TECHNICAL REPORT

ISO/IEC TR 15446

Second edition
2009-03-01

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 15446:2009(E)

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*.

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.