



DPC: 24/30482243 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 19 August 2024

Origin: European

Latest date for receipt of comments: 12 October 2024

Project No. 2023/02580

Responsible committee: IST/33/3 Security Evaluation, Testing and Specification

Interested committees:

Title: Draft BS EN ISO/IEC 15408-3 BS EN ISO/IEC 15408-3 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security. Part 3: Security assurance components.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 12 October 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Ms Joy Tan (BSI)

Direct tel:

E-mail: joy.tan@bsigroup.com

Full document details: 24/30482243 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 15408-3

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components

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

Partie 3: Composants d'assurance de sécurité

ICS: ISO ics

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Voting begins on:
2024-08-19

Voting terminates on:
2024-11-11

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

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

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

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

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

Full document details: 24/30482243 DC

© ISO/IEC 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	x
Introduction	xii
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
4 Overview	5
5 Assurance paradigm	6
5.1 General	6
5.2 ISO/IEC 15408 series approach	6
5.3 Assurance approach	6
5.3.1 General	6
5.3.2 Significance of vulnerabilities	6
5.3.3 Cause of vulnerabilities	7
5.3.4 ISO/IEC 15408 series assurance	7
5.3.5 Assurance through evaluation	7
5.4 ISO/IEC 15408 series evaluation assurance scale	8
6 Security assurance components	8
6.1 Overview	8
6.2 Assurance class structure	8
6.2.1 General	8
6.2.2 Class name	8
6.2.3 Class introduction	9
6.2.4 Assurance families	9
6.3 Assurance family structure	9
6.3.1 General	9
6.3.2 Family name	9
6.3.3 Family objectives	9
6.3.4 Component levelling	10
6.3.5 Family application notes	10
6.3.6 Assurance components	10
6.4 Assurance component structure	10
6.4.1 General	10
6.4.2 Component name	10
6.4.3 Component objectives	11
6.4.4 Component application notes	11
6.4.5 Component dependencies	11
6.4.6 Assurance elements	11
6.5 Assurance elements	12
6.6 Component taxonomy	12
7 Class APE Protection Profile (PP) evaluation	12
7.1 Introduction	12
7.2 Conformance claims (APE_CCL)	14
7.2.1 Objectives	14
7.2.2 Conformance claims (APE_CCL.1)	14
7.3 Extended components definition (APE_ECD)	16
7.3.1 Objectives	16
7.3.2 Extended components definition (APE_ECD.1)	16
7.4 PP introduction (APE_INT)	17
7.4.1 Objectives	17
7.4.2 PP introduction (APE_INT.1)	17
7.5 Security objectives (APE_OBJ)	17
7.5.1 Objectives	17

7.5.2	Component levelling.....	17
7.5.3	Security objectives for the operational environment (APE_OBJ.1).....	18
7.5.4	Security objectives (APE_OBJ.2).....	18
7.6	Security requirements (APE_REQ).....	19
7.6.1	Objectives.....	19
7.6.2	Component levelling.....	19
7.6.3	Direct rationale security requirements (APE_REQ.1).....	19
7.6.4	Derived security requirements (APE_REQ.2).....	20
7.7	Security problem definition (APE_SPD).....	22
7.7.1	Objectives.....	22
7.7.2	Security problem definition (APE_SPD.1).....	22
8	Class ACE Protection Profile Configuration evaluation.....	22
8.1	Introduction.....	22
8.2	PP-Module conformance claims (ACE_CCL).....	24
8.2.1	Objectives.....	24
8.2.2	PP-Module conformance claims (ACE_CCL.1).....	24
8.3	PP-Configuration consistency (ACE_CCO).....	25
8.3.1	Objectives.....	25
8.3.2	PP-Configuration consistency (ACE_CCO.1).....	26
8.4	PP-Module extended components definition (ACE_ECD).....	29
8.4.1	Objectives.....	29
8.4.2	PP-Module extended components definition (ACE_ECD.1).....	29
8.5	PP-Module introduction (ACE_INT).....	30
8.5.1	Objectives.....	30
8.5.2	PP-Module introduction (ACE_INT.1).....	30
8.6	PP-Module consistency (ACE_MCO).....	31
8.6.1	Objectives.....	31
8.6.2	PP-Module consistency (ACE_MCO.1).....	31
8.7	PP-Module security objectives (ACE_OBJ).....	32
8.7.1	Objectives.....	32
8.7.2	Component levelling.....	32
8.7.3	PP-Module security objectives for the operational environment (ACE_OBJ.1).....	32
8.7.4	PP-Module security objectives (ACE_OBJ.2).....	33
8.8	PP-Module security requirements (ACE_REQ).....	34
8.8.1	Objectives.....	34
8.8.2	Component levelling.....	34
8.8.3	PP-Module direct rationale security requirements (ACE_REQ.1).....	34
8.8.4	PP-Module derived security requirements (ACE_REQ.2).....	35
8.9	PP-Module security problem definition (ACE_SPD).....	37
8.9.1	Objectives.....	37
8.9.2	PP-Module security problem definition (ACE_SPD.1).....	37
9	Class ASE Security Target (ST) evaluation.....	37
9.1	Introduction.....	37
9.2	Conformance claims (ASE_CCL).....	39
9.2.1	Objectives.....	39
9.2.2	Conformance claims (ASE_CCL.1).....	39
9.3	Consistency of composite product Security Target (ASE_COMP).....	41
9.3.1	Objectives.....	41
9.3.2	Component levelling.....	41
9.3.3	Application notes.....	41
9.3.4	Consistency of Security Target (ST) (ASE_COMP.1).....	42
9.4	Extended components definition (ASE_ECD).....	42
9.4.1	Objectives.....	42
9.4.2	Extended components definition (ASE_ECD.1).....	43
9.5	ST introduction (ASE_INT).....	43
9.5.1	Objectives.....	43
9.5.2	ST introduction (ASE_INT.1).....	44
9.6	Security objectives (ASE_OBJ).....	45

