TECHNICAL REPORT

# ISO/IEC TR 22216

First edition
2022-05

# Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

*Sécurité de l'information, cybersécurité et protection de la vie privée — Nouveaux concepts et modifications dans l'ISO/IEC 15408:2022 et l'ISO/IEC 18045:2022*

Reference number
ISO/IEC TR 22216:2022(E)

© ISO/IEC 2022



## COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland



© ISO/IEC 2022 – All rights reserved

# Contents

Page

**Foreword** ..... **vi**

**Introduction** ..... **vii**

**1 Scope** ..... **1**

**2 Normative references** ..... **1**

**3 Terms, definitions and abbreviated terms** ..... **1**
3.1 Terms and definitions ..... 1
3.2 Abbreviated terms ..... 2

**4 Overview** ..... **2**
4.1 General ..... 2
4.2 Structure of this document ..... 2
4.3 Impacts of the revision on the structure and partition of the documents ..... 2
4.4 Using this document for transitional information ..... 4
4.5 Using the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 for specific needs ..... 4

**5 Major new concepts introduced in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022** ..... **5**
5.1 Approaches to security evaluation ..... 5
5.1.1 General ..... 5
5.1.2 The attack-based approach ..... 6
5.1.3 The specification-based approach ..... 7
5.2 Modularity ..... 9
5.2.1 General ..... 9
5.2.2 Composition mechanisms ..... 10
5.2.3 Packages ..... 11
5.2.4 Modular Protection Profiles ..... 12
5.2.5 Multi-assurance evaluations ..... 13
5.2.6 Evaluation by composition and multi-assurance ..... 17

**6 Applying the ISO/IEC 15408:2022 series to specific needs** ..... **21**
6.1 Refining and deriving requirements ..... 21
6.1.1 General ..... 21
6.1.2 Refinements ..... 21
6.1.3 Application Notes ..... 21
6.1.4 Extended requirements ..... 21
6.2 Refining and deriving evaluation methods ..... 22
6.2.1 General ..... 22
6.2.2 Attack-based approach ..... 22
6.2.3 Specification-based approach ..... 22
6.3 Practical aspects of supporting documents ..... 22

**7 Evolutions in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022** ..... **22**
7.1 Changes in ISO/IEC 15408-1:2022 ..... 22
7.2 Changes in ISO/IEC 15408-2:2022 ..... 28
7.3 Changes in ISO/IEC 15408-3:2022 ..... 31
7.4 Addition of ISO/IEC 15408-4:2022 ..... 42
7.5 Addition of ISO/IEC 15408-5:2022 ..... 44
7.6 Changes in ISO/IEC 18045:2022 ..... 44

**Bibliography** ..... **45**

© ISO/IEC 2022 – All rights reserved

# List of Figures

Figure 1 — ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 structure and mapping to former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 ..... 3
Figure 2 — Specification-based and attack-based approaches ..... 6
Figure 3 — Smartphone with hardware key store ..... 14
Figure 4 — IoT gateway with personal area network ..... 15
Figure 5 — POI developer ..... 16
Figure 6 — POI risk owner ..... 16
Figure 7 — POI developer vs risk owner ..... 17
Figure 8 — POI assurance requirements ..... 17
Figure 9 — Multi-assurance TOE ..... 18
Figure 10 — Multiple single evaluations ..... 19
Figure 11 — Composite TOE ..... 19
Figure 12 — Composite evaluation ..... 20
Figure 13 — Multi-assurance evaluation of a composite TOE ..... 20
Figure 14 — Multi-assurance composite evaluation ..... 21
Figure 15 — Clause structure — ISO/IEC 15408-1:2022 vs. CC v3.1 revision 5 [14] ..... 24
Figure 16 — Contents of a PP —ISO/IEC 15408-1:2022 vs. CC v3.1 revision 5 [14] ..... 25
Figure 17 — Contents of an ST — ISO/IEC 15408-1:2022 vs. CC v3.1 revision 5 [14] ..... 26
Figure 18 — Contents of a PP-Module — ISO/IEC 15408-1:2022 vs. CC v3.1 revision 5 [14] ..... 27
Figure 19 — Contents of a PP-Configuration — ISO/IEC 15408-1:2022 vs. CC v3.1 revision 5 [14] ..... 28


