? ... 63
12.3.10 How to develop the security requirements rationale ... 63
12.4 How to specify assurance requirements in a PP or ST ... 64
12.4.1 How should security assurance requirements be selected? ... 64
12.4.2 How to perform operations on security assurance requirements ... 65
12.4.3 How should SARs not included in ISO/IEC 15408-3:2008 be specified in a PP or ST? ... 66
12.4.4 Security assurance requirements rationale ... 66

13 The TOE summary specification ... 67

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

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

16 Use of automated tools ... 73

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

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

Bibliography ... 79

 © ISO/IEC 2017 – All rights reserved

Foreword

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

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

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

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

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

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

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

© ISO/IEC 2017 – All rights reserved

Introduction

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

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

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

© ISO/IEC 2017 – All rights reserved

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

1 Scope

This document provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408 (all parts). It is also applicable to PPs and STs compliant with Common Criteria Version 3.1 Revision 4[6], a technically identical standard published by the Common Criteria Management Board, a consortium of governmental organizations involved in IT security evaluation and certification.

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms and definitions

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

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

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

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

4 Abbreviated terms

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

COTS Commercial Off The Shelf

CRL Certificate Revocation List

LDAP Lightweight Directory Access Protocol

SPD Security Problem Definition

SSL Secure Sockets Layer

TLS Transport Layer Security

© ISO/IEC 2017 – All rights reserved