DIN EN ISO/IEC 15408-3

DIN

ICS 35.030

Entwurf

Einsprüche bis 2019-12-11
Vorgesehen als Ersatz für
die 2011-03 zurückgezogene
Norm
DIN ISO/IEC 15408-3:2007-11

Informationstechnik – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit – Teil 3: Komponenten zur Sicherheitskontrolle (ISO/IEC 15408-3:2008); Englische Fassung prEN ISO/IEC 15408-3:2019

Information technology –
Security techniques – Evaluation criteria for IT security –
Part 3: Security assurance components (ISO/IEC 15408-3:2008);
English version prEN ISO/IEC 15408-3:2019

Technologies de l'information –
Techniques de sécurité – Critères d'évaluation pour la sécurité TI –
Partie 3: Composants d'assurance de sécurité (ISO/IEC 15408-3:2008);
Version anglaise prEN ISO/IEC 15408-3:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-11 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 186 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Nationales Vorwort

Der Text von ISO/IEC 15408-3:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 15408-3:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieser Europäische Norm-Entwurf enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO/IEC Norm.

Änderungen

Gegenüber der bereits 2011-03 zurückgezogenen Norm DIN ISO/IEC 15408-3:2007-11 wurden folgende Änderungen vorgenommen:

a) redaktionelle Überarbeitung, insbesondere bezogen auf ADV_FSP, ADV_TDS, ATE_DPT.2, ATE_IND und ALC;

b) Aktualisierung des technischen Inhalts

Nationaler Anhang NA
(informativ)

Begriffe und Abkürzungen

3. Begriffe, Symbole und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Contents

Page

Foreword ix
Introduction xi
1 Scope 1
2 Normative references 1
3 Terms and definitions, symbols and abbreviated terms 1
4 Overview 1
4.1 Organisation of this part of ISO/IEC 15408 1
5 Assurance paradigm 2
5.1 ISO/IEC 15408 philosophy 2
5.2 Assurance approach 2
5.2.1 Significance of vulnerabilities 2
5.2.2 Cause of vulnerabilities 3
5.2.3 ISO/IEC 15408 assurance 3
5.2.4 Assurance through evaluation 3
5.3 ISO/IEC 15408 evaluation assurance scale 3
6 Security assurance components 4
6.1 Security assurance classes, families and components structure 4
6.1.1 Assurance class structure 4
6.1.2 Assurance family structure 5
6.1.3 Assurance component structure 6
6.1.4 Assurance elements 8
6.1.5 Component taxonomy 8
6.2 EAL structure 9
6.2.1 EAL name 9
6.2.2 Objectives 9
6.2.3 Application notes 9
6.2.4 Assurance components 10
6.2.5 Relationship between assurances and assurance levels 10
6.3 CAP structure 11
6.3.1 CAP name 11
6.3.2 Objectives 11
6.3.3 Application notes 11
6.3.4 Assurance components 12
6.3.5 Relationship between assurances and assurance levels 13
7 Evaluation assurance levels 13
7.1 Evaluation assurance level (EAL) overview 14
7.2 Evaluation assurance level details 15
7.3 Evaluation assurance level 1 (EAL1) - functionally tested 15
7.3.1 Objectives 15
7.3.2 Assurance components 16
7.4 Evaluation assurance level 2 (EAL2) - structurally tested 16
7.4.1 Objectives 16
7.4.2 Assurance components 16
7.5 Evaluation assurance level 3 (EAL3) - methodically tested and checked 17
7.5.1 Objectives 17
7.5.2 Assurance components 17
7.6 Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed 18
7.6.1 Objectives 18
7.6.2 Assurance components 18

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

7.7 Evaluation assurance level 5 (EAL5) - semiformally designed and tested 19
7.7.1 Objectives 19
7.7.2 Assurance components 19
7.8 Evaluation assurance level 6 (EAL6) - semiformally verified design and tested 20
7.8.1 Objectives 20
7.8.2 Assurance components 20
7.9 Evaluation assurance level 7 (EAL7) - formally verified design and tested 21
7.9.1 Objectives 21
7.9.2 Assurance components 22

8 Composed assurance packages 23
8.1 Composed assurance package (CAP) overview 23
8.2 Composed assurance package details 24
8.3 Composition assurance level A (CAP-A) - Structurally composed 24
8.3.1 Objectives 24
8.3.2 Assurance components 24
8.4 Composition assurance level B (CAP-B) - Methodically composed 25
8.4.1 Objectives 25
8.4.2 Assurance components 25
8.5 Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed 26
8.5.1 Objectives 26
8.5.2 Assurance components 26

9 Class APE: Protection Profile evaluation 27
9.1 PP introduction (APE_INT) 28
9.1.1 Objectives 28
9.1.2 APE_INT.1 PP introduction 28
9.2 Conformance claims (APE_CCL) 29
9.2.1 Objectives 29
9.2.2 APE_CCL.1 Conformance claims 29
9.3 Security problem definition (APE_SPD) 31
9.3.1 Objectives 31
9.3.2 APE_SPD.1 Security problem definition 31
9.4 Security objectives (APE_OBJ) 31
9.4.1 Objectives 31
9.4.2 Component levelling 32
9.4.3 APE_OBJ.1 Security objectives for the operational environment 32
9.4.4 APE_OBJ.2 Security objectives 32
9.5 Extended components definition (APE_ECD) 33
9.5.1 Objectives 33
9.5.2 APE_ECD.1 Extended components definition 33
9.6 Security requirements (APE_REQ) 34
9.6.1 Objectives 34
9.6.2 Component levelling 34
9.6.3 APE_REQ.1 Stated security requirements 34
9.6.4 APE_REQ.2 Derived security requirements 35

10 Class ASE: Security Target evaluation 36
10.1 ST introduction (ASE_INT) 37
10.1.1 Objectives 37
10.1.2 ASE_INT.1 ST introduction 37
10.2 Conformance claims (ASE_CCL) 38
10.2.1 Objectives 38
10.2.2 ASE_CCL.1 Conformance claims 38
10.3 Security problem definition (ASE_SPD) 40
10.3.1 Objectives 40
10.3.2 ASE_SPD.1 Security problem definition 40
10.4 Security objectives (ASE_OBJ) 41
10.4.1 Objectives 41
10.4.2 Component levelling 41
10.4.3 ASE_OBJ.1 Security objectives for the operational environment 41

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

10.4.4 ASE_OBJ.2 Security objectives 41
10.5 Extended components definition (ASE_ECD) 42
10.5.1 Objectives 42
10.5.2 ASE_ECD.1 Extended components definition 42
10.6 Security requirements (ASE_REQ) 43
10.6.1 Objectives 43
10.6.2 Component levelling 43
10.6.3 ASE_REQ.1 Stated security requirements 44
10.6.4 ASE_REQ.2 Derived security requirements 44
10.7 TOE summary specification (ASE_TSS) 46
10.7.1 Objectives 46
10.7.2 Component levelling 46
10.7.3 ASE_TSS.1 TOE summary specification 46
10.7.4 ASE_TSS.2 TOE summary specification with architectural design summary 47

11 Class ADV: Development 48
11.1 Security Architecture (ADV_ARC) 52
11.1.1 Objectives 52
11.1.2 Component levelling 52
11.1.3 Application notes 52
11.1.4 ADV_ARC.1 Security architecture description 53
11.2 Functional specification (ADV_FSP) 54
11.2.1 Objectives 54
11.2.2 Component levelling 54
11.2.3 Application notes 54
11.2.4 ADV_FSP.1 Basic functional specification 56
11.2.5 ADV_FSP.2 Security-enforcing functional specification 57
11.2.6 ADV_FSP.3 Functional specification with complete summary 58
11.2.7 ADV_FSP.4 Complete functional specification 59
11.2.8 ADV_FSP.5 Complete semi-formal functional specification with additional error information 60
11.2.9 ADV_FSP.6 Complete semi-formal functional specification with additional formal specification 61
11.3 Implementation representation (ADV_IMP) 63
11.3.1 Objectives 63
11.3.2 Component levelling 63
11.3.3 Application notes 63
11.3.4 ADV_IMP.1 Implementation representation of the TSF 64
11.3.5 ADV_IMP.2 Complete mapping of the implementation representation of the TSF 64
11.4 TSF internals (ADV_INT) 65
11.4.1 Objectives 65
11.4.2 Component levelling 65
11.4.3 Application notes 65
11.4.4 ADV_INT.1 Well-structured subset of TSF internals 66
11.4.5 ADV_INT.2 Well-structured internals 67
11.4.6 ADV_INT.3 Minimally complex internals 68
11.5 Security policy modelling (ADV_SPM) 69
11.5.1 Objectives 69
11.5.2 Component levelling 69
11.5.3 Application notes 69
11.5.4 ADV_SPM.1 Formal TOE security policy model 70
11.6 TOE design (ADV_TDS) 71
11.6.1 Objectives 71
11.6.2 Component levelling 71
11.6.3 Application notes 71
11.6.4 ADV_TDS.1 Basic design 72
11.6.5 ADV_TDS.2 Architectural design 73
11.6.6 ADV_TDS.3 Basic modular design 74
11.6.7 ADV_TDS.4 Semiformal modular design 76
11.6.8 ADV_TDS.5 Complete semiformal modular design 77

