INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe hindamise kriteeriumid
Osa 1: Sissejuhatus ja üldmudel

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

EESTI STANDARDIKESKUS **EVS**
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-ISO/IEC 15408-1:2011 "Infotehnoloogia. Turbemeetodid. Infoturbe hindamise kriteeriumid. Osa 1: Sissejuhatus ja üldmudel" sisaldab rahvusvahelise standardi ISO/IEC 15408-1:2009 „Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model" identset ingliskeelset teksti.

Standard EVS-ISO/IEC 15408-1:2011 on kinnitatud Eesti Standardikeskuse 10.02.2011 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.

Standard on kättesaadav Eesti Standardikeskusest.

This Estonian Standard EVS-ISO/IEC 15408-1:2011 consists of the identical English text of the International Standard ISO/IEC 15408-1:2009 "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

This standard is ratified with the order of Estonian Centre for Standardisation dated 10.02.2011 and is endorsed with the notification published in the official bulletin of the Estonian centre for Standardisation.

This standard is available from the Estonian Centre for Standardisation.

Käsitlusala

ISO/IEC 15408 selles osas kehtestatakse infoturbe hindamise üldmõisted ja põhimõtted ning määratakse kindlaks hindamise üldmudel, mis on esitatud standardi eri osades ning mis on tervikuna mõeldud kasutamiseks IT-toodete turvaomaduste hindamise alusena.

Standardi ISO/IEC 15408 esimeses osas kirjeldatakse standardi kõiki osi, määratletakse terminid ja lühendid, mida kasutatakse kõigis osades, kehtestatakse hindamisobjekti (*Target of Evaluation* - TOE) tuummõiste, määratakse hindamise kontekst ja kirjeldatakse lugejaskonda, kellele on hindamise kriteeriumid suunatud. Sissejuhatavalt kirjeldatakse põhilisi turvamõisteid, mis on vajalikud IT-toodete hindamiseks.
Standard määratleb mitmesugused operatsioonid, millega saab lubatavate operatsioonide kasutamise teel kohandada funktsionaalseid ja tagatislikke komponente, mis on esitatud standardi osades ISO/IEC 15408-2 ja ISO/IEC 15408-3.

Esitatud on kaitseprofiilide (PP) tuummõisted, turvanõuete paketid ja vastavuse teema ning kirjeldatud on hindamise tagajärgi ja tulemeid. ISO/IEC 15408 käesolev, esimeses osas antakse suunised turvasihtide (ST) spetsifitseerimiseks ja kirjeldatakse komponentide korraldust kogu mudeli ulatuses. Hindamismetoodika üldteave ja hindamisskeemide käsitlusala on standardis ISO/IEC 18045.

ICS 35.040 - Märgistikud ja informatsiooni kodeerimine

Contents

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 part of ISO/IEC 15408 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 15408-1 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. The common XML source for both publications can be found at http://www.oc.ccn.cni.es/xml

This third edition cancels and replaces the second edition (ISO/IEC 15408-1:2005), 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 components*

— *Part 3: Security assurance components*

Introduction

This part of ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of this International Standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below.

a) ISO/IEC 15408 does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls.

b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.

c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.

d) ISO/IEC 15408 does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 will be used for evaluation purposes in the context of such a framework.

e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the

evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.

f)   The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term "should" has an additional meaning applicable when using this International Standard. See the note below. The following definition is given for the use of "should" in ISO/IEC 15408.

should

within normative text, "should" indicates "that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required" (ISO/IEC Directives, Part 2)

NOTE   ISO/IEC 15408 interprets "not necessarily required" to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

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

Part 1:
Introduction and general model

1 Scope

This part of ISO/IEC 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the International Standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the International Standard; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

2 Normative references

The following referenced documents are indispensable for the application of this part of ISO/IEC 15408. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE   This clause contains only those terms which are used in a specialized way throughout ISO/IEC 15408. Some combinations of common terms used in ISO/IEC 15408, while not meriting inclusion in this clause, are explained for clarity in the context where they are used.