9.6.1	Objectives	45
9.6.2	Component levelling	45
9.6.3	Security objectives for the operational environment (ASE_OBJ.1)	45
9.6.4	Security objectives (ASE_OBJ.2)	45
9.7	Security requirements (ASE_REQ)	46
9.7.1	Objectives	46
9.7.2	Component levelling	47
9.7.3	Direct rationale security requirements (ASE_REQ.1)	47
9.7.4	Derived security requirements (ASE_REQ.2)	48
9.8	Security problem definition (ASE_SPD)	49
9.8.1	Objectives	49
9.8.2	Security problem definition (ASE_SPD.1)	50
9.9	TOE summary specification (ASE_TSS)	50
9.9.1	Objectives	50
9.9.2	Component levelling	50
9.9.3	TOE summary specification (ASE_TSS.1)	51
9.9.4	TOE summary specification with architectural design summary (ASE_TSS.2)	51
10	Class ADV Development	52
10.1	Introduction	52
10.2	Security architecture (ADV_ARC)	57
10.2.1	Objectives	57
10.2.2	Component levelling	57
10.2.3	Application notes	57
10.2.4	Security architecture description (ADV_ARC.1)	58
10.3	Composite design compliance (ADV_COMP)	59
10.3.1	Objectives	59
10.3.2	Component levelling	59
10.3.3	Application notes	59
10.3.4	Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority (ADV_COMP.1)	60
10.4	Functional specification (ADV_FSP)	60
10.4.1	Objectives	60
10.4.2	Component levelling	61
10.4.3	Application notes	61
10.4.4	Basic functional specification (ADV_FSP.1)	63
10.4.5	Security-enforcing functional specification (ADV_FSP.2)	64
10.4.6	Functional specification with complete summary (ADV_FSP.3)	65
10.4.7	Complete functional specification (ADV_FSP.4)	66
10.4.8	Complete semi-formal functional specification with additional error information (ADV_FSP.5)	66
10.4.9	Complete semi-formal functional specification with additional formal specification (ADV_FSP.6)	68
10.5	Implementation representation (ADV_IMP)	69
10.5.1	Objectives	69
10.5.2	Component levelling	69
10.5.3	Application notes	69
10.5.4	Implementation representation of the TSF (ADV_IMP.1)	70
10.5.5	Complete mapping of the implementation representation of the TSF (ADV_IMP.2)	71
10.6	TSF internals (ADV_INT)	71
10.6.1	Objectives	71
10.6.2	Component levelling	72
10.6.3	Application notes	72
10.6.4	Well-structured subset of TSF internals (ADV_INT.1)	72
10.6.5	Well-structured internals (ADV_INT.2)	73
10.6.6	Minimally complex internals (ADV_INT.3)	74
10.7	Formal TSF model (ADV_SPM)	75
10.7.1	Objectives	75

10.7.2	Component levelling.....	75
10.7.3	Application notes	75
10.7.4	Formal TSF model (ADV_SPM.1).....	76
10.8	TOE design (ADV_TDS)	77
10.8.1	Objectives	77
10.8.2	Component levelling.....	77
10.8.3	Application notes	77
10.8.4	Basic design (ADV_TDS.1).....	79
10.8.5	Architectural design (ADV_TDS.2)	80
10.8.6	Basic modular design (ADV_TDS.3)	81
10.8.7	Semi-Formal modular design (ADV_TDS.4).....	82
10.8.8	Complete semi-formal modular design (ADV_TDS.5).....	83
10.8.9	Complete semi-formal modular design with formal high-level design presentation (ADV_TDS.6)	84
11	Class AGD Guidance documents.....	85
11.1	Introduction.....	85
11.2	Operational user guidance (AGD_OPE).....	86
11.2.1	Objectives	86
11.2.2	Component levelling.....	86
11.2.3	Application notes	87
11.2.4	Operational user guidance (AGD_OPE.1)	87
11.3	Preparative procedures (AGD_PRE).....	88
11.3.1	Objectives	88
11.3.2	Component levelling.....	88
11.3.3	Application notes	88
11.3.4	Preparative procedures (AGD_PRE.1).....	89
12	Class ALC Life-cycle support.....	89
12.1	Introduction.....	89
12.2	CM capabilities (ALC_CMC)	91
12.2.1	Objectives	91
12.2.2	Component levelling.....	92
12.2.3	Application notes	92
12.2.4	Labelling of the TOE (ALC_CMC.1).....	92
12.2.5	Use of the CM system (ALC_CMC.2).....	93
12.2.6	Authorization controls (ALC_CMC.3).....	94
12.2.7	Production support, acceptance procedures and automation (ALC_CMC.4)	95
12.2.8	Advanced support (ALC_CMC.5).....	97
12.3	CM scope (ALC_CMS)	99
12.3.1	Objectives	99
12.3.2	Component levelling.....	99
12.3.3	Application notes	99
12.3.4	TOE CM coverage (ALC_CMS.1).....	99
12.3.5	Parts of the TOE CM coverage (ALC_CMS.2).....	100
12.3.6	Implementation representation CM coverage (ALC_CMS.3).....	101
12.3.7	Problem tracking CM coverage (ALC_CMS.4).....	101
12.3.8	Development tools CM coverage (ALC_CMS.5).....	102
12.4	Integration of composition parts and consistency check of delivery procedures (ALC_COMP).....	103
12.4.1	Objectives	103
12.4.2	Component levelling.....	103
12.4.3	Application notes	103
12.4.4	Integration of the dependent component into the related base component and Consistency check for delivery and acceptance procedures (ALC_COMP.1)	104
12.5	Delivery (ALC_DEL).....	105
12.5.1	Objectives	105
12.5.2	Component levelling.....	105
12.5.3	Application notes	105
12.5.4	Delivery procedures (ALC_DEL.1)	105

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

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

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

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

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

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

The main changes are as follows:

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

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

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

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

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Centro Criptológico Nacional
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency and the National Institute of Standards and Technology

Introduction

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

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

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

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

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

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

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

Part 3: Security assurance components

1 Scope

This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information security — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation*

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

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions, and abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045, ISO/IEC IEEE 24765 and the following apply.

