SLOVENSKI STANDARD
oSIST prEN ISO/IEC 15408-3:2024

01-november-2024

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za vrednotenje varnosti IT - 3. del: Komponente za zagotavljanje varnosti (ISO/IEC DIS 15408-3:2024)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components (ISO/IEC DIS 15408-3:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 3: Komponenten für die Vertrauenswürdigkeit der Sicherheit

Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 3: Composants d'assurance de sécurité (ISO/IEC DIS 15408-3:2024)

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

Ta slovenski standard je istoveten z: prEN ISO/IEC 15408-3

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 15408-3:2024 en,fr,de

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

DRAFT
International
Standard

ISO/IEC DIS 15408-3

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

Part 3: Security assurance components

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 3: Composants d'assurance de sécurité

ICS: ISO ics

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-08-19

Voting terminates on:
2024-11-11

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024

https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 15408-3:2024(en)

© ISO/IEC 2024

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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

Contents

Page

Foreword .... **x**

Introduction .... **xii**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions and abbreviated terms **1**

4 Overview **5**

5 Assurance paradigm **6**

- 5.1 General 6
- 5.2 ISO/IEC 15408 series approach 6
- 5.3 Assurance approach 6
  - 5.3.1 General 6
  - 5.3.2 Significance of vulnerabilities 6
  - 5.3.3 Cause of vulnerabilities 7
  - 5.3.4 ISO/IEC 15408 series assurance 7
  - 5.3.5 Assurance through evaluation 7
- 5.4 ISO/IEC 15408 series evaluation assurance scale 8

6 Security assurance components **8**

- 6.1 Overview 8
- 6.2 Assurance class structure 8
  - 6.2.1 General 8
  - 6.2.2 Class name 8
  - 6.2.3 Class introduction 9
  - 6.2.4 Assurance families 9
- 6.3 Assurance family structure 9
  - 6.3.1 General 9
  - 6.3.2 Family name 9
  - 6.3.3 Family objectives 9
  - 6.3.4 Component levelling 10
  - 6.3.5 Family application notes 10
  - 6.3.6 Assurance components 10
- 6.4 Assurance component structure 10
  - 6.4.1 General 10
  - 6.4.2 Component name 10
  - 6.4.3 Component objectives 11
  - 6.4.4 Component application notes 11
  - 6.4.5 Component dependencies 11
  - 6.4.6 Assurance elements 11
- 6.5 Assurance elements 12
- 6.6 Component taxonomy 12

7 Class APE Protection Profile (PP) evaluation **12**

- 7.1 Introduction 12
- 7.2 Conformance claims (APE_CCL) 14
  - 7.2.1 Objectives 14
  - 7.2.2 Conformance claims (APE_CCL.1) 14
- 7.3 Extended components definition (APE_ECD) 16
  - 7.3.1 Objectives 16
  - 7.3.2 Extended components definition (APE_ECD.1) 16
- 7.4 PP introduction (APE_INT) 17
  - 7.4.1 Objectives 17
  - 7.4.2 PP introduction (APE_INT.1) 17
- 7.5 Security objectives (APE_OBJ) 17
  - 7.5.1 Objectives 17

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ae5d1fef-c586-4b30-99b7-544ac8be70fc/osist-pren-iso-iec-15408-3-2024

© ISO/IEC 2024 – All rights reserved

7.5.2 Component levelling ... 17
7.5.3 Security objectives for the operational environment (APE_OBJ.1) ... 18
7.5.4 Security objectives (APE_OBJ.2) ... 18
7.6 Security requirements (APE_REQ) ... 19
7.6.1 Objectives ... 19
7.6.2 Component levelling ... 19
7.6.3 Direct rationale security requirements (APE_REQ.1) ... 19
7.6.4 Derived security requirements (APE_REQ.2) ... 20
7.7 Security problem definition (APE_SPD) ... 22
7.7.1 Objectives ... 22
7.7.2 Security problem definition (APE_SPD.1) ... 22