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

11.6.9 ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation 78
12 Class AGD: Guidance documents 80
12.1 Operational user guidance (AGD_OPE) 80
12.1.1 Objectives 80
12.1.2 Component levelling 81
12.1.3 Application notes 81
12.1.4 AGD_OPE.1 Operational user guidance 81
12.2 Preparative procedures (AGD_PRE) 82
12.2.1 Objectives 82
12.2.2 Component levelling 82
12.2.3 Application notes 82
12.2.4 AGD_PRE.1 Preparative procedures 83
13 Class ALC: Life-cycle support 83
13.1 CM capabilities (ALC_CMC) 84
13.1.1 Objectives 84
13.1.2 Component levelling 85
13.1.3 Application notes 85
13.1.4 ALC_CMC.1 Labelling of the TOE 85
13.1.5 ALC_CMC.2 Use of a CM system 86
13.1.6 ALC_CMC.3 Authorisation controls 87
13.1.7 ALC_CMC.4 Production support, acceptance procedures and automation 88
13.1.8 ALC_CMC.5 Advanced support 90
13.2 CM scope (ALC_CMS) 92
13.2.1 Objectives 92
13.2.2 Component levelling 93
13.2.3 Application notes 93
13.2.4 ALC_CMS.1 TOE CM coverage 93
13.2.5 ALC_CMS.2 Parts of the TOE CM coverage 93
13.2.6 ALC_CMS.3 Implementation representation CM coverage 94
13.2.7 ALC_CMS.4 Problem tracking CM coverage 95
13.2.8 ALC_CMS.5 Development tools CM coverage 96
13.3 Delivery (ALC_DEL) 97
13.3.1 Objectives 97
13.3.2 Component levelling 97
13.3.3 Application notes 97
13.3.4 ALC_DEL.1 Delivery procedures 98
13.4 Development security (ALC_DVS) 98
13.4.1 Objectives 98
13.4.2 Component levelling 98
13.4.3 Application notes 98
13.4.4 ALC_DVS.1 Identification of security measures 99
13.4.5 ALC_DVS.2 Sufficiency of security measures 99
13.5 Flaw remediation (ALC_FLR) 100
13.5.1 Objectives 100
13.5.2 Component levelling 100
13.5.3 Application notes 100
13.5.4 ALC_FLR.1 Basic flaw remediation 100
13.5.5 ALC_FLR.2 Flaw reporting procedures 101
13.5.6 ALC_FLR.3 Systematic flaw remediation 102
13.6 Life-cycle definition (ALC_LCD) 104
13.6.1 Objectives 104
13.6.2 Component levelling 104
13.6.3 Application notes 104
13.6.4 ALC_LCD.1 Developer defined life-cycle model 105
13.6.5 ALC_LCD.2 Measurable life-cycle model 106
13.7 Tools and techniques (ALC_TAT) 106
13.7.1 Objectives 106
13.7.2 Component levelling 107

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

13.7.3 Application notes 107
13.7.4 ALC_TAT.1 Well-defined development tools 107
13.7.5 ALC_TAT.2 Compliance with implementation standards 108
13.7.6 ALC_TAT.3 Compliance with implementation standards - all parts 108

14 Class ATE: Tests 109
14.1 Coverage (ATE_COV) 110
14.1.1 Objectives 110
14.1.2 Component levelling 110
14.1.3 Application notes 110
14.1.4 ATE_COV.1 Evidence of coverage 110
14.1.5 ATE_COV.2 Analysis of coverage 111
14.1.6 ATE_COV.3 Rigorous analysis of coverage 112
14.2 Depth (ATE_DPT) 112
14.2.1 Objectives 112
14.2.2 Component levelling 113
14.2.3 Application notes 113
14.2.4 ATE_DPT.1 Testing: basic design 113
14.2.5 ATE_DPT.2 Testing: security enforcing modules 114
14.2.6 ATE_DPT.3 Testing: modular design 114
14.2.7 ATE_DPT.4 Testing: implementation representation 115
14.3 Functional tests (ATE_FUN) 116
14.3.1 Objectives 116
14.3.2 Component levelling 116
14.3.3 Application notes 116
14.3.4 ATE_FUN.1 Functional testing 117
14.3.5 ATE_FUN.2 Ordered functional testing 117
14.4 Independent testing (ATE_IND) 118
14.4.1 Objectives 118
14.4.2 Component levelling 118
14.4.3 Application notes 119
14.4.4 ATE_IND.1 Independent testing - conformance 119
14.4.5 ATE_IND.2 Independent testing - sample 120
14.4.6 ATE_IND.3 Independent testing - complete 121

15 Class AVA: Vulnerability assessment 122
15.1 Application notes 122
15.2 Vulnerability analysis (AVA_VAN) 123
15.2.1 Objectives 123
15.2.2 Component levelling 123
15.2.3 AVA_VAN.1 Vulnerability survey 123
15.2.4 AVA_VAN.2 Vulnerability analysis 124
15.2.5 AVA_VAN.3 Focused vulnerability analysis 125
15.2.6 AVA_VAN.4 Methodical vulnerability analysis 126
15.2.7 AVA_VAN.5 Advanced methodical vulnerability analysis 127

16 Class ACO: Composition 128
16.1 Composition rationale (ACO_COR) 130
16.1.1 Objectives 130
16.1.2 Component levelling 130
16.1.3 ACO_COR.1 Composition rationale 131
16.2 Development evidence (ACO_DEV) 131
16.2.1 Objectives 131
16.2.2 Component levelling 131
16.2.3 Application notes 131
16.2.4 ACO_DEV.1 Functional Description 132
16.2.5 ACO_DEV.2 Basic evidence of design 132
16.2.6 ACO_DEV.3 Detailed evidence of design 133
16.3 Reliance of dependent component (ACO_REL) 134
16.3.1 Objectives 134
16.3.2 Component levelling 135

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

16.3.3 Application notes 135
16.3.4 ACO_REL.1 Basic reliance information 135
16.3.5 ACO_REL.2 Reliance information 136
16.4 Composed TOE testing (ACO_CTT) 136
16.4.1 Objectives 136
16.4.2 Component levelling 136
16.4.3 Application notes 136
16.4.4 ACO_CTT.1 Interface testing 137
16.4.5 ACO_CTT.2 Rigorous interface testing 138
16.5 Composition vulnerability analysis (ACO_VUL) 139
16.5.1 Objectives 139
16.5.2 Component levelling 139
16.5.3 Application notes 140
16.5.4 ACO_VUL.1 Composition vulnerability review 140
16.5.5 ACO_VUL.2 Composition vulnerability analysis 141
16.5.6 ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis 141

Annex A (informative) Development (ADV) 143
A.1 ADV_ARC: Supplementary material on security architectures 143
A.1.1 Security architecture properties 143
A.1.2 Security architecture descriptions 144
A.2 ADV_FSP: Supplementary material on TSFIs 146
A.2.1 Determining the TSFI 146
A.2.2 Example: A complex DBMS 148
A.2.3 Example Functional Specification 149
A.3 ADV_INT: Supplementary material on TSF internals 151
A.3.1 Structure of procedural software 151
A.3.2 Complexity of procedural software 153
A.4 ADV_TDS: Subsystems and Modules 154
A.4.1 Subsystems 154
A.4.2 Modules 155
A.4.3 Levelling Approach 157
A.5 Supplementary material on formal methods 159

Annex B (informative) Composition (ACO) 161
B.1 Necessity for composed TOE evaluations 161
B.2 Performing Security Target evaluation for a composed TOE 162
B.3 Interactions between composed IT entities 163

Annex C (informative) Cross reference of assurance component dependencies 168

Annex D (informative) Cross reference of PPs and assurance components 172

Annex E (informative) Cross reference of EALs and assurance components 173

Annex F (informative) Cross reference of CAPs and assurance components 174

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

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 document 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 15408-3 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 15408-3:2005), 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*

This corrected version of ISO/IEC 15408-3:2008 incorporates miscellaneous editorial corrections mainly related to EAL4 and EAL6 assurance components, ADV_FSP, ADV_TDS, ATE_DPT.2, ATE_IND, and ALC.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

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, version 3.1 Parts 1 through 3 (called CC 3.1), they hereby grant non-exclusive license to ISO/IEC to use CC 3.1 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 3.1 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale 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;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Introduction

Security assurance components, as defined in this part of ISO/IEC 15408, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogues the set of assurance components, families and classes. This part of ISO/IEC 15408 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for Targets of Evaluation (TOEs), which is called the Evaluation Assurance Levels (EALs).

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1:2009, Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

a) Consumers, who use this part of ISO/IEC 15408 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.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part of ISO/IEC 15408 when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this part of ISO/IEC 15408 as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Information technology Security techniques — Evaluation criteria for IT security —

Part 3:
Security assurance components

1 Scope

This part of ISO/IEC 15408 defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component Targets of Evaluation (TOEs), the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).

2 Normative references

The following referenced documents are indispensable for the application 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, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

3 Terms and definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

4 Overview

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security assurance requirements of this part of ISO/IEC 15408.

Clause 6 describes the presentation structure of the assurance classes, families, components, evaluation assurance levels along with their relationships, and the structure of the composed assurance packages. It also characterises the assurance classes and families found in Clauses 9 through 16.

Clause 7 provides detailed definitions of the EALs.

Clause 8 provides detailed definitions of the CAPs.

Clauses 9 through 16 provide the detailed definitions of this part of ISO/IEC 15408 assurance classes.

Annex A provides further explanations and examples of the concepts behind the Development class.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Annex B provides an explanation of the concepts behind composed TOE evaluations and the Composition class.

Annex C provides a summary of the dependencies between the assurance components.

Annex D provides a cross reference between PPs and the families and components of the APE class.