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

- ISO Online browsing platform: available at www.iso.org/obp/ui;
- IEC Electropedia: available at www.electropedia.org.

3.1

acceptance procedure

procedure followed in order to accept newly created or modified *configuration item* (3.3) (s) as part of the target of evaluation (TOE), or to move them to the next step of the life-cycle

Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance.

Note 2 to entry: There are several types of acceptance situations some of which can overlap:

- acceptance of an item into the configuration management system for the first time, in particular as part of an integration process;
- progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE

EXAMPLE 1

Module, subsystem, quality control of the finished TOE;

- subsequent to transport of configuration items

EXAMPLE 2

Parts of the TOE or preliminary products between different *development* (3.15) sites;

- subsequent to the *delivery* (3.14) of the TOE to the consumer;
- subsequent to the integration of the TOE

EXAMPLE 3

Inclusion of software, firmware and hardware components from other sources into the TOE.

3.2

action

evaluator or developer action element of ISO/IEC 15408-3

Note 1 to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.3

configuration item

item or aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process, during the target of evaluation (TOE) *development* (3.15)

Note 1 to entry: These can be either parts of the TOE or objects related to the development of the TOE, e.g. evaluation documents or development tools. Configuration management items can be stored in the configuration management system directly (for example, files) or by reference (for example, hardware parts) together with their version.

3.4

configuration list

configuration management output (3.8) document listing all *configuration item* (3.3) (s) for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product

Note 1 to entry: This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course, the list can be an electronic document inside of a *configuration management tool* (3.12). In that case, it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of CM capabilities (ALC_CMC) (see 12.2).

3.5 configuration management

CM
discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a *configuration item* (3.3), control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

[SOURCE: ISO/IEC IEEE 24765:2017, 3.779 1]

3.6 configuration management documentation

CM documentation
documentation including *configuration management output* (3.8), *configuration list* (3.4) (s), *configuration management system record* (3.11) (s), *configuration management plan* (3.9) and *configuration management usage documentation* (3.13)

3.7 configuration management evidence

everything that may be used to establish confidence in the correct operation of the configuration management system

EXAMPLE

configuration management output (3.8), rationales provided by the developer, observations, experiments, or interviews made by the evaluator during a site visit.

3.8 configuration management output

results, related to configuration management, produced, or enforced by the configuration management system

EXAMPLE

These configuration management related results can occur as documents (e.g. filled paper forms, *configuration management system record* (3.11) (s), logging data, hard-copies, and electronic output data) as well as actions (e.g. manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are *configuration list* (3.4) (s), *configuration management plan* (3.9) (s) and/or behaviours during the product life-cycle.

3.9 configuration management plan

description of how the configuration management system is used for the target of evaluation (TOE)

Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it can be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system can be used to a different extent for other products. The configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE *development* (3.15).

EXAMPLE

The structure and content of a configuration management plan are presented in ISO 10007:2017, Annex A.

3.10 configuration management system

set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of their products during their life-cycles

Note 1 to entry: Configuration management systems can have varying degrees of rigour and function. At higher levels, configuration management systems can be automated, with flaw remediation, change controls, and other tracking mechanisms.

3.11

configuration management system record

output produced during the operation of the configuration management system documenting important configuration management activities

EXAMPLE

Configuration management item change control forms and configuration management item access approval forms.

3.12

configuration management tool

manually operated or automated tool realizing or supporting a configuration management system

EXAMPLE

Tools for the version management of the parts of the target of evaluation (TOE).

3.13

configuration management usage documentation

part of the configuration management system, which describes how the configuration management system is defined and applied by using, e.g. handbooks, regulations and/or documentation of tools and procedures

3.14

delivery

transmission of the finished target of evaluation (TOE) from the *production* ([3.24](#)) environment into the hands of the customer

Note 1 to entry: This product life-cycle phase can include packaging and storage at the *development* ([3.15](#)) site, but does not include transportation of the unfinished TOE or parts of the TOE between different developers or different development sites.

3.15

development

product life-cycle phase which is concerned with generating the implementation representation of the target of evaluation (TOE)

Note 1 to entry: Throughout the Class ALC Life-cycle support (see [Clause 12](#)) requirements, development, and related terms (developer, develop) are meant in the more general sense to comprise *development* ([3.15](#)) and *production* ([3.24](#)).

3.16

encountered potential vulnerability

potential weakness in the target of evaluation (TOE) identified by the evaluator while performing evaluation activities that can be used to violate the security functional requirements (SFRs)

3.17

evaluation deliverable

resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities

3.18

exploitable vulnerability

weakness in the target of evaluation (TOE) that can be used to violate the security functional requirements (SFRs) in the operational environment for the TOE

3.19**installation**

procedure performed by a human user embedding the target of evaluation (TOE) in its operational environment and putting it into an operational state

Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the security target (ST). If similar processes have to be performed by the developer, they are denoted as “generation” throughout Class ALC Life-cycle support (see [Clause 12](#)). If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.

