ISO/IEC TR 22216:2022-05 (E)

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

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**

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

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