Annex E provides a cross reference between the EALs and the assurance components.

Annex F provides a cross reference between the CAPs and the assurance components.

5 Assurance paradigm

The purpose of this clause is to document the philosophy that underpins ISO/IEC 15408 approach to assurance. An understanding of this clause will permit the reader to understand the rationale behind this part of ISO/IEC 15408 assurance requirements.

5.1 ISO/IEC 15408 philosophy

ISO/IEC 15408 philosophy is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security measures be demonstrably sufficient for their intended purpose.

Furthermore, measures should be adopted that reduce the likelihood of vulnerabilities, the ability to exercise (i.e. intentionally exploit or unintentionally trigger) a vulnerability, and the extent of the damage that could occur from a vulnerability being exercised. Additionally, measures should be adopted that facilitate the subsequent identification of vulnerabilities and the elimination, mitigation, and/or notification that a vulnerability has been exploited or triggered.

5.2 Assurance approach

ISO/IEC 15408 philosophy is to provide assurance based upon an evaluation (active investigation) of the IT product that is to be trusted. Evaluation has been the traditional means of providing assurance and is the basis for prior evaluation criteria documents. In aligning the existing approaches, ISO/IEC 15408 adopts the same philosophy. ISO/IEC 15408 proposes measuring the validity of the documentation and of the resulting IT product by expert evaluators with increasing emphasis on scope, depth, and rigour.

ISO/IEC 15408 does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance. Research continues with respect to alternative ways of gaining assurance. As mature alternative approaches emerge from these research activities, they will be considered for inclusion in ISO/IEC 15408, which is so structured as to allow their future introduction.

5.2.1 Significance of vulnerabilities

It is assumed that there are threat agents that will actively seek to exploit opportunities to violate security policies both for illicit gains and for well-intentioned, but nonetheless insecure actions. Threat agents may also accidentally trigger security vulnerabilities, causing harm to the organisation. Due to the need to process sensitive information and the lack of availability of sufficiently trusted products, there is significant risk due to failures of IT. It is, therefore, likely that IT security breaches could lead to significant loss.

IT security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the application of IT within business concerns.

Steps should be taken to prevent vulnerabilities arising in IT products. To the extent feasible, vulnerabilities should be:

a) eliminated -- that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;

AVA Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

b) minimised -- that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;

c) monitored -- that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

5.2.2 Cause of vulnerabilities

Vulnerabilities can arise through failures in:

a) requirements -- that is, an IT product may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;

b) development -- that is, an IT product does not meet its specifications and/or vulnerabilities have been introduced as a result of poor development standards or incorrect design choices;

c) operation -- that is, an IT product has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

5.2.3 ISO/IEC 15408 assurance

Assurance is grounds for confidence that an IT product meets its security objectives. Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, ISO/IEC 15408 provides assurance through active investigation. Active investigation is an evaluation of the IT product in order to determine its security properties.

5.2.4 Assurance through evaluation

Evaluation has been the traditional means of gaining assurance, and is the basis of ISO/IEC 15408 approach. Evaluation techniques can include, but are not limited to:

a) analysis and checking of process(es) and procedure(s);

b) checking that process(es) and procedure(s) are being applied;

c) analysis of the correspondence between TOE design representations;

d) analysis of the TOE design representation against the requirements;

e) verification of proofs;

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

5.3 ISO/IEC 15408 evaluation assurance scale

ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon:

a) scope -- that is, the effort is greater because a larger portion of the IT product is included;

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

b) depth -- that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

c) rigour -- that is, the effort is greater because it is applied in a more structured, formal manner.

6 Security assurance components

6.1 Security assurance classes, families and components structure

The following subclauses describe the constructs used in representing the assurance classes, families, and components.

Figure 1 illustrates the SARs defined in this part of ISO/IEC 15408. Note that the most abstract collection of SARs is referred to as a class. Each class contains assurance families, which then contain assurance components, which in turn contain assurance elements. Classes and families are used to provide a taxonomy for classifying SARs, while components are used to specify SARs in a PP/ST.

6.1.1 Assurance class structure

Figure 1 illustrates the assurance class structure.

6.1.1.1 Class name

Each assurance class is assigned a unique name. The name indicates the topics covered by the assurance class.

A unique short form of the assurance class name is also provided. This is the primary means for referencing the assurance class. The convention adopted is an “A” followed by two letters related to the class name.

6.1.1.2 Class introduction

Each assurance class has an introductory subclause that describes the composition of the class and contains supportive text covering the intent of the class.

6.1.1.3 Assurance families

Each assurance class contains at least one assurance family. The structure of the assurance families is described in the following subclause.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

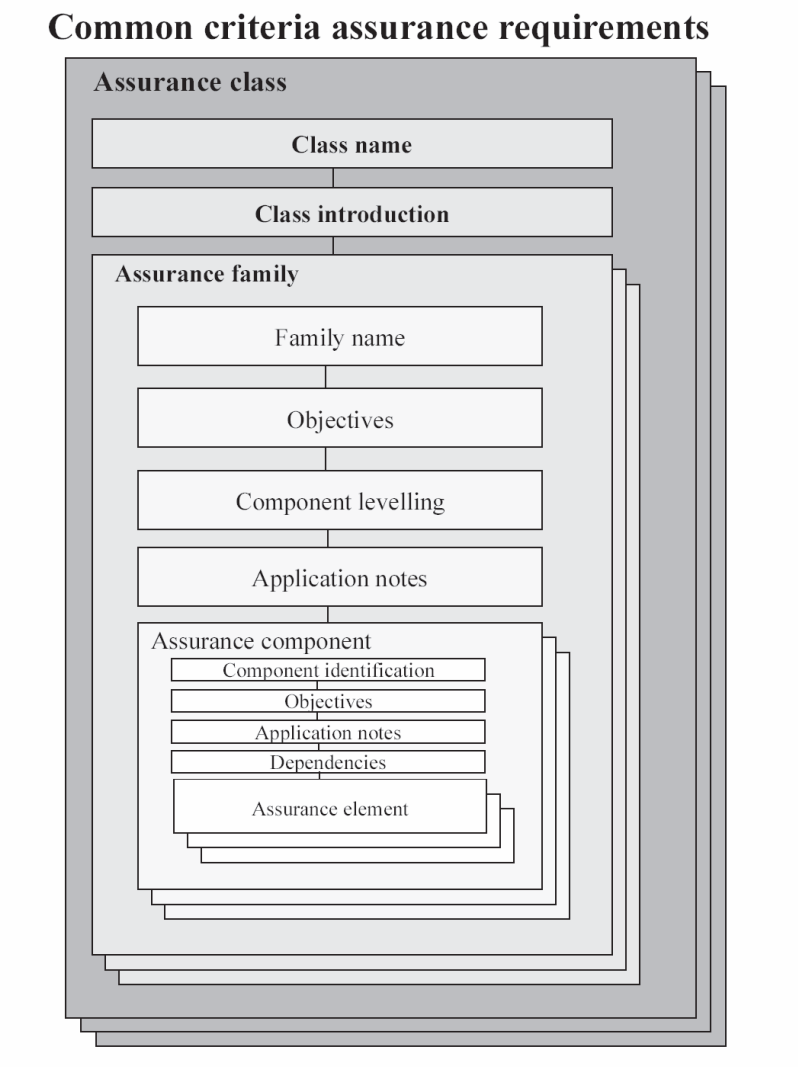


Figure 1 — Assurance class/family/component/element hierarchy

6.1.2 Assurance family structure

Figure 1 illustrates the assurance family structure.

6.1.2.1 Family name

Every assurance family is assigned a unique name. The name provides descriptive information about the topics covered by the assurance family. Each assurance family is placed within the assurance class that contains other families with the same intent.

A unique short form of the assurance family name is also provided. This is the primary means used to reference the assurance family. The convention adopted is that the short form of the class name is used, followed by an underscore, and then three letters related to the family name.

6.1.2.2 Objectives

The objectives subclause of the assurance family presents the intent of the assurance family.

This subclause describes the objectives, particularly those related to ISO/IEC 15408 assurance paradigm, that the family is intended to address. The description for the assurance family is kept at a general level. Any specific details required for objectives are incorporated in the particular assurance component.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

6.1.2.3 Component levelling

Each assurance family contains one or more assurance components. This subclause of the assurance family describes the components available and explains the distinctions between them. Its main purpose is to differentiate between the assurance components once it has been determined that the assurance family is a necessary or useful part of the SARs for a PP/ST.

Assurance families containing more than one component are levelled and rationale is provided as to how the components are levelled. This rationale is in terms of scope, depth, and/or rigour.

6.1.2.4 Application notes

The application notes subclause of the assurance family, if present, contains additional information for the assurance family. This information should be of particular interest to users of the assurance family (e.g. PP and ST authors, designers of TOEs, evaluators). The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

6.1.2.5 Assurance components

Each assurance family has at least one assurance component. The structure of the assurance components is provided in the following subclause.

6.1.3 Assurance component structure

Figure 2 illustrates the assurance component structure.