8 Class ACE Protection Profile Configuration evaluation ... 22
8.1 Introduction ... 22
8.2 PP-Module conformance claims (ACE_CCL) ... 24
8.2.1 Objectives ... 24
8.2.2 PP-Module conformance claims (ACE_CCL.1) ... 24
8.3 PP-Configuration consistency (ACE_CCO) ... 25
8.3.1 Objectives ... 25
8.3.2 PP-Configuration consistency (ACE_CCO.1) ... 26
8.4 PP-Module extended components definition (ACE_ECD) ... 29
8.4.1 Objectives ... 29
8.4.2 PP-Module extended components definition (ACE_ECD.1) ... 29
8.5 PP-Module introduction (ACE_INT) ... 30
8.5.1 Objectives ... 30
8.5.2 PP-Module introduction (ACE_INT.1) ... 30
8.6 PP-Module consistency (ACE_MCO) ... 31
8.6.1 Objectives ... 31
8.6.2 PP-Module consistency (ACE_MCO.1) ... 31
8.7 PP-Module security objectives (ACE_OBJ) ... 32
8.7.1 Objectives ... 32
8.7.2 Component levelling ... 32
8.7.3 PP-Module security objectives for the operational environment (ACE_OBJ.1) ... 32
8.7.4 PP-Module security objectives (ACE_OBJ.2) ... 33
8.8 PP-Module security requirements (ACE_REQ) ... 34
8.8.1 Objectives ... 34
8.8.2 Component levelling ... 34
8.8.3 PP-Module direct rationale security requirements (ACE_REQ.1) ... 34
8.8.4 PP-Module derived security requirements (ACE_REQ.2) ... 35
8.9 PP-Module security problem definition (ACE_SPD) ... 37
8.9.1 Objectives ... 37
8.9.2 PP-Module security problem definition (ACE_SPD.1) ... 37

9 Class ASE Security Target (ST) evaluation ... 37
9.1 Introduction ... 37
9.2 Conformance claims (ASE_CCL) ... 39
9.2.1 Objectives ... 39
9.2.2 Conformance claims (ASE_CCL.1) ... 39
9.3 Consistency of composite product Security Target (ASE_COMP) ... 41
9.3.1 Objectives ... 41
9.3.2 Component levelling ... 41
9.3.3 Application notes ... 41
9.3.4 Consistency of Security Target (ST) (ASE_COMP.1) ... 42
9.4 Extended components definition (ASE_ECD) ... 42
9.4.1 Objectives ... 42
9.4.2 Extended components definition (ASE_ECD.1) ... 43
9.5 ST introduction (ASE_INT) ... 43
9.5.1 Objectives ... 43
9.5.2 ST introduction (ASE_INT.1) ... 44
9.6 Security objectives (ASE_OBJ) ... 45

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

9.6.1 Objectives 45
9.6.2 Component levelling 45
9.6.3 Security objectives for the operational environment (ASE_OBJ.1) 45
9.6.4 Security objectives (ASE_OBJ.2) 45
9.7 Security requirements (ASE_REQ) 46
9.7.1 Objectives 46
9.7.2 Component levelling 47
9.7.3 Direct rationale security requirements (ASE_REQ.1) 47
9.7.4 Derived security requirements (ASE_REQ.2) 48
9.8 Security problem definition (ASE_SPD) 49
9.8.1 Objectives 49
9.8.2 Security problem definition (ASE_SPD.1) 50
9.9 TOE summary specification (ASE_TSS) 50
9.9.1 Objectives 50
9.9.2 Component levelling 50
9.9.3 TOE summary specification (ASE_TSS.1) 51
9.9.4 TOE summary specification with architectural design summary (ASE_TSS.2) 51