3.20**life-cycle model**

framework containing the processes, activities, and tasks involved in the *development* ([3.15](#)), *operation* ([3.21](#)), and maintenance of a product, spanning the life of the system from the definition of its requirements to the termination of its use

[SOURCE: ISO/IEC IEEE 24765:2017 3.2219 2]

3.21**operation**

⟨TOE life-cycle⟩ usage phase of the target of evaluation (TOE) including normal usage, administration, and maintenance of the TOE after *delivery* ([3.14](#)) and *preparation* ([3.23](#))

3.22**potential vulnerability**

suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the security functional requirements (SFRs).

3.23**preparation**

activity in the life-cycle phase of a product, comprising the customer’s acceptance of the delivered target of evaluation (TOE) and its *installation* ([3.19](#))

Note 1 to entry: Preparation can include such things as booting, initialization, start-up and progressing the TOE to a state ready for operation.

3.24**production**

life-cycle phase which consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for *delivery* ([3.14](#)) to the customer

Note 1 to entry: This phase can comprise manufacturing, integration, generation, internal transport, storage, and labelling of the TOE.

3.25**residual vulnerability**

weakness that cannot be exploited in the operational environment for the target of evaluation (TOE), but that can be used to violate the security functional requirements (SFRs) by an attacker with greater attack potential than is anticipated in the operational environment for the TOE

3.26**vulnerability**

weakness in the TOE that can be used to violate the security functional requirements (SFRs) in some environment

4 Overview

[Clause 5](#) describes the paradigm used in the security assurance requirements of this document.

[Clause 6](#) describes the presentation structure of the assurance classes, families, components.

Class APE Protection Profile (PP) evaluation (see [Clause 7](#)) through Class ACO Composition (see [Clause 15](#)) provide the detailed definitions of this document assurance classes.

[Annex A](#) provides further explanations and examples of the concepts behind the development class.

[Annex B](#) provides an explanation of the concepts behind composed target of evaluation (TOE) evaluations and the composition class.

5 Assurance paradigm

5.1 General

The purpose of this clause is to document the underlying approach of the ISO/IEC 15408 series approach to assurance. An understanding of this clause allows the reader to understand the rationale behind the assurance requirements of this document.

5.2 ISO/IEC 15408 series approach

The approach of the ISO/IEC 15408 series is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security controls 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 can 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.

5.3 Assurance approach

5.3.1 General

The approach of the ISO/IEC 15408 series is to provide assurance based upon an evaluation 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, the ISO/IEC 15408 series adopts the same approach. The ISO/IEC 15408 series proposes measuring the validity of the documentation and of the resulting IT product by expert evaluators with increasing emphasis on scope, depth, and rigour.

The ISO/IEC 15408 series 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 the ISO/IEC 15408 series, which is so structured as to allow their future introduction.

5.3.2 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 organization. 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 can 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:

- eliminated: active steps should be taken to expose, and remove or neutralize, all exercisable vulnerabilities;

- minimised: active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;
- monitored: 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.

5.3.3 Cause of vulnerabilities

Vulnerabilities can arise through failures in:

- requirements: 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;
- design: an IT product has been poorly designed. Building a secure product, system, or application requires not only the implementation of functional requirements but also an architecture that allows for the effective enforcement of specific security properties the product, system, or application is supposed to enforce. The ability to withstand attacks the product, system, or application may be face in its intended operational environment is highly dependent on an architecture that prohibits those attacks or, if they cannot be prohibited, allows for detection of such attacks and/or limitation of the damage such an attack can cause;
- development: 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;
- delivery, installation and configuration: an IT product has vulnerabilities introduced during the delivery, installation and configuration of the product;
- operation: 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;
- maintenance: an IT product is maintained in such a way that new vulnerabilities are introduced.

5.3.4 ISO/IEC 15408 series assurance

Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, the ISO/IEC 15408 series provides assurance through active investigation or a specification-based approach. Active investigation is an evaluation of the IT product in order to determine its security properties.

5.3.5 Assurance through evaluation

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

- analysis and checking of process(es) and procedure(s);
- checking that process(es) and procedure(s) are being applied;
- analysis of the correspondence between TOE design representations;
- analysis of the TOE design representation against the requirements;
- verification of proofs;
- analysis of guidance documents;
- analysis of functional tests developed and the results provided;
- independent functional testing;
- analysis for vulnerabilities (including flaw hypotheses);

- penetration testing;
- analysis of the delivery process;
- analysis of the maintenance process.

5.4 ISO/IEC 15408 series evaluation assurance scale

The approach of the ISO/IEC 15408 series 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 assurance. The increasing level of effort is based upon:

- scope: the effort is greater because a larger portion of the IT product is included;
- depth: the effort is greater because it is deployed to a finer level of design and implementation detail;
- rigour: the effort is greater because it is applied in a more structured, formal manner.

6 Security assurance components

6.1 Overview

This clause describes the constructs used in representing the assurance classes, families, and components that define the security assurance requirements (SARs) defined in this document.

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, PP-Module, assurance package or ST.

6.2 Assurance class structure

6.2.1 General

[Figure 1](#) illustrates the assurance class structure in diagrammatic form. Each assurance class includes a class name, class introduction, an optional application notes, and one or more assurance families.

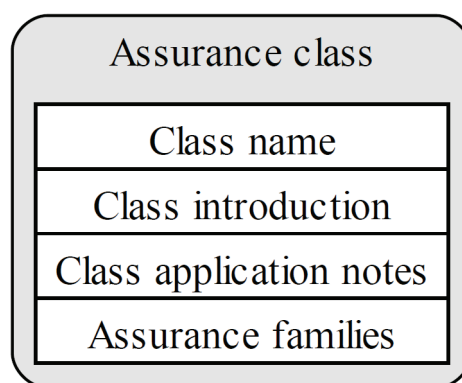


Figure 1 — Assurance class structure

6.2.2 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.