© ISO/IEC 2022 – All rights reserved

# List of Tables

**Table 1 — Overview of newly introduced concepts** 3
**Table 2 — Changes in ISO/IEC 15408-1:2022** 23
**Table 3 — Changes in ISO/IEC 15408-2:2022** 29
**Table 4 — Changes in ISO/IEC 15408-3:2022** 31
**Table 5 — Class APE — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 31
**Table 6 — Class ACE — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 33
**Table 7 — Class ASE — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 36
**Table 8 — Class ADV — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 38
**Table 9 — Class AGD — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 39
**Table 10 — Class ALC — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 40
**Table 11 — Class ATE — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 41
**Table 12 — Class AVA — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 41
**Table 13 — Class ACO — ISO/IEC 15408-3:2022 vs. CC v3.1 revision 5** 42
**Table 14 — ISO/IEC 15408-4:2022 — Summary** 42
**Table 15 — ISO/IEC 15408-5:2022 — Summary** 44
**Table 16 — Changes in ISO/IEC 18045:2022** 44

© ISO/IEC 2022 – 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.

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 Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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.


© ISO/IEC 2022 – All rights reserved

# Introduction

The ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 include substantial changes compared to the former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 and subsequent Common Criteria and Common Evaluation Methodology Version 3.1 Revision 5 [14]-[17] (also called CC 3.1 and CEM 3.1 in the following). The edition:

— covers complex products and communities' needs;

— offers compatibility with currently existing processes.

The goal of the revision of the ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 was manifold and intended to support and fluidify the work of all main groups with a general interest in the evaluation of the security properties of Target of Evaluations (TOEs) by restructuring the documents, introducing new concepts and updating the existing ones after rigorous consideration of commonly used approaches for the criteria. Specifically, the revision aimed to:

— take into consideration Common Criteria users, especially existing Mutual Recognition Agreements (MRAs), and their stakeholders,

NOTE The only existing recognition arrangements are the Common Criteria Recognition Arrangement[1)] (CCRA) and Senior Officials Group — Information Systems Security Mutual Recognition Agreement[2)] (SOG-IS MRA).

— offer continued alignment with the supporting documents developed in the context of the existing MRAs;

— take into consideration commonly used approaches for the criteria (including but not limited to CC 3.1 and CEM 3.1) and introduce technical changes accordingly.

This document is meant to provide information and support to users of the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022. The audience for this document includes:

— security assurance consumers;

— IT product developers and those authoring Security Targets;

— technical community subject matter experts (SMEs) developing Packages, Protection Profiles, evaluation methodologies, and other supportive documents;

— evaluators;

— evaluation schemes, and evaluation authorities;

— consultants, including developers of supportive tools;

— others, including those involved with mutual recognition arrangements and academia.

It is expected that the audience for this document is familiar with CC 3.1 and CEM 3.1.

1) https://www.commoncriteriaportal.org/ccra/index.cfm

2) https://sogis.org

© ISO/IEC 2022 – All rights reserved

# Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

## 1 Scope

This document:

— introduces the break down between the former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008) and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 and the new parts introduced in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022;

— presents the concepts newly introduced as well as the rationale for their inclusion;

— proposes an evolution path and information on how to move from CC 3.1 and CEM 3.1 to the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022, respectively;

— maps the evolutions between the CC 3.1 and CEM 3.1 and the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022, respectively.

## 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 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

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 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

## 3 Terms, definitions and abbreviated terms

### 3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, and ISO/IEC 18045:2022 apply.

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

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

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

© ISO/IEC 2022 – All rights reserved