10 Class ADV Development 52
10.1 Introduction 52
10.2 Security architecture (ADV_ARC) 57
10.2.1 Objectives 57
10.2.2 Component levelling 57
10.2.3 Application notes 57
10.2.4 Security architecture description (ADV_ARC.1) 58
10.3 Composite design compliance (ADV_COMP) 59
10.3.1 Objectives 59
10.3.2 Component levelling 59
10.3.3 Application notes 59
10.3.4 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority (ADV_COMP.1) 60
10.4 Functional specification (ADV_FSP) 60
10.4.1 Objectives 60
10.4.2 Component levelling 61
10.4.3 Application notes 61
10.4.4 Basic functional specification (ADV_FSP.1) 63
10.4.5 Security-enforcing functional specification (ADV_FSP.2) 64
10.4.6 Functional specification with complete summary (ADV_FSP.3) 65
10.4.7 Complete functional specification (ADV_FSP.4) 66
10.4.8 Complete semi-formal functional specification with additional error information (ADV_FSP.5) 66
10.4.9 Complete semi-formal functional specification with additional formal specification (ADV_FSP.6) 68
10.5 Implementation representation (ADV_IMP) 69
10.5.1 Objectives 69
10.5.2 Component levelling 69
10.5.3 Application notes 69
10.5.4 Implementation representation of the TSF (ADV_IMP.1) 70
10.5.5 Complete mapping of the implementation representation of the TSF (ADV_IMP.2) 71
10.6 TSF internals (ADV_INT) 71
10.6.1 Objectives 71
10.6.2 Component levelling 72
10.6.3 Application notes 72
10.6.4 Well-structured subset of TSF internals (ADV_INT.1) 72
10.6.5 Well-structured internals (ADV_INT.2) 73
10.6.6 Minimally complex internals (ADV_INT.3) 74
10.7 Formal TSF model (ADV_SPM) 75
10.7.1 Objectives 75

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

© ISO/IEC 2024 – All rights reserved

10.7.2 Component levelling 75
10.7.3 Application notes 75
10.7.4 Formal TSF model (ADV_SPM.1) 76
10.8 TOE design (ADV_TDS) 77
10.8.1 Objectives 77
10.8.2 Component levelling 77
10.8.3 Application notes 77
10.8.4 Basic design (ADV_TDS.1) 79
10.8.5 Architectural design (ADV_TDS.2) 80
10.8.6 Basic modular design (ADV_TDS.3) 81
10.8.7 Semi-Formal modular design (ADV_TDS.4) 82
10.8.8 Complete semi-formal modular design (ADV_TDS.5) 83
10.8.9 Complete semi-formal modular design with formal high-level design presentation (ADV_TDS.6) 84

11 Class AGD Guidance documents 85
11.1 Introduction 85
11.2 Operational user guidance (AGD_OPE) 86
11.2.1 Objectives 86
11.2.2 Component levelling 86
11.2.3 Application notes 87
11.2.4 Operational user guidance (AGD_OPE.1) 87
11.3 Preparative procedures (AGD_PRE) 88
11.3.1 Objectives 88
11.3.2 Component levelling 88
11.3.3 Application notes 88
11.3.4 Preparative procedures (AGD_PRE.1) 89

12 Class ALC Life-cycle support 89
12.1 Introduction 89
12.2 CM capabilities (ALC_CMC) 91
12.2.1 Objectives 91
12.2.2 Component levelling 92
12.2.3 Application notes 92
12.2.4 Labelling of the TOE (ALC_CMC.1) 92
12.2.5 Use of the CM system (ALC_CMC.2) 93
12.2.6 Authorization controls (ALC_CMC.3) 94
12.2.7 Production support, acceptance procedures and automation (ALC_CMC.4) 95
12.2.8 Advanced support (ALC_CMC.5) 97
12.3 CM scope (ALC_CMS) 99
12.3.1 Objectives 99
12.3.2 Component levelling 99
12.3.3 Application notes 99
12.3.4 TOE CM coverage (ALC_CMS.1) 99
12.3.5 Parts of the TOE CM coverage (ALC_CMS.2) 100
12.3.6 Implementation representation CM coverage (ALC_CMS.3) 101
12.3.7 Problem tracking CM coverage (ALC_CMS.4) 101
12.3.8 Development tools CM coverage (ALC_CMS.5) 102
12.4 Integration of composition parts and consistency check of delivery procedures (ALC_COMP) 103
12.4.1 Objectives 103
12.4.2 Component levelling 103
12.4.3 Application notes 103
12.4.4 Integration of the dependent component into the related base component and Consistency check for delivery and acceptance procedures (ALC_COMP.1) 104
12.5 Delivery (ALC_DEL) 105
12.5.1 Objectives 105
12.5.2 Component levelling 105
12.5.3 Application notes 105
12.5.4 Delivery procedures (ALC_DEL.1) 105

