

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC 15408-1:2022)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

<p>See Eesti standard EVS-EN ISO/IEC 15408-1:2023 sisaldab Euroopa standardi EN ISO/IEC 15408-1:2023 ingliskeelset teksti.</p> <p>Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.</p> <p>Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 06.12.2023.</p> <p>Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.</p>	<p>This Estonian standard EVS-EN ISO/IEC 15408-1:2023 consists of the English text of the European standard EN ISO/IEC 15408-1:2023.</p> <p>This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.</p> <p>Date of Availability of the European standard is 06.12.2023.</p> <p>The standard is available from the Estonian Centre for Standardisation and Accreditation.</p>
---	---

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele. Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis-ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis-ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English version

Information security, cybersecurity and privacy protection
- Evaluation criteria for IT security - Part 1: Introduction
and general model (ISO/IEC 15408-1:2022)

Sécurité de l'information, cybersécurité et protection
de la vie privée - Critères d'évaluation pour la sécurité
des technologies de l'information - Partie 1:
Introduction et modèle général (ISO/IEC 15408-
1:2022)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Evaluationskriterien für IT-
Sicherheit - Teil 1: Einführung und allgemeines Modell
(ISO/IEC 15408-1:2022)

This European Standard was approved by CEN on 20 November 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

The text of ISO/IEC 15408-1:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 15408-1:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2024, and conflicting national standards shall be withdrawn at the latest by June 2024.

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

This document supersedes EN ISO/IEC 15408-1:2020.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 15408-1:2022 has been approved by CEN-CENELEC as EN ISO/IEC 15408-1:2023 without any modification.

Contents

Page

Foreword	vi
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Abbreviated terms	13
5 Overview	15
5.1 General	15
5.2 ISO/IEC 15408 series description	15
5.2.1 General	15
5.2.2 Audience	16
5.3 Target of evaluation (TOE)	19
5.3.1 General	19
5.3.2 TOE boundaries	19
5.3.3 Different representations of the TOE	20
5.3.4 Different configurations of the TOE	20
5.3.5 Operational environment of the TOE	20
5.4 Presentation of material in this document	21
6 General model	21
6.1 Background	21
6.2 Assets and security controls	21
6.3 Core constructs of the paradigm of the ISO/IEC 15408 series	24
6.3.1 General	24
6.3.2 Conformance types	24
6.3.3 Communicating security requirements	24
6.3.4 Meeting the needs of consumers (risk owners)	27
7 Specifying security requirements	29
7.1 Security problem definition (SPD)	29
7.1.1 General	29
7.1.2 Threats	29
7.1.3 Organizational security policies (OSPs)	30
7.1.4 Assumptions	30
7.2 Security objectives	31
7.2.1 General	31
7.2.2 Security objectives for the TOE	31
7.2.3 Security objectives for the operational environment	31
7.2.4 Relation between security objectives and the SPD	32
7.2.5 Tracing between security objectives and the SPD	32
7.2.6 Providing a justification for the tracing	33
7.2.7 On countering threats	33
7.2.8 Security objectives: conclusion	33
7.3 Security requirements	33
7.3.1 General	33
7.3.2 Security Functional Requirements (SFRs)	34
7.3.3 Security assurance requirements (SARs)	36
7.3.4 Security requirements: conclusion	37
8 Security components	38
8.1 Hierarchical structure of security components	38
8.1.1 General	38
8.1.2 Class	38
8.1.3 Family	39

8.1.4	Component	39
8.1.5	Element	39
8.2	Operations	39
8.2.1	General	39
8.2.2	Iteration	40
8.2.3	Assignment	40
8.2.4	Selection	41
8.2.5	Refinement	43
8.3	Dependencies between components	44
8.4	Extended components	44
8.4.1	General	44
8.4.2	Defining extended components	45
9	Packages	45
9.1	General	45
9.2	Package types	46
9.2.1	General	46
9.2.2	Assurance packages	46
9.2.3	Functional packages	47
9.3	Package dependencies	47
9.4	Evaluation method(s) and activities	47
10	Protection Profiles (PPs)	48
10.1	General	48
10.2	PP introduction	48
10.3	Conformance claims and conformance statements	48
10.4	Security assurance requirements (SARs)	51
10.5	Additional requirements common to strict and demonstrable conformance	51
10.5.1	Conformance claims and conformance statements	51
10.5.2	Security problem definition (SPD)	51
10.5.3	Security objectives	52
10.6	Additional requirements specific to strict conformance	52
10.6.1	Requirements for the security problem definition (SPD)	52
10.6.2	Requirements for the security objectives	52
10.6.3	Requirements for the security requirements	52
10.7	Additional requirements specific to demonstrable conformance	53
10.8	Additional requirements specific to exact conformance	53
10.8.1	General	53
10.8.2	Conformance claims and statements	53
10.9	Using PPs	54
10.10	Conformance statements and claims in the case of multiple PPs	54
10.10.1	General	54
10.10.2	Where strict or demonstrable conformance is specified	54
10.10.3	Where exact conformance is specified	54
11	Modular requirements construction	54
11.1	General	54
11.2	PP-Modules	55
11.2.1	General	55
11.2.2	PP-Module Base	55
11.2.3	Requirements for PP-Modules	55
11.3	PP-Configurations	59
11.3.1	General	59
11.3.2	Requirements for PP-Configurations	59
11.3.3	Usage of PP-Configurations	65
12	Security Targets (STs)	68
12.1	General	68
12.2	Conformance claims and statements	68
12.3	Assurance requirements	71

