INTERNATIONAL STANDARD

ISO/IEC 15408-2

Second edition
2005-10-01

Information technology — Security techniques — Evaluation criteria for IT security —

Part 2: Security functional requirements

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 2: Exigences fonctionnelles de sécurité

This document is a preview generated by EVS

Reference number
ISO/IEC 15408-2:2005(E)

© ISO/IEC 2005

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

© ISO/IEC 2005

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

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

Document is a preview generated by EVS

 © ISO/IEC 2005 - All rights reserved

This preview is generated by EVS

© ISO/IEC 2005 - All rights reserved

ISO Documents is a preview generated by EVS

 © ISO/IEC 2005 - All rights reserved

This preview is generated by EVS

© ISO/IEC 2005 - All rights reserved

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

This preview is generated by EVS

© ISO/IEC 2005 - All rights reserved

ISO document is a preview generated by EVS

 © ISO/IEC 2005 - All rights reserved

ISO/IEC 15408-2:2005 - This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

This document is a preview generated by EVS

 © ISO/IEC 2005 - All rights reserved

This preview is generated by EVS

© ISO/IEC 2005 - All rights reserved

Document Preview generated by EVS

© ISO/IEC 2005 - All rights reserved

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

This document is a preview generated by EVS

© ISO/IEC 2005 - 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.

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.

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 15408-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation.

This second edition cancels and replaces the first edition (ISO/IEC 15408-2:1999), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

— *Part 1: Introduction and general model*

— *Part 2: Security functional requirements*

— *Part 3: Security assurance requirements*

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.3 Parts 1 through 3 (called CC 2.3), they hereby grant non-exclusive license to ISO/IEC to use CC 2.3 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 2.3 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

Introduction

Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) or the IT environment of the TOE and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 Subclause 5.3 provides more detailed information on the relationship between security objectives and security requirements.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functions and mechanisms that comply with those requirements.

c) Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

This document is a preview generated by EVS

© ISO/IEC 2005 - All rights reserved

Information technology — Security techniques — Evaluation criteria for IT security —

Part 2: Security functional requirements

This document is a preview generated by EVS

1 Scope

This part of ISO/IEC 15408 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products and systems.

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

3 Terms, definitions, symbols and abbreviated terms

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

4 Overview

ISO/IEC 15408 and the associated security functional requirements described herein are not meant to be a definitive answer to all the problems of IT security. Rather, ISO/IEC 15408 offers a set of well understood security functional requirements that can be used to create trusted products or systems reflecting the needs of the market. These security functional requirements are presented as the current state of the art in requirements specification and evaluation.

This part of ISO/IEC 15408 does not presume to include all possible security functional requirements but rather contains those that are known and agreed to be of value by this part of ISO/IEC 15408 authors at the time of release.

Since the understanding and needs of consumers may change, the functional requirements in this part of ISO/IEC 15408 will need to be maintained. It is envisioned that some PP/ST authors may have security needs not (yet) covered by the functional requirement components in this part of ISO/IEC 15408. In those cases the PP/ST author may choose to consider using functional requirements not taken from ISO/IEC 15408 (referred to as extensibility), as explained in annexes A and B of ISO/IEC 15408-1.

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security functional requirements of this part of ISO/IEC 15408.

Clause 6 introduces the catalogue of this part of ISO/IEC 15408 functional components while clauses 7 through 17 describe the functional classes.

© ISO/IEC 2005 - All rights reserved