6.2.3 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.

The class introduction includes a class decomposition diagram, showing the families and components of the class. It also provides a dependency table that shows the hierarchical, direct, indirect, and optional dependencies among assurance components, as explained in [subclause 6.4.5](#).

6.2.3.1 Class application notes

The optional application notes contain additional information that supports the interpretation and understanding of the concepts, structure and usage of the assurance class.

6.2.4 Assurance families

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

6.3 Assurance family structure

6.3.1 General

[Figure 2](#) illustrates the assurance family structure in diagrammatic form.

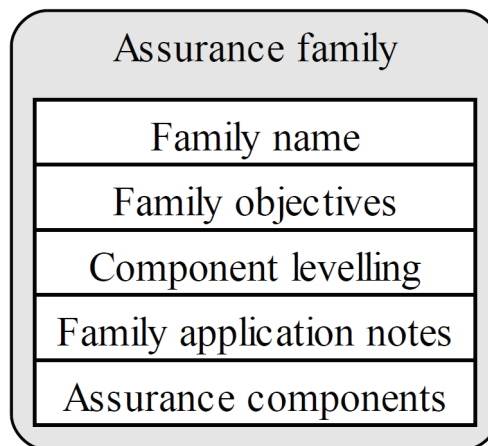


Figure 2 — Assurance family structure

6.3.2 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.

6.3.3 Family objectives

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

This subclause describes the objectives, particularly those related to the ISO/IEC 15408 series 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.

6.3.4 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.

6.3.5 Family 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.

6.3.6 Assurance components

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

6.4 Assurance component structure

6.4.1 General

[Figure 3](#) illustrates the assurance component structure.

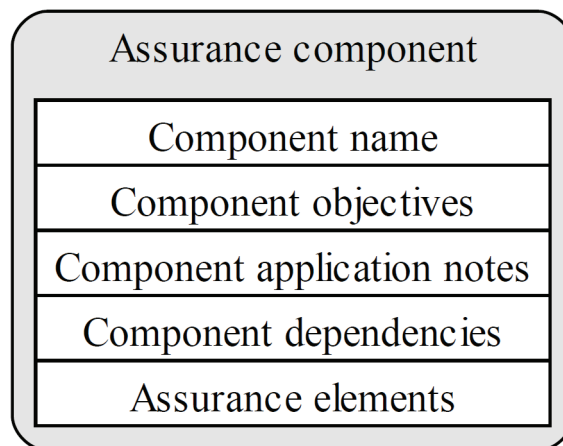


Figure 3 — Assurance component structure

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.

6.4.2 Component name

The component name provides descriptive information necessary to identify, categorize, 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, followed by a period, and then a numeric character. The numeric characters for the components within each family are assigned sequentially, starting from 1.

6.4.3 Component 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.

6.4.4 Component application notes

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

6.4.5 Component 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 it is possible that the indicated dependencies will not be applicable. The PP, PP-Module, PP-Configuration or ST author, by providing rationale for why a given dependency is not applicable, may elect not to satisfy that dependency.

The dependencies of assurance components are shown in a table at the class introduction clause, where each of the components that is a dependency of some other assurance component is allocated a column. Each assurance component is allocated a row. The value in the table cell indicates whether the column label component is a hierarchical requirement (indicated by an “H”), directly required (indicated by a cross “X”), indirectly required (indicated by a dash “-”), or optionally required (indicated by a “O”) by the row label component. Sets of optional requirements are indicated by using an entry of type O^x (e.g. O¹) whereby a SAR with such entry requires at minimum only one of the SARs contained in that O^x-set.

6.4.6 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 recognized in the ISO/IEC 15408 series.

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

- 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.
- 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.

- 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, PP-Module, PP-Configuration or ST.

The evaluator actions define the evaluator’s responsibilities in two aspects of evaluation. The first aspect is validation of the applicable PP, PP-Module, PP-Configuration or ST, in accordance with Class ACE Protection Profile Configuration evaluation (see [Clause 8](#)), Class APE Protection Profile (PP) evaluation (see [Clause 7](#)) and Class ASE Security Target (ST) evaluation (see [Clause 9](#)). The second aspect is verification of the TOE’s conformance with its SFRs and SARs. By demonstrating that the PP, PP-Module, PP-Configuration or 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.

6.5 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.

6.6 Component taxonomy

This document 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.

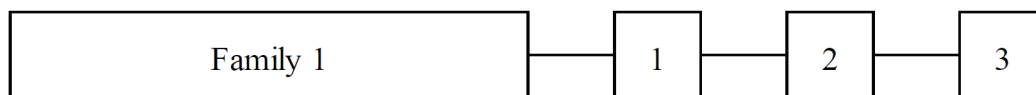


Figure 4 — Sample class decomposition diagram

In [Figure 4](#) 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 document are all linearly hierarchical, although linearity is not a mandatory criterion for assurance families that may be added in the future.

7 Class APE Protection Profile (PP) evaluation

7.1 Introduction

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 ISO/IEC 15408-1, Annex B and ISO/IEC 15408-1, Annex D, as these annexes clarify the concepts here and provide many examples.