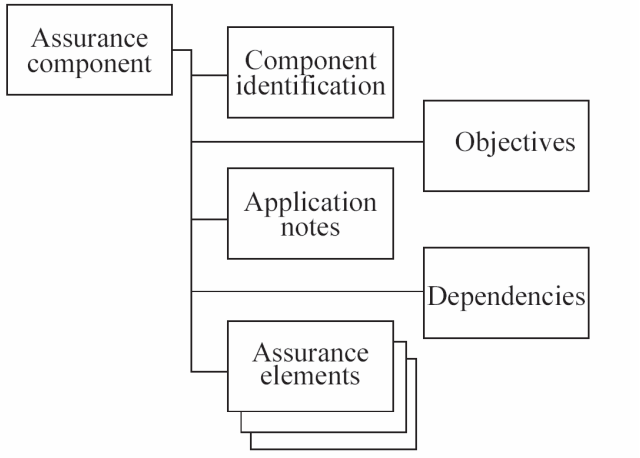


Figure 2 — Assurance component structure

The relationship between components within a family is highlighted using a bolding convention. Those parts of the requirements that are new, enhanced or modified beyond the requirements of the previous component within a hierarchy are bolded.

6.1.3.1 Component identification

The component identification subclause provides descriptive information necessary to identify, categorise, register, and reference a component.

Every assurance component is assigned a unique name. The name provides descriptive information about the topics covered by the assurance component. Each assurance component is placed within the assurance family that shares its security objective.

A unique short form of the assurance component name is also provided. This is the primary means used to reference the assurance component. The convention used is that the short form of the family name is used,

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

followed by a period, and then a numeric character. The numeric characters for the components within each family are assigned sequentially, starting from 1.

6.1.3.2 Objectives

The objectives subclause of the assurance component, if present, contains specific objectives for the particular assurance component. For those assurance components that have this subclause, it presents the specific intent of the component and a more detailed explanation of the objectives.

6.1.3.3 Application notes

The application notes subclause of an assurance component, if present, contains additional information to facilitate the use of the component.

6.1.3.4 Dependencies

Dependencies among assurance components arise when a component is not self-sufficient, and relies upon the presence of another component.

Each assurance component provides a complete list of dependencies to other assurance components. Some components may list “No dependencies”, to indicate that no dependencies have been identified. The components depended upon may have dependencies on other components.

The dependency list identifies the minimum set of assurance components which are relied upon. Components which are hierarchical to a component in the dependency list may also be used to satisfy the dependency.

In specific situations the indicated dependencies might not be applicable. The PP/ST author, by providing rationale for why a given dependency is not applicable, may elect not to satisfy that dependency.

6.1.3.5 Assurance elements

A set of assurance elements is provided for each assurance component. An assurance element is a security requirement which, if further divided, would not yield a meaningful evaluation result. It is the smallest security requirement recognised in ISO/IEC 15408.

Each assurance element is identified as belonging to one of the three sets of assurance elements:

a) Developer action elements: the activities that shall be performed by the developer. This set of actions is further qualified by evidential material referenced in the following set of elements. Requirements for developer actions are identified by appending the letter “D” to the element number.

b) Content and presentation of evidence elements: the evidence required, what the evidence shall demonstrate, and what information the evidence shall convey. Requirements for content and presentation of evidence are identified by appending the letter “C” to the element number.

c) Evaluator action elements: the activities that shall be performed by the evaluator. This set of actions explicitly includes confirmation that the requirements prescribed in the content and presentation of evidence elements have been met. It also includes explicit actions and analysis that shall be performed in addition to that already performed by the developer. Implicit evaluator actions are also to be performed as a result of developer action elements which are not covered by content and presentation of evidence requirements. Requirements for evaluator actions are identified by appending the letter “E” to the element number.

The developer actions and content and presentation of evidence define the assurance requirements that are used to represent a developer's responsibilities in demonstrating assurance in the TOE meeting the SFRs of a PP or ST.

The evaluator actions define the evaluator's responsibilities in the two aspects of evaluation. The first aspect is validation of the PP/ST, in accordance with the classes APE and ASE in Clauses APE: Protection Profile

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

evaluation and ASE: Security Target evaluation. The second aspect is verification of the TOE's conformance with its SFRs and SARs. By demonstrating that the PP/ST is valid and that the requirements are met by the TOE, the evaluator can provide a basis for confidence that the TOE in its operational environment solves the defined security problem.

The developer action elements, content and presentation of evidence elements, and explicit evaluator action elements, identify the evaluator effort that shall be expended in verifying the security claims made in the ST of the TOE.

6.1.4 Assurance elements

Each element represents a requirement to be met. These statements of requirements are intended to be clear, concise, and unambiguous. Therefore, there are no compound sentences: each separable requirement is stated as an individual element.

6.1.5 Component taxonomy

This part of ISO/IEC 15408 contains classes of families and components that are grouped on the basis of related assurance. At the start of each class is a diagram that indicates the families in the class and the components in each family.

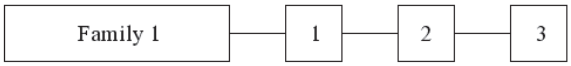


Figure 3 — Sample class decomposition diagram

In Figure 3, above, the class as shown contains a single family. The family contains three components that are linearly hierarchical (i.e. component 2 requires more than component 1, in terms of specific actions, specific evidence, or rigour of the actions or evidence). The assurance families in this part of ISO/IEC 15408 are all linearly hierarchical, although linearity is not a mandatory criterion for assurance families that may be added in the future.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

6.2 EAL structure

Figure 4 illustrates the EALs and associated structure defined in this part of ISO/IEC 15408. Note that while the figure shows the contents of the assurance components, it is intended that this information would be included in an EAL by reference to the actual components defined in ISO/IEC 15408.

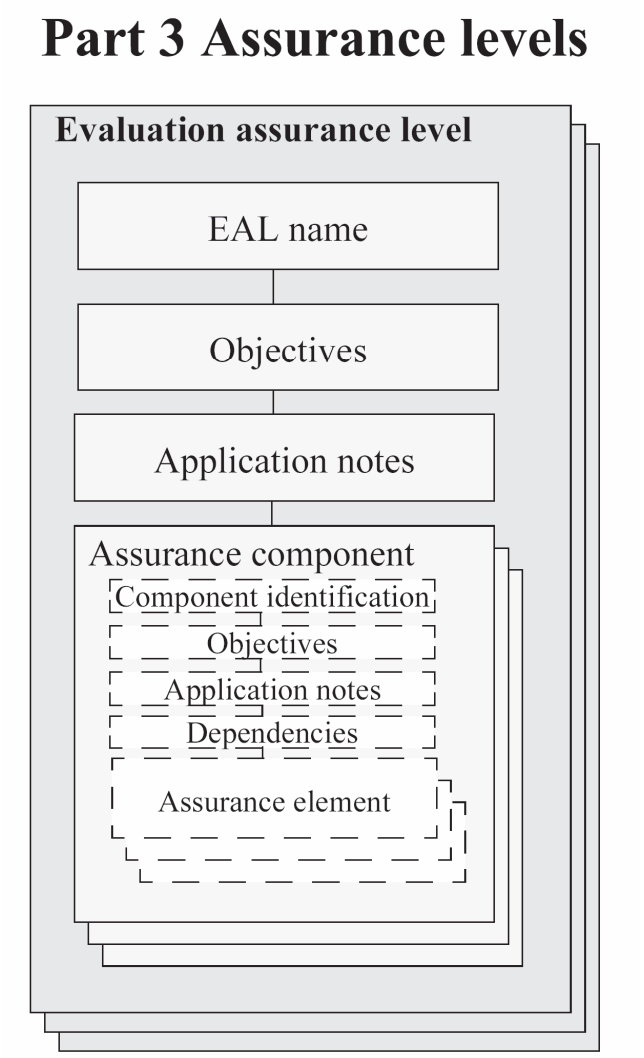


Figure 4 — EAL structure

6.2.1 EAL name

Each EAL is assigned a unique name. The name provides descriptive information about the intent of the EAL.

A unique short form of the EAL name is also provided. This is the primary means used to reference the EAL.

6.2.2 Objectives

The objectives subclause of the EAL presents the intent of the EAL.

6.2.3 Application notes

The application notes subclause of the EAL, if present, contains information of particular interest to users of the EAL (e.g. PP and ST authors, designers of TOEs targeting this EAL, evaluators). The presentation is

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

6.2.4 Assurance components

A set of assurance components have been chosen for each EAL.

A higher level of assurance than that provided by a given EAL can be achieved by:

a) including additional assurance components from other assurance families; or

b) replacing an assurance component with a higher level assurance component from the same assurance family.

6.2.5 Relationship between assurances and assurance levels

Figure 5 illustrates the relationship between the SARs and the assurance levels defined in ISO/IEC 15408. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance levels. Note that the arrow in the figure represents a reference from an EAL to an assurance component within the class where it is defined.