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/...30-99b7-544ae8be70fe/osist-pren-iso-iec-15408-3-2024

oSIST prEN ISO/IEC 15408-3:2024

12.6 Developer environment security (ALC_DVS) 106
12.6.1 Objectives 106
12.6.2 Component levelling 106
12.6.3 Application notes 106
12.6.4 Identification of security controls (ALC_DVS.1) 106
12.6.5 Sufficiency of security controls (ALC_DVS.2) 107
12.7 Flaw remediation (ALC_FLR) 107
12.7.1 Objectives 107
12.7.2 Component levelling 107
12.7.3 Application notes 108
12.7.4 Basic flaw remediation (ALC_FLR.1) 108
12.7.5 Flaw reporting procedures (ALC_FLR.2) 109
12.7.6 Systematic flaw remediation (ALC_FLR.3) 110
12.8 Development life-cycle definition (ALC_LCD) 111
12.8.1 Objectives 111
12.8.2 Component levelling 111
12.8.3 Application notes 112
12.8.4 Developer defined life-cycle processes (ALC_LCD.1) 112
12.8.5 Measurable life-cycle model (ALC_LCD.2) 113
12.9 Tools and techniques (ALC_TAT) 114
12.9.1 Objectives 114
12.9.2 Component levelling 114
12.9.3 Application notes 114
12.9.4 Well-defined development tools (ALC_TAT.1) 114
12.9.5 Compliance with implementation standards (ALC_TAT.2) 115
12.9.6 Compliance with implementation standards - all parts (ALC_TAT.3) 116
12.10 TOE development artefacts (ALC_TDA) 116
12.10.1 Objectives 116
12.10.2 Component levelling 117
12.10.3 Application notes 117
12.10.4 Uniquely identifying implementation representation (ALC_TDA.1) 117
12.10.5 Matching CMS scope of implementation representation (ALC_TDA.2) 119
12.10.6 Regenerate TOE with well-defined development tools (ALC_TDA.3) 121
13 Class ATE Tests 124
13.1 Introduction 124
13.2 Composite functional testing (ATE_COMP) 125
13.2.1 Objectives 125
13.2.2 Component levelling 125
13.2.3 Application notes 125
13.2.4 Composite product functional testing (ATE_COMP.1) 126
13.3 Coverage (ATE_COV) 126
13.3.1 Objectives 126
13.3.2 Component levelling 126
13.3.3 Evidence of coverage (ATE_COV.1) 127
13.3.4 Analysis of coverage (ATE_COV.2) 127
13.3.5 Rigorous analysis of coverage (ATE_COV.3) 128
13.4 Depth (ATE_DPT) 129
13.4.1 Objectives 129
13.4.2 Component levelling 129
13.4.3 Application notes 129
13.4.4 Testing: basic design (ATE_DPT.1) 129
13.4.5 Testing: security enforcing modules (ATE_DPT.2) 130
13.4.6 Testing: modular design (ATE_DPT.3) 131
13.4.7 Testing: implementation representation (ATE_DPT.4) 131
13.5 Functional tests (ATE_FUN) 132
13.5.1 Objectives 132
13.5.2 Component levelling 132
13.5.3 Application notes 133