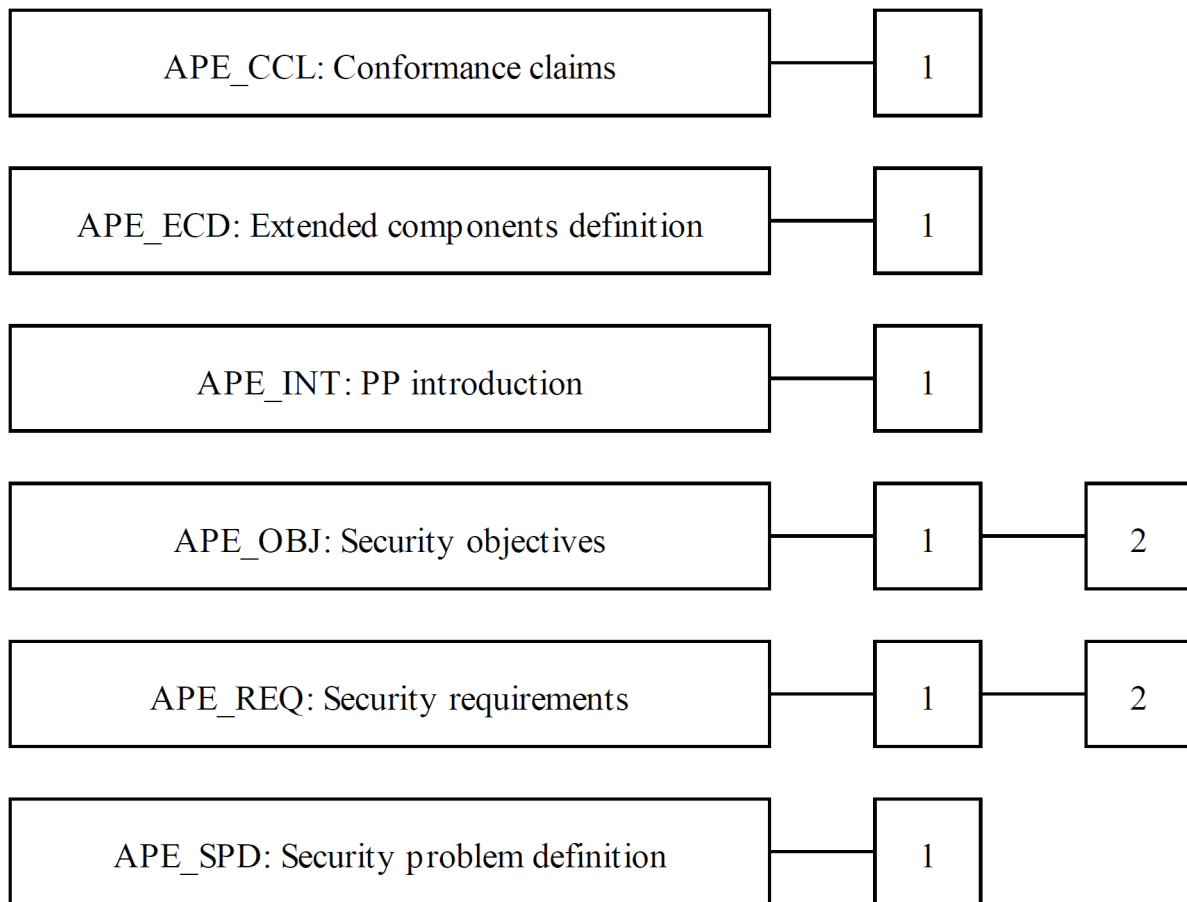


Figure 5 — APE: Protection Profile (PP) evaluation, class decomposition

Table 1 — Dependency table for Class APE: Protection Profile (PP) evaluation

	APE_ECD.1	APE_INT.1	APE_OBJ.1	APE_OBJ.2	APE_REQ.1	APE_SPD.1
APE_CCL.1	X	X	-		X	-
APE_ECD.1						
APE_INT.1						
APE_OBJ.1						X
APE_OBJ.2						X
APE_REQ.1	X		X			X
APE_REQ.2	X			X		-
APE_SPD.1						

7.2 Conformance claims (APE_CCL)

7.2.1 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.

7.2.2 Conformance claims (APE_CCL.1)

Dependencies:

- APE_INT.1, PP introduction
- APE_ECD.1, Extended components definition
- APE_REQ.1, Direct rationale security requirements

7.2.2.1 Developer action elements

APE_CCL.1.1D

The developer shall provide a conformance claim.

APE_CCL.1.2D

The developer shall provide a conformance claim rationale.

APE_CCL.1.3D

The developer shall provide a conformance statement.

7.2.2.2 Content and presentation elements

APE_CCL.1.1C

The conformance claim shall identify the ISO/IEC 15408 edition to which the PP claims conformance.

APE_CCL.1.2C

The 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”.

APE_CCL.1.3C

The conformance claim shall describe the conformance of the PP to ISO/IEC 15408-3 as either “ISO/IEC 15408-3 conformant” or “ISO/IEC 15408-3 extended”.

APE_CCL.1.4C

The conformance claim shall be consistent with the extended components definition.

APE_CCL.1.5C

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

APE_CCL.1.6C

The conformance claim shall describe any conformance of the PP to a functional package as one of package-conformant, package-augmented, or package-tailored.

APE_CCL.1.7C

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

APE_CCL.1.8C

The conformance claim shall describe any conformance of the PP to another PP as PP Conformant.

APE_CCL.1.9C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP(s) to which conformance is being claimed.

APE_CCL.1.10C

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 and any functional packages for which conformance is being claimed.

APE_CCL.1.11C

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

APE_CCL.1.12C

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

APE_CCL.1.13C

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

APE_CCL.1.14C

For an exact conformance PP, the conformance statement shall contain an allowed-with statement that identifies the set of PPs (if any) to which, in combination with the PP under evaluation, exact conformance is allowed to be claimed.