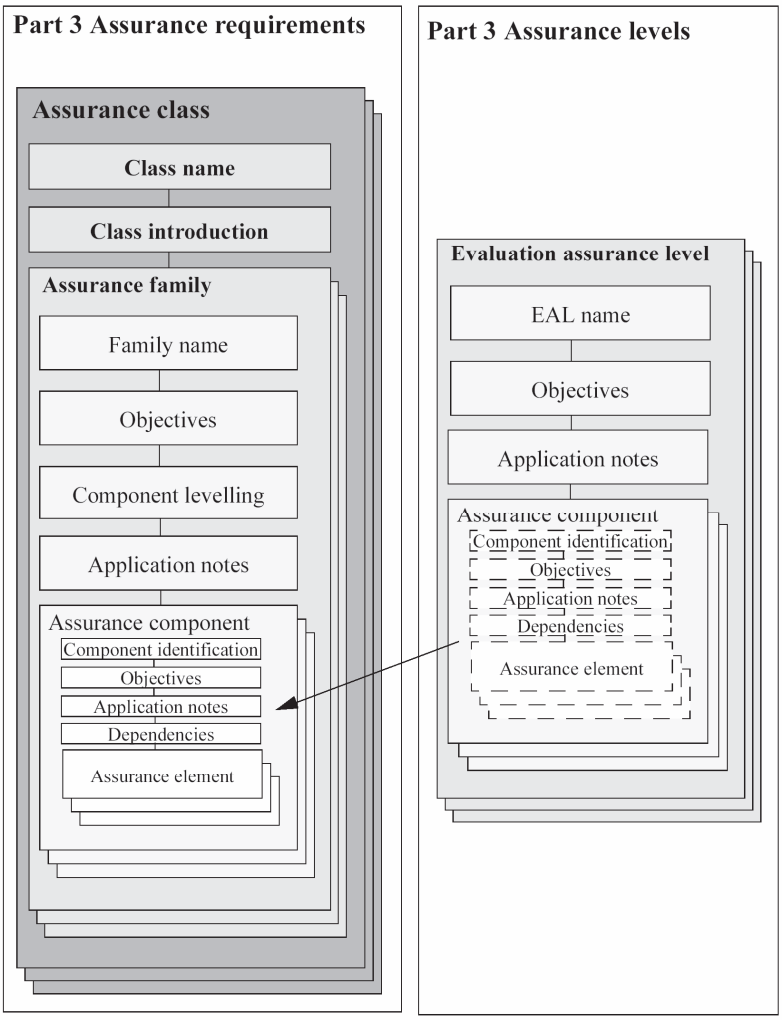


Figure 5 — Assurance and assurance level association

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

6.3 CAP structure

The structure of the CAPs is similar to that of the EALs. The main difference between these two types of package is the type of TOE they apply to; the EALs applying to component TOEs and the CAPs applying to composed TOEs.

Figure 6 illustrates the CAPs and associated structure defined in this part of ISO/IEC 15408. Note that while the figure shows the contents of the assurance components, it is intended that this information would be included in a CAP by reference to the actual components defined in ISO/IEC 15408.

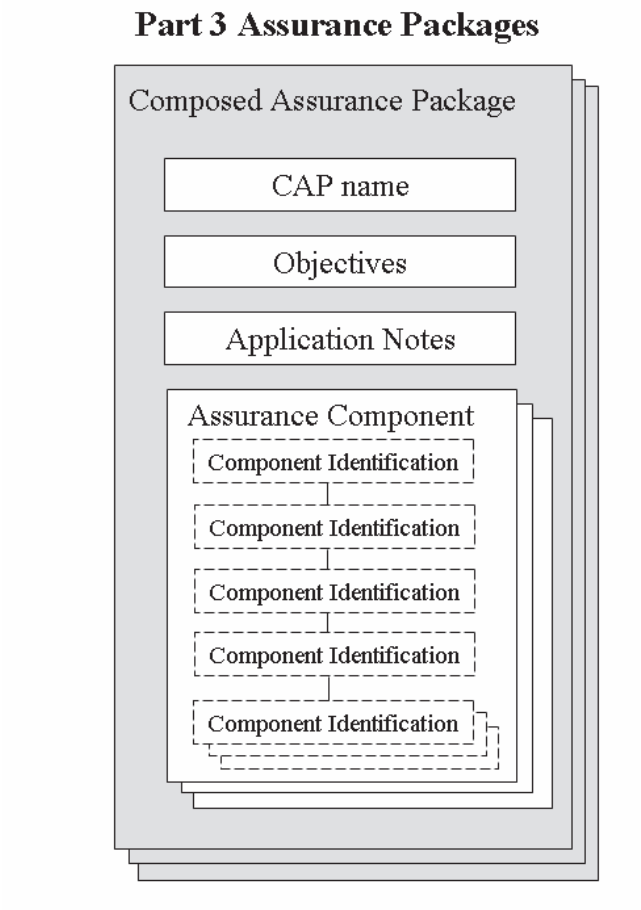


Figure 6 — CAP structure

6.3.1 CAP name

Each CAP is assigned a unique name. The name provides descriptive information about the intent of the CAP.

A unique short form of the CAP name is also provided. This is the primary means used to reference the CAP.

6.3.2 Objectives

The objectives subclause of the CAP presents the intent of the CAP.

6.3.3 Application notes

The application notes subclause of the CAP, if present, contains information of particular interest to users of the CAP (e.g. PP and ST authors, integrators of composed TOEs targeting this CAP, evaluators). The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

6.3.4 Assurance components

A set of assurance components have been chosen for each CAP.

Some dependencies identify the activities performed during the evaluation of the dependent component on which the composed TOE activity relies. Where it is not explicitly identified that the dependency is on a dependent component activity, the dependency is to another evaluation activity of the composed TOE.

A higher level of assurance than that provided by a given CAP can be achieved by:

a) including additional assurance components from other assurance families; or

b) replacing an assurance component with a higher level assurance component from the same assurance family.

The ACO: Composition components included in the CAP assurance packages should not be used as augmentations for component TOE evaluations, as this would provide no meaningful assurance for the component.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

6.3.5 Relationship between assurances and assurance levels

Figure 7 illustrates the relationship between the SARs and the composed assurance packages defined in ISO/IEC 15408. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance packages. Note that the arrow in the figure represents a reference from a CAP to an assurance component within the class where it is defined.

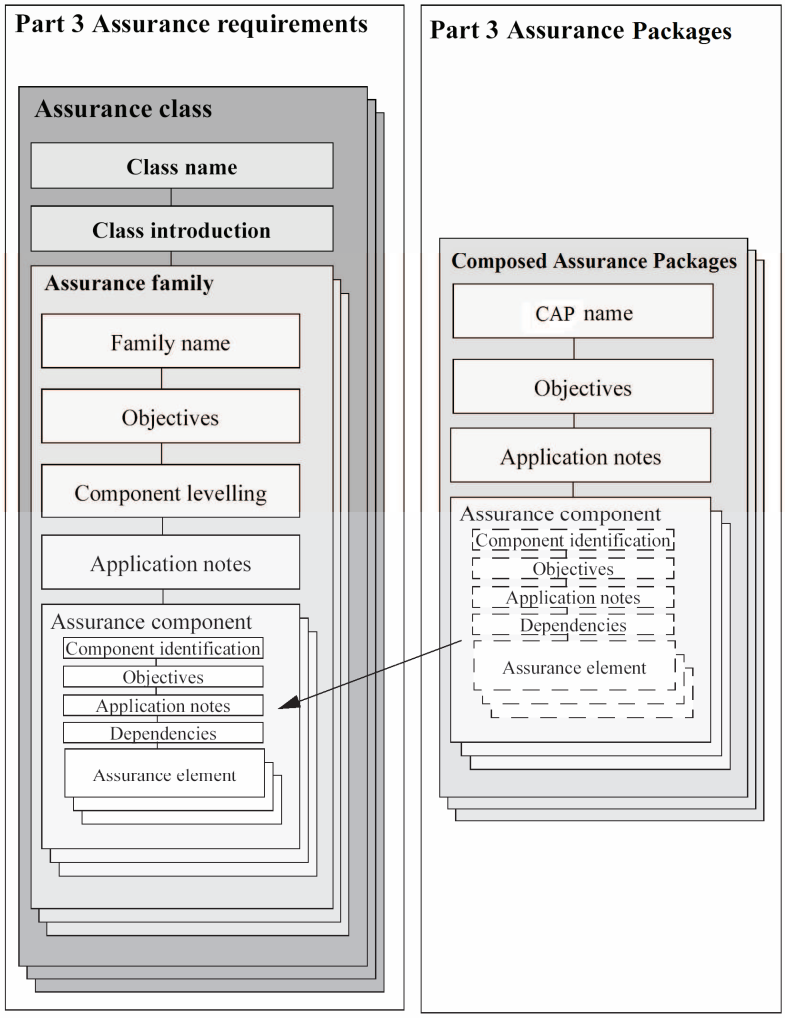


Figure 7 — Assurance and composed assurance package association

7 Evaluation assurance levels

The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. ISO/IEC 15408 approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from this part of ISO/IEC 15408 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

7.1 Evaluation assurance level (EAL) overview

Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next subclause, seven hierarchically ordered evaluation assurance levels are defined in ISO/IEC 15408 for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Clause 6 of this part of ISO/IEC 15408. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in ISO/IEC 15408, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in ISO/IEC 15408, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Table 1 — Evaluation assurance level summary

7.2 Evaluation assurance level details

The following subclauses provide definitions of the EALs, highlighting differences between the specific requirements and the prose characterisations of those requirements using bold type.

7.3 Evaluation assurance level 1 (EAL1) - functionally tested

7.3.1 Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

7.3.2 Assurance components

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance Class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 2 — EAL1

7.4 Evaluation assurance level 2 (EAL2) - structurally tested

7.4.1 Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

7.4.2 Assurance components

EAL2 provides assurance by a **full** security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation **and a basic description of the architecture of the TOE,** to understand the security behaviour.