12.4	Additional requirements in the exact conformance case.....	71
12.4.1	Additional requirements for the conformance claim	71
12.4.2	Additional requirements for the SPD	71
12.4.3	Additional requirements for the security objectives.....	72
12.4.4	Additional requirements for the security requirements	72
12.5	Additional requirements in the multi-assurance case.....	72
13	Evaluation and evaluation results.....	74
13.1	General.....	74
13.2	Evaluation context.....	76
13.3	Evaluation of PPs and PP-Configurations.....	77
13.4	Evaluation of STs.....	77
13.5	Evaluation of TOEs.....	77
13.6	Evaluation methods and evaluation activities.....	78
13.7	Evaluation results.....	78
13.7.1	Results of a PP evaluation.....	78
13.7.2	Results of a PP-Configuration evaluation	78
13.7.3	Results of a ST/TOE evaluation.....	78
13.8	Multi-assurance evaluation.....	79
14	Composition of assurance.....	80
14.1	General.....	80
14.2	Composition models.....	81
14.2.1	Layered composition model.....	81
14.2.2	Network or bi-directional composition model.....	82
14.2.3	Embedded composition model.....	82
14.3	Evaluation techniques for providing assurance in composition models.....	83
14.3.1	General.....	83
14.3.2	ACO class for composed TOEs.....	83
14.3.3	Composite evaluation for composite products.....	84
14.4	Requirements for evaluations using composition techniques.....	95
14.4.1	Re-use of evaluation results.....	95
14.4.2	Composition evaluation issues.....	96
14.5	Evaluation by composition and multi-assurance.....	97
	Annex A (normative) Specification of packages.....	98
	Annex B (normative) Specification of Protection Profiles (PPs).....	102
	Annex C (normative) Specification of PP-Modules and PP-Configurations.....	112
	Annex D (normative) Specification of Security Targets (STs) and Direct Rationale STs.....	125
	Annex E (normative) PP/PP-Configuration conformance.....	136
	Bibliography.....	141

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.

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 document 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 or www.iec.ch/members_experts/refdocs).

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. 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) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

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

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 15408-1:2009), which has been technically revised.

The main changes are as follows:

- the document has been restructured;
- technical changes have been introduced:
 - the terminology has been reviewed and updated;
 - the exact conformance type has been introduced;
 - low assurance protection profiles (PPs) have been removed and direct rationale PPs have been introduced;
 - PP-Modules and PP-Configurations for modular evaluations have been introduced;
 - multi-assurance evaluation has been introduced.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations 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.

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

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/activities, irrelevant security properties, or inappropriate IT products, can 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 provides 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.

The ISO/IEC 15408 series addresses the protection of assets from unauthorized 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. The ISO/IEC 15408 series may also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series 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 the ISO/IEC 15408 series. Some of these are identified below:

- a) the ISO/IEC 15408 series does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls;
- b) the ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied;

NOTE 1 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

- c) the ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to be used for evaluation purposes in the context of such a framework;
- d) the procedures for use of evaluation results in accreditation are outside the scope of the ISO/IEC 15408 series. 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 must make separate provisions for those aspects;

- e) the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the ISO/IEC 15408 series. In the case that independent assessment of mathematical properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied shall make provision for such assessments.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 1: Introduction and general model

1 Scope

This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

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

This document introduces:

- the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;
- a description of the organization of security components throughout the model;
- the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;
- general information about the evaluation methods given in ISO/IEC 18045;
- guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;
- general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;
- information in regard to the scope of evaluation schemes.

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 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

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

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*