APE_CCL.1.15C

For an exact conformance PP, the conformance statement shall contain an allowed-with statement that identifies the set of PP-Modules (if any) that are allowed to be used with the PP under evaluation in a PP-Configuration.

APE_CCL.1.16C

The conformance statement shall identify the set of derived Evaluation Methods and Evaluation Activities (if any) that shall be used with the PP under evaluation. This list shall contain:

- any Evaluation methods and Evaluation activities that are specified for the PP under evaluation;
- any Evaluation methods and Evaluation activities specified in conformance statements of PPs to which conformance is being claimed by the PP under evaluation;
- any Evaluation methods and Evaluation activities specified in the Security Requirements sections of packages to which conformance is being claimed by the PP under evaluation.

7.2.2.3 Evaluator action elements

APE_CCL.1.1E

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

7.3 Extended components definition (APE_ECD)

7.3.1 Objectives

Extended security requirements are requirements that are not based on components from ISO/IEC 15408-2 or this document, but which 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 document components.

7.3.2 Extended components definition (APE_ECD.1)

7.3.2.1 Developer action elements

APE_ECD.1.1D

The developer shall provide a statement of security requirements.

APE_ECD.1.2D

The developer shall provide an extended components definition.

7.3.2.2 Content and presentation elements

APE_ECD.1.1C

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

APE_ECD.1.2C

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

APE_ECD.1.3C

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

APE_ECD.1.4C

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

APE_ECD.1.5C

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

7.3.2.3 Evaluator action elements

APE_ECD.1.1E

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

APE_ECD.1.2E

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

7.4 PP introduction (APE_INT)

7.4.1 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.

7.4.2 PP introduction (APE_INT.1)

7.4.2.1 Developer action elements

APE_INT.1.1D

The developer shall provide a PP introduction.

7.4.2.2 Content and presentation elements

APE_INT.1.1C

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

APE_INT.1.2C

The PP reference shall uniquely identify the PP.

APE_INT.1.3C

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

APE_INT.1.4C

The TOE overview shall identify the TOE type.

APE_INT.1.5C

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

7.4.2.3 Evaluator action elements

APE_INT.1.1E

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

7.5 Security objectives (APE_OBJ)

7.5.1 Objectives

The security objectives are a concise statement of the intended response to the security problem defined through the Security problem definition (APE_SPD) (see [7.7](#)) 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.

7.5.2 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.

7.5.3 Security objectives for the operational environment (APE_OBJ.1)

Dependencies: APE_SPD.1, Security problem definition

7.5.3.1 Developer action elements

APE_OBJ.1.1D

The developer shall provide a statement of security objectives for the operational environment.

APE_OBJ.1.2D

The developer shall provide a security objectives rationale for the security objectives for the operational environment.

7.5.3.2 Content and presentation elements

APE_OBJ.1.1C

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

APE_OBJ.1.2C

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.

APE_OBJ.1.3C

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

7.5.3.3 Evaluator action elements

APE_OBJ.1.1E

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

7.5.4 Security objectives (APE_OBJ.2)

Dependencies: APE_SPD.1, Security problem definition

7.5.4.1 Developer action elements

APE_OBJ.2.1D

The developer shall provide a statement of security objectives.

APE_OBJ.2.2D

The developer shall provide a security objectives rationale.

7.5.4.2 Content and presentation elements

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.

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.

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.

APE_OBJ.2.4C

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

APE_OBJ.2.5C

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

APE_OBJ.2.6C

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

7.5.4.3 Evaluator action elements**APE_OBJ.2.1E**

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

7.6 Security requirements (APE_REQ)**7.6.1 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.

7.6.2 Component levelling

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

7.6.3 Direct rationale security requirements (APE_REQ.1)

Dependencies:

- APE_ECD.1, Extended components definition
- APE_OBJ.1, Security objectives for the operational environment
- APE_SPD.1, Security problem definition

7.6.3.1 Developer action elements**APE_REQ.1.1D**

The developer shall provide a statement of security requirements.

APE_REQ.1.2D

The developer shall provide a security requirements rationale.

7.6.3.2 Content and presentation elements

APE_REQ.1.1C

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

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.

APE_REQ.1.3C

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

APE_REQ.1.4C

All operations shall be performed correctly.

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.

APE_REQ.1.6C

The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.

APE_REQ.1.7C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) counter all threats for the TOE.

APE_REQ.1.8C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) enforce all OSPs for the TOE.

APE_REQ.1.9C

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

APE_REQ.1.10C

The statement of security requirements shall be internally consistent.

7.6.3.3 Evaluator action elements

APE_REQ.1.1E

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

7.6.4 Derived security requirements (APE_REQ.2)

Dependencies: APE_OBJ.2, Security objectives
 APE_ECD.1, Extended components definition

7.6.4.1 Developer action elements

APE_REQ.2.1D

The developer shall provide a statement of security requirements.

APE_REQ.2.2D

The developer shall provide a security requirements rationale.

7.6.4.2 Content and presentation elements

APE_REQ.2.1C

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

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.

APE_REQ.2.3C

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

APE_REQ.2.4C

All operations shall be performed correctly.

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.

APE_REQ.2.6C

The security requirements rationale shall trace each SFR back to the **security objectives** for the TOE enforced by that SFR.

APE_REQ.2.7C

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

APE_REQ.2.8C

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

APE_REQ.2.9C

The statement of security requirements shall be internally consistent.

7.6.4.3 Evaluator action elements

APE_REQ.2.1E

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

7.7 Security problem definition (APE_SPD)

7.7.1 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.

7.7.2 Security problem definition (APE_SPD.1)

7.7.2.1 Developer action elements

APE_SPD.1.1D

The developer shall provide a security problem definition.