The analysis is supported by independent testing of the TSF, **evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.**

EAL2 also provides assurance through **use** of **a configuration management system** and **evidence** of **secure delivery procedures.**

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

This EAL **represents** a meaningful increase in assurance **from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.**

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 3 — EAL2

7.5 Evaluation assurance level 3 (EAL3) - methodically tested and checked

7.5.1 Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

7.5.2 Assurance components

EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and **an architectural** description of the **design** of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification **and TOE design,** selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL3 also provides assurance through **the** use of **development environment controls, TOE** configuration management, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL2** by requiring **more complete** testing **coverage** of the **security functionality** and **mechanisms and/or procedures that provide some confidence that the** TOE **will not be tampered with during development.**

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 4 — EAL3

7.6 Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

7.6.1 Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

7.6.2 Assurance components

EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and **complete** interface specification, guidance documentation, **a** description of the **basic modular** design of the TOE, **and a subset of the implementation,** to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, **implementation representation,** security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with **an Enhanced-Basic** attack potential.

EAL4 also provides assurance through the use of development environment controls **and additional** TOE configuration management **including automation,** and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL3** by requiring more **design description,** the **implementation representation for the entire TSF,** and **improved** mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 5 — EAL4

7.7 Evaluation assurance level 5 (EAL5) - semiformally designed and tested

7.7.1 Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

7.7.2 Assurance components

EAL5 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the design of the TOE, and the implementation, to understand the security behaviour. **A modular TSF design is also required.**

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, TOE design, selective independent confirmation of the developer test results, and **an independent** vulnerability analysis demonstrating resistance to penetration attackers with **a moderate** attack potential.

EAL5 also provides assurance through the use of **a** development environment controls, and **comprehensive** TOE configuration management including automation, and evidence of secure delivery procedures.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

This EAL represents a meaningful increase in assurance from **EAL4** by requiring **semiformal design descriptions, a** more **structured (and hence analysable) architecture,** and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT.2 Well-structured internals
	ADV_TDS.4 Semiformal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.2 Compliance with implementation standards
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.4 Methodical vulnerability analysis

Table 6 — EAL5

7.8 Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

7.8.1 Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

7.8.2 Assurance components

EAL6 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and the implementation to understand the security behaviour. **Assurance is additionally gained through a formal model of select TOE security policies and a semiformal presentation of the functional specification and TOE design.** A modular, **layered and simple** TSF design is also required.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, TOE design, selective independent confirmation of the developer test results, and an

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

independent vulnerability analysis demonstrating resistance to penetration attackers with a **high** attack potential.

EAL6 also provides assurance through the use of a **structured** development **process, development** environment controls, and comprehensive TOE configuration management including **complete** automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL5** by requiring **more comprehensive analysis,** a **structured representation of the implementation,** more **architectural structure (e.g. layering), more comprehensive independent vulnerability analysis,** and improved **configuration management and** development **environment controls.**

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.5 Complete semiformal modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.3 Testing: modular design
	ATE_FUN.2 Ordered functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 7 — EAL6

7.9 Evaluation assurance level 7 (EAL7) - formally verified design and tested

7.9.1 Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

7.9.2 Assurance components

EAL7 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, the design of the TOE, and **a structured presentation of** the implementation to understand the security behaviour. Assurance is additionally gained through a formal model of select TOE security policies and a semiformal presentation of the functional specification and TOE design. A modular, layered and simple TSF design is also required.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, TOE design **and implementation representation, complete** independent confirmation of the developer test results, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a high attack potential.

EAL7 also provides assurance through the use of a structured development process, development environment controls, and comprehensive TOE configuration management including complete automation, and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from **EAL6** by requiring more comprehensive analysis **using formal representations** and **formal correspondence,** and **comprehensive testing.**

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.2 Complete mapping of the implementation representation of the TSF
	ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.3 Compliance with implementation standards - all parts
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.4 Testing: implementation representation
	ATE_FUN.2 Ordered functional testing
	ATE_IND.3 Independent testing - complete
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 8 — EAL7

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

8 Composed assurance packages

The Composed Assurance Packages (CAPs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance for composed TOEs.

It is important to note that there are only a small number of families and components from this part of ISO/IEC 15408 included in the CAPs. This is due to their nature of building upon evaluation results of previously evaluated entities (base components and dependent components), and is not to say that these do not provide meaningful and desirable assurances.

8.1 Composed assurance package (CAP) overview

CAPs are to be applied to composed TOEs, which are comprised of components that have been (are going through) component TOE evaluation (see Annex B). The individual components will have been certified to an EAL or another assurance package specified in the ST. It is expected that a basic level of assurance in a composed TOE will be gained through application of EAL1, which can be achieved with information about the components that is generally available in the public domain. (EAL1 can be applied as specified within to both component and composed TOEs.) CAPs provide an alternative approach to obtaining higher levels of assurance for a composed TOE than application of the EALs above EAL1.

While a dependent component can be evaluated using a previously evaluated and certified base component to satisfy the IT platform requirements in the environment, this does not provide any formal assurance of the interactions between the components or the possible introduction of vulnerabilities resulting from the composition. Composed assurance packages consider these interactions and, at higher levels of assurance, ensure that the interface between the components has itself been the subject of testing. A vulnerability analysis of the composed TOE is also performed to consider the possible introduction of vulnerabilities as a result of composing the components.

Table 9 represents a summary of the CAPs. The columns represent a hierarchically ordered set of CAPs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next subclause, three hierarchically ordered composed assurance packages are defined in ISO/IEC 15408 for the rating of a composed TOE's assurance. They are hierarchically ordered inasmuch as each CAP represents more assurance than all lower CAPs. The increase in assurance from CAP to CAP is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements). These increases result in greater analysis of the composition to identify the impact on the evaluation results gained for the individual component TOEs.

These CAPs consist of an appropriate combination of assurance components as described in Clause 6 of this part of ISO/IEC 15408. More precisely, each CAP includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

The CAPs only consider resistance against an attacker with an attack potential up to Enhanced-Basic. This is due to the level of design information that can be provided through the ACO_DEV, limiting some of the factors associated with attack potential (knowledge of the composed TOE) and subsequently affecting the rigour of vulnerability analysis that can be performed by the evaluator. Therefore, the level of assurance in the composed TOE is limited, although the assurance in the individual components within the composed TOE may be much higher.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance class	Assurance Family	Assurance Components by Composition Assurance Package		
		CAP-A	CAP-B	CAP-C
Composition	ACO_COR	**1**	1	1
	ACO_CTT	**1**	**2**	2
	ACO_DEV	**1**	**2**	**3**
	ACO_REL	**1**	1	**2**
	ACO_VUL	**1**	**2**	**3**
Guidance documents	AGD_OPE	**1**	1	1
	AGD_PRE	**1**	1	1
Life-cycle support	ALC_CMC	**1**	1	1
	ALC_CMS	**2**	2	2
	ALC_DEL			
	ALC_DVS			
	ALC_FLR			
	ALC_LCD			
	ALC_TAT			
Security Target evaluation	ASE_CCL	**1**	1	1
	ASE_ECD	**1**	1	1
	ASE_INT	**1**	1	1
	ASE_OBJ	**1**	**2**	2
	ASE_REQ	**1**	**2**	2
	ASE_SPD		**1**	1
	ASE_TSS	**1**	1	1

Table 9 — Composition assurance level summary

8.2 Composed assurance package details

The following subclauses provide definitions of the CAPs, highlighting differences between the specific requirements and the prose characterisations of those requirements using bold type.

8.3 Composition assurance level A (CAP-A) - Structurally composed

8.3.1 Objectives

CAP-A is applicable when a composed TOE is integrated and confidence in the correct security operation of the resulting composite is required. This requires the cooperation of the developer of the dependent component in terms of delivery of design information and test results from the dependent component certification, without requiring the involvement of the base component developer.

CAP-A is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

8.3.2 Assurance components

CAP-A provides assurance by analysis of a security target for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation) and a specification for the interfaces between the component TOEs in the composed TOE to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied upon by the dependent component, as described in the reliance information, evidence of developer testing based on the reliance information, development information and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability review of the composed TOE by the evaluator.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

CAP-A also provides assurance through unique identification of the composed TOE (i.e. IT TOE and guidance documentation).

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.1 Interface testing
	ACO_DEV.1 Functional Description
	ACO_REL.1 Basic reliance information
	ACO_VUL.1 Composition vulnerability review
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.2 Parts of the TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification

Table 10 — CAP-A

8.4 Composition assurance level B (CAP-B) - Methodically composed

8.4.1 Objectives

CAP-B permits a conscientious developer to gain maximum assurance from understanding, at a subsystem level, the affects of interactions between component TOEs integrated in the composed TOE, whilst minimising the demand of involvement of the base component developer.

CAP-B is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the composed TOE and its development without substantial re-engineering.

8.4.2 Assurance components

CAP-B provides assurance by analysis of a **full** security target for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation), a specification for the interfaces between the component TOEs **and the TOE design (describing TSF subsystems) contained** in the composed **development information** to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied upon by the dependent component, as described in the reliance information **(now also including TOE design),** evidence of developer testing based on the reliance information, development information and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability **analysis** of the composed TOE by the evaluator **demonstrating resistance to attackers with basic attack potential.**

This CAP represents a meaningful increase in assurance from CAP-A **by requiring more complete testing coverage** of the **security functionality.**

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.2 Rigorous interface testing
	ACO_DEV.2 Basic evidence of design
	ACO_REL.1 Basic reliance information
	ACO_VUL.2 Composition vulnerability analysis
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.2 Parts of the TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Table 11 — CAP-B

8.5 Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed

8.5.1 Objectives

CAP-C permits a developer to gain maximum assurance from positive analysis of the interactions between the components of the composed TOE, which, though rigorous, do not require full access to all evaluation evidence of the base component.

CAP-C is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity composed TOEs and are prepared to incur additional security-specific engineering costs.