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

13.5.4 Functional testing (ATE_FUN.1) 133
13.5.5 Ordered functional testing (ATE_FUN.2) 134
13.6 Independent testing (ATE_IND) 135
13.6.1 Objectives 135
13.6.2 Component levelling 135
13.6.3 Application notes 135
13.6.4 Independent testing - conformance (ATE_IND.1) 135
13.6.5 Independent testing - sample (ATE_IND.2) 136
13.6.6 Independent testing - complete (ATE_IND.3) 137
14 Class AVA Vulnerability assessment 138
14.1 Introduction 138
14.2 Application notes 139
14.3 Composite vulnerability assessment (AVA_COMP) 140
14.3.1 Objectives 140
14.3.2 Component levelling 140
14.3.3 Application notes 140
14.3.4 Composite product vulnerability assessment (AVA_COMP.1) 141
14.4 Vulnerability analysis (AVA_VAN) 141
14.4.1 Objectives 141
14.4.2 Component levelling 141
14.4.3 Vulnerability survey (AVA_VAN.1) 141
14.4.4 Vulnerability analysis (AVA_VAN.2) 142
14.4.5 Focused vulnerability analysis (AVA_VAN.3) 143
14.4.6 Methodical vulnerability analysis (AVA_VAN.4) 144
14.4.7 Advanced methodical vulnerability analysis (AVA_VAN.5) 145
15 Class ACO Composition 147
15.1 Introduction 147
15.2 Composition rationale (ACO_COR) 150
15.2.1 Objectives 150
15.2.2 Component levelling 151
15.2.3 Composition rationale (ACO_COR.1) 151
15.3 Composed TOE testing (ACO_CTT) 151
15.3.1 Objectives 151
15.3.2 Component levelling 151
15.3.3 Application notes 151
15.3.4 Interface testing (ACO_CTT.1) 152
15.3.5 Rigorous interface testing (ACO_CTT.2) 153
15.4 Development evidence (ACO_DEV) 154
15.4.1 Objectives 154
15.4.2 Component levelling 154
15.4.3 Application notes 154
15.4.4 Functional description (ACO_DEV.1) 155
15.4.5 Basic evidence of design (ACO_DEV.2) 156
15.4.6 Detailed evidence of design (ACO_DEV.3) 156
15.5 Reliance of dependent component (ACO_REL) 157
15.5.1 Objectives 157
15.5.2 Component levelling 158
15.5.3 Application notes 158
15.5.4 Basic reliance information (ACO_REL.1) 158
15.5.5 Reliance information (ACO_REL.2) 158
15.6 Composition vulnerability analysis (ACO_VUL) 159
15.6.1 Objectives 159
15.6.2 Component levelling 159
15.6.3 Application notes 159
15.6.4 Composition vulnerability review (ACO_VUL.1) 160
15.6.5 Composition vulnerability analysis (ACO_VUL.2) 160
15.6.6 Enhanced-Basic composition vulnerability analysis (ACO_VUL.3) 161

iTeh Standards
(https://standards.iteh.ai)
Document Preview
oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/a65d44ef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

Annex A (informative) **Development (ADV)** 163
Annex B (informative) **Composition (ACO)** 183
Bibliography 190

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

© ISO/IEC 2024 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO *[had/had not]* received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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.

iTeh Standards (https://standards.iteh.ai) Document Preview

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

This fifth edition cancels and replaces the fourth edition (ISO 15408-3:2022), which has been technically revised.

The main changes are as follows:

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

- the terminology has been reviewed and updated;
- a missing developer action element has been added (ADV_SPM.1.7D).

A list of all parts in the ISO 15408 series can be found on the ISO website.

The catalogue of security assurance requirements defined in this document is provided in machine readable format (XML) at: https://standards.iso.org/iso-iec/TBD.

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.

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 (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale 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
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Centro Criptológico Nacional
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency and the National Institute of Standards and Technology

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

Introduction

Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PP-Configuration, or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs.

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

- Consumers, who use this document when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE.
- Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this document when interpreting statements of assurance requirements and determining assurance approaches of TOEs.
- Evaluators, who use the assurance requirements defined in this document as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

NOTE 1 This document uses bold type to highlight hierarchical relationships between requirements. This convention calls for the use of bold type for all new requirements.

NOTE 2 For security assurance requirements, special verbs relating to mandatory evaluation activities are presented in bold italic type.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

oSIST prEN ISO/IEC 15408-3:2024
https://standards.iteh.ai/catalog/standards/sist/ac5d4fef-c586-4b30-99b7-544ae8be70fc/osist-pren-iso-iec-15408-3-2024

© ISO/IEC 2024 – All rights reserved