8.5.2 Assurance components

CAP-C provides assurance by analysis of a full security target for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation), a specification for the interfaces between the component TOEs and the TOE design (describing TSF **modules)** contained in the composed development information to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied upon by the dependent component, as described in the reliance information (now including TOE design), evidence of developer testing based on the reliance information, development information and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability analysis of the composed TOE by the evaluator demonstrating resistance to attackers with **Enhanced-Basic** attack potential.

This CAP represents a meaningful increase in assurance from **CAP-B** by requiring more **design description and demonstration** of **resistance to a higher attack potential.**

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Assurance Class	Assurance components
ACO: Composition	ACO_COR.1 Composition rationale
	ACO_CTT.2 Rigorous interface testing
	ACO_DEV.3 Detailed evidence of design
	ACO_REL.2 Reliance information
	ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.2 Parts of the TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

Table 12 — CAP-C

9 Class APE: Protection Profile evaluation

Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

This clause should be used in conjunction with Annexes A, B and C in ISO/IEC 15408-1:2009, as these annexes clarify the concepts here and provide many examples.

This standard defines two assurance packages for PP evaluation as follows:

a) Low assurance PP evaluation package;

b) (Standard) PP evaluation package.

The assurance components for these packages are defined by table 13.

Assurance class	Assurance family	Assurance component	
		Low Assurance PP	PP
Protection Profile evaluation	APE_CCL	**1**	1
	APE_ECD	**1**	1
	APE_INT	**1**	1
	APE_OBJ	**1**	**2**
	APE_REQ	**1**	**2**
	APE_SPD		**1**

Table 13 — PP assurance packages

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Figure 8 shows the families within this class, and the hierarchy of components within the families.

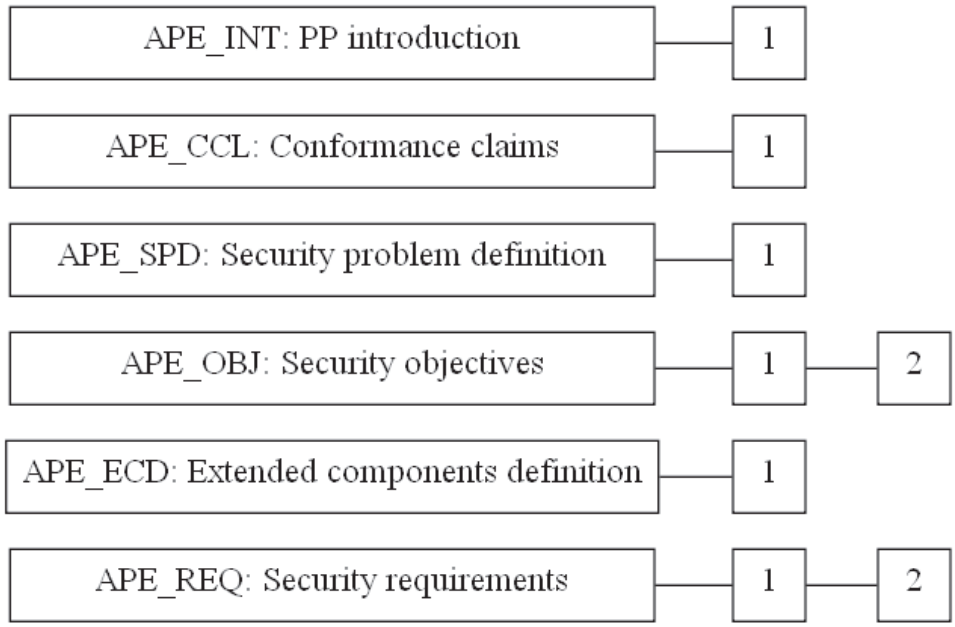


Figure 8 — APE: Protection Profile evaluation class decomposition

9.1 PP introduction (APE_INT)

9.1.1 Objectives

The objective of this family is to describe the TOE in a narrative way.

Evaluation of the PP introduction is required to demonstrate that the PP is correctly identified, and that the PP reference and TOE overview are consistent with each other.

9.1.2 APE_INT.1 PP introduction

Dependencies: No dependencies.

9.1.2.1 Developer action elements

9.1.2.1.1 APE_INT.1.1D

The developer shall provide a PP introduction.

9.1.2.2 Content and presentation elements

9.1.2.2.1 APE_INT.1.1C

The PP introduction shall contain a PP reference and a TOE overview.

9.1.2.2.2 APE_INT.1.2C

The PP reference shall uniquely identify the PP.

9.1.2.2.3 APE_INT.1.3C

The TOE overview shall summarise the usage and major security features of the TOE.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.1.2.2.4 APE_INT.1.4C

The TOE overview shall identify the TOE type.

9.1.2.2.5 APE_INT.1.5C

The TOE overview shall identify any non-TOE hardware/software/firmware available to the TOE.

9.1.2.3 Evaluator action elements

9.1.2.3.1 APE_INT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.2 Conformance claims (APE_CCL)

9.2.1 Objectives

The objective of this family is to determine the validity of the conformance claim. In addition, this family specifies how STs and other PPs are to claim conformance with the PP.

9.2.2 APE_CCL.1 Conformance claims

Dependencies: APE_INT.1 PP introduction

APE_ECD.1 Extended components definition

APE_REQ.1 Stated security requirements

9.2.2.1 Developer action elements

9.2.2.1.1 APE_CCL.1.1D

The developer shall provide a conformance claim.

9.2.2.1.2 APE_CCL.1.2D

The developer shall provide a conformance claim rationale.

9.2.2.1.3 APE_CCL.1.3D

The developer shall provide a conformance statement.

9.2.2.2 Content and presentation elements

9.2.2.2.1 APE_CCL.1.1C

The conformance claim shall contain an ISO/IEC 15408 conformance claim that identifies the version of ISO/IEC 15408 to which the PP claims conformance.

9.2.2.2.2 APE_CCL.1.2C

ISO/IEC 15408 conformance claim shall describe the conformance of the PP to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 extended.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.2.2.2.3 APE_CCL.1.3C

ISO/IEC 15408 conformance claim shall describe the conformance of the PP to this part of ISO/IEC 15408 as either this part of ISO/IEC 15408 conformant or this part of ISO/IEC 15408 extended.

9.2.2.2.4 APE_CCL.1.4C

ISO/IEC 15408 conformance claim shall be consistent with the extended components definition.

9.2.2.2.5 APE_CCL.1.5C

The conformance claim shall identify all PPs and security requirement packages to which the PP claims conformance.

9.2.2.2.6 APE_CCL.1.6C

The conformance claim shall describe any conformance of the PP to a package as either package-conformant or package-augmented.

9.2.2.2.7 APE_CCL.1.7C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

9.2.2.2.8 APE_CCL.1.8C

The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

9.2.2.2.9 APE_CCL.1.9C

The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

9.2.2.2.10 APE_CCL.1.10C

The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

9.2.2.2.11 APE_CCL.1.11C

The conformance statement shall describe the conformance required of any PPs/STs to the PP as strict-PP or demonstrable-PP conformance.

9.2.2.3 Evaluator action elements

9.2.2.3.1 APE_CCL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.3 Security problem definition (APE_SPD)

9.3.1 Objectives

This part of the PP defines the security problem to be addressed by the TOE and the operational environment of the TOE.

Evaluation of the security problem definition is required to demonstrate that the security problem intended to be addressed by the TOE and its operational environment, is clearly defined.

9.3.2 APE_SPD.1 Security problem definition

Dependencies: No dependencies.

9.3.2.1 Developer action elements

9.3.2.1.1 APE_SPD.1.1D

The developer shall provide a security problem definition.

9.3.2.2 Content and presentation elements

9.3.2.2.1 APE_SPD.1.1C

The security problem definition shall describe the threats.

9.3.2.2.2 APE_SPD.1.2C

All threats shall be described in terms of a threat agent, an asset, and an adverse action.

9.3.2.2.3 APE_SPD.1.3C

The security problem definition shall describe the OSPs.

9.3.2.2.4 APE_SPD.1.4C

The security problem definition shall describe the assumptions about the operational environment of the TOE.

9.3.2.3 Evaluator action elements

9.3.2.3.1 APE_SPD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.4 Security objectives (APE_OBJ)

9.4.1 Objectives

The security objectives are a concise statement of the intended response to the security problem defined through the Security problem definition (APE_SPD) family.

Evaluation of the security objectives is required to demonstrate that the security objectives adequately and completely address the security problem definition and that the division of this problem between the TOE and its operational environment is clearly defined.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.4.2 Component levelling

The components in this family are levelled on whether they prescribe only security objectives for the operational environment, or also security objectives for the TOE.

9.4.3 APE_OBJ.1 Security objectives for the operational environment

Dependencies: No dependencies.

9.4.3.1 Developer action elements

9.4.3.1.1 APE_OBJ.1.1D

The developer shall provide a statement of security objectives.

9.4.3.2 Content and presentation elements

9.4.3.2.1 APE_OBJ.1.1C

The statement of security objectives shall describe the security objectives for the operational environment.

9.4.3.3 Evaluator action elements

9.4.3.3.1 APE_OBJ.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.4.4 APE_OBJ.2 Security objectives

Dependencies: APE_SPD.1 Security problem definition

9.4.4.1 Developer action elements

9.4.4.1.1 APE_OBJ.2.1D

The developer shall provide a statement of security objectives.

9.4.4.1.2 APE_OBJ.2.2D

The developer shall provide a security objectives rationale.

9.4.4.2 Content and presentation elements

9.4.4.2.1 APE_OBJ.2.1C

The statement of security objectives shall describe the security objectives for the **TOE and the security objectives for the** operational environment.

9.4.4.2.2 APE_OBJ.2.2C

The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.4.4.2.3 APE_OBJ.2.3C

The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

9.4.4.2.4 APE_OBJ.2.4C

The security objectives rationale shall demonstrate that the security objectives counter all threats.

9.4.4.2.5 APE_OBJ.2.5C

The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

9.4.4.2.6 APE_OBJ.2.6C

The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

9.4.4.3 Evaluator action elements

9.4.4.3.1 APE_OBJ.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.5 Extended components definition (APE_ECD)

9.5.1 Objectives

Extended security requirements are requirements that are not based on components from ISO/IEC 15408-2 or this part of ISO/IEC 15408, but are based on extended components: components defined by the PP author.

Evaluation of the definition of extended components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they may not be clearly expressed using existing ISO/IEC 15408-2 or this part of ISO/IEC 15408 components.

9.5.2 APE_ECD.1 Extended components definition

Dependencies: No dependencies.

9.5.2.1 Developer action elements

9.5.2.1.1 APE_ECD.1.1D

The developer shall provide a statement of security requirements.

9.5.2.1.2 APE_ECD.1.2D

The developer shall provide an extended components definition.

9.5.2.2 Content and presentation elements

9.5.2.2.1 APE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.5.2.2.2 APE_ECD.1.2C

The extended components definition shall define an extended component for each extended security requirement.

9.5.2.2.3 APE_ECD.1.3C

The extended components definition shall describe how each extended component is related to the existing ISO/IEC 15408 components, families, and classes.

9.5.2.2.4 APE_ECD.1.4C

The extended components definition shall use the existing ISO/IEC 15408 components, families, classes, and methodology as a model for presentation.

9.5.2.2.5 APE_ECD.1.5C

The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

9.5.2.3 Evaluator action elements

9.5.2.3.1 APE_ECD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.5.2.3.2 APE_ECD.1.2E

The evaluator shall confirm that no extended component may be clearly expressed using existing components.

9.6 Security requirements (APE_REQ)

9.6.1 Objectives

The SFRs form a clear, unambiguous and well-defined description of the expected security behaviour of the TOE. The SARs form a clear, unambiguous and well-defined description of the expected activities that will be undertaken to gain assurance in the TOE.

Evaluation of the security requirements is required to ensure that they are clear, unambiguous and well-defined.

9.6.2 Component levelling

The components in this family are levelled on whether they are stated as is, or whether the SFRs are derived from security objectives for the TOE.

9.6.3 APE_REQ.1 Stated security requirements

Dependencies: APE_ECD.1 Extended components definition

9.6.3.1 Developer action elements

9.6.3.1.1 APE_REQ.1.1D

The developer shall provide a statement of security requirements.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.6.3.1.2 APE_REQ.1.2D

The developer shall provide a security requirements rationale.

9.6.3.2 Content and presentation elements

9.6.3.2.1 APE_REQ.1.1C

The statement of security requirements shall describe the SFRs and the SARs.

9.6.3.2.2 APE_REQ.1.2C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

9.6.3.2.3 APE_REQ.1.3C

The statement of security requirements shall identify all operations on the security requirements.

9.6.3.2.4 APE_REQ.1.4C

All operations shall be performed correctly.

9.6.3.2.5 APE_REQ.1.5C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

9.6.3.2.6 APE_REQ.1.6C

The statement of security requirements shall be internally consistent.

9.6.3.3 Evaluator action elements

9.6.3.3.1 APE_REQ.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

9.6.4 APE_REQ.2 Derived security requirements

Dependencies: APE_OBJ.2 Security objectives

APE_ECD.1 Extended components definition

9.6.4.1 Developer action elements

9.6.4.1.1 APE_REQ.2.1D

The developer shall provide a statement of security requirements.

9.6.4.1.2 APE_REQ.2.2D

The developer shall provide a security requirements rationale.

AVA Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

9.6.4.2 Content and presentation elements

9.6.4.2.1 APE_REQ.2.1C

The statement of security requirements shall describe the SFRs and the SARs.

9.6.4.2.2 APE_REQ.2.2C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

9.6.4.2.3 APE_REQ.2.3C

The statement of security requirements shall identify all operations on the security requirements.

9.6.4.2.4 APE_REQ.2.4C

All operations shall be performed correctly.

9.6.4.2.5 APE_REQ.2.5C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

9.6.4.2.6 APE_REQ.2.6C

The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

9.6.4.2.7 APE_REQ.2.7C

The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

9.6.4.2.8 APE_REQ.2.8C

The security requirements rationale shall explain why the SARs were chosen.

9.6.4.2.9 APE_REQ.2.9C

The statement of security requirements shall be internally consistent.

9.6.4.3 Evaluator action elements

9.6.4.3.1 APE_REQ.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

10 Class ASE: Security Target evaluation

Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.

This clause should be used in conjunction with Annexes A, B and C in ISO/IEC 15408-1:2009, as these annexes clarify the concepts here and provide many examples.

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11

Figure 9 shows the families within this class, and the hierarchy of components within the families.

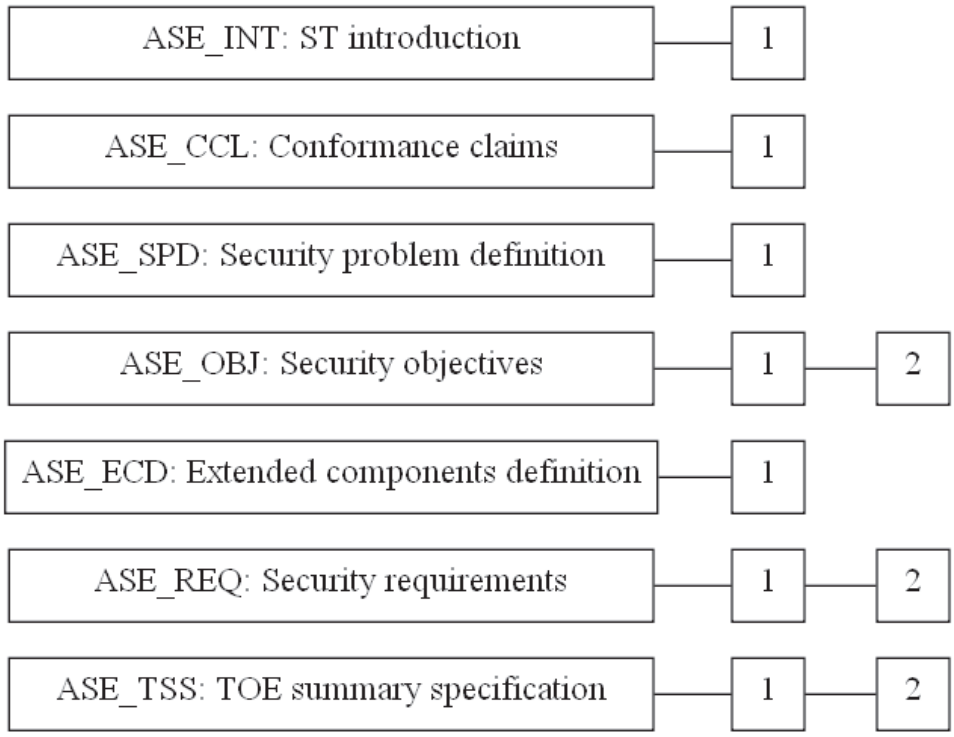


Figure 9 — ASE: Security Target evaluation class decomposition

10.1 ST introduction (ASE_INT)

10.1.1 Objectives

The objective of this family is to describe the TOE in a narrative way on three levels of abstraction: TOE reference, TOE overview and TOE description.

Evaluation of the ST introduction is required to demonstrate that the ST and the TOE are correctly identified, that the TOE is correctly described at three levels of abstraction and that these three descriptions are consistent with each other.

10.1.2 ASE_INT.1 ST introduction

Dependencies: No dependencies.

10.1.2.1 Developer action elements

10.1.2.1.1 ASE_INT.1.1D

The developer shall provide an ST introduction.

10.1.2.2 Content and presentation elements

10.1.2.2.1 ASE_INT.1.1C

The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

Documents
Document Sharing Hub

Full document details: E DIN EN ISO/IEC 15408-3:2019-11

10.1.2.2.2 ASE_INT.1.2C

The ST reference shall uniquely identify the ST.

10.1.2.2.3 ASE_INT.1.3C

The TOE reference shall identify the TOE.

10.1.2.2.4 ASE_INT.1.4C

The TOE overview shall summarise the usage and major security features of the TOE.

10.1.2.2.5 ASE_INT.1.5C

The TOE overview shall identify the TOE type.

10.1.2.2.6 ASE_INT.1.6C

The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

10.1.2.2.7 ASE_INT.1.7C

The TOE description shall describe the physical scope of the TOE.

10.1.2.2.8 ASE_INT.1.8C

The TOE description shall describe the logical scope of the TOE.

10.1.2.3 Evaluator action elements

10.1.2.3.1 ASE_INT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

10.1.2.3.2 ASE_INT.1.2E

The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

10.2 Conformance claims (ASE_CCL)

10.2.1 Objectives

The objective of this family is to determine the validity of the conformance claim. In addition, this family specifies how STs are to claim conformance with the PP.

10.2.2 ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Documents
Document Sharing Hub
Full document details: E DIN EN ISO/IEC 15408-3:2019-11