7.7.2.2 Content and presentation elements

APE_SPD.1.1C

The security problem definition shall describe the threats.

APE_SPD.1.2C

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

APE_SPD.1.3C

The security problem definition shall describe the organizational security policies (OSPs).

APE_SPD.1.4C

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

7.7.2.3 Evaluator action elements

APE_SPD.1.1E

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

8 Class ACE Protection Profile Configuration evaluation

8.1 Introduction

Evaluating a PP-Configuration is required to demonstrate that the PP-Configuration is sound and consistent. These properties are necessary for the PP-Configuration to be suitable for use as the basis for writing an ST.

Class ACE Protection Profile Configuration evaluation (see [Clause 8](#)) is defined for the evaluation of a PP-Configuration composed of at least one PP and one other component (PPs and/or PP-Modules). The evaluation of PPs is addressed in Class APE Protection Profile (PP) evaluation (see [Clause 7](#)). Class ACE Protection Profile Configuration evaluation (see [Clause 8](#)) defines the requirements for:

- Evaluating the PP-Modules in the framework of their PP-Modules Base(s) (components ACE_INT.1, PP-Module introduction, ACE_CCL.1, PP-Module conformance claims, ACE_SPD.1, PP-Module security problem definition, ACE_OBJ.1, PP-Module security objectives for the operational environment or ACE_

OBJ.2, PP-Module security objectives, ACE_REQ.1, PP-Module direct rationale security requirements or ACE_REQ.2, PP-Module derived security requirements, and ACE_MCO.1, PP-Module consistency).

- Evaluating the consistency of the combination of all the PPs and PP-Modules that belong to the PP-Configuration (see ACE_CCO.1, PP-Configuration consistency).

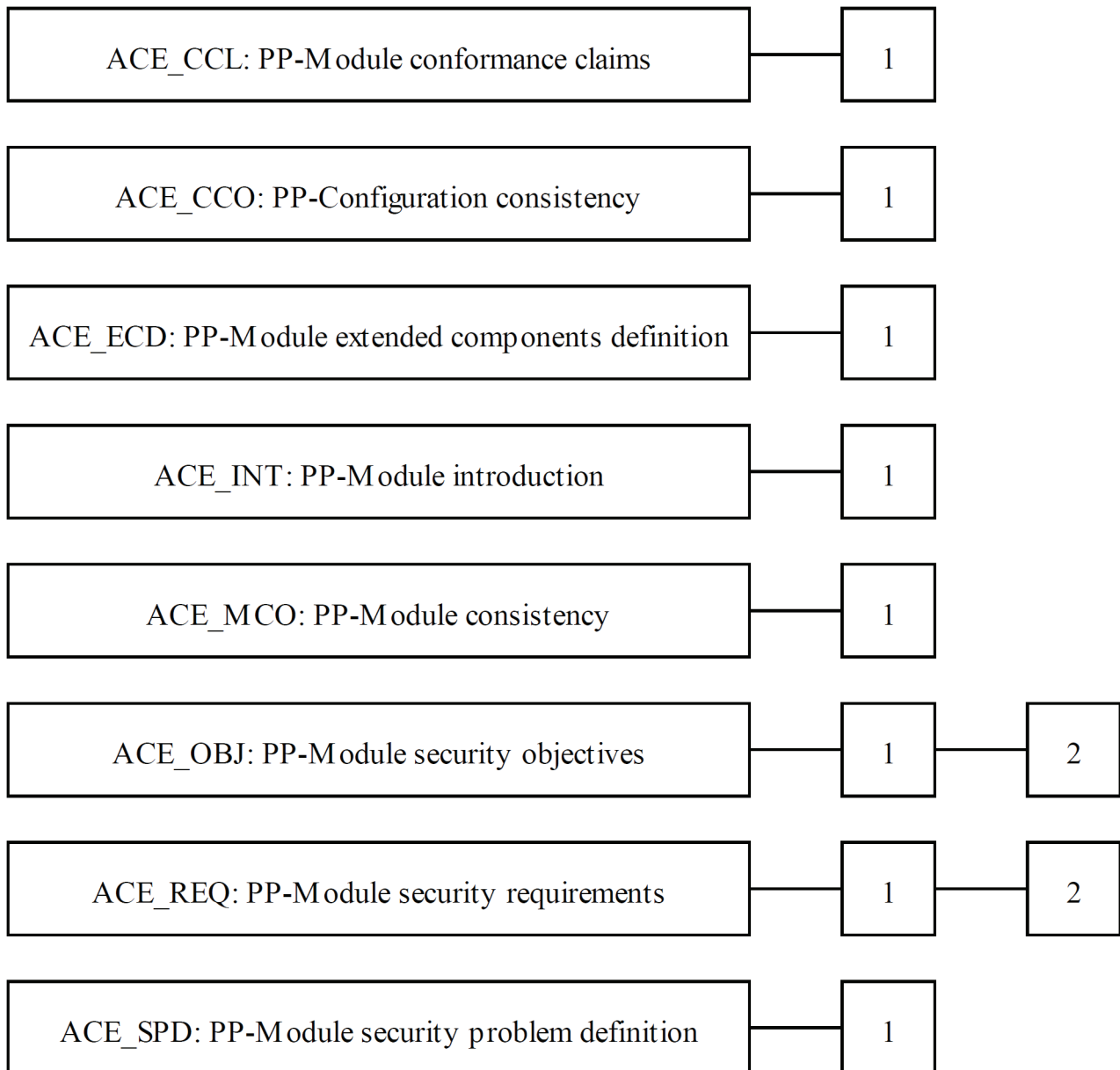


Figure 6 — ACE: Protection Profile Configuration evaluation, class decomposition

Table 2 — Dependency table for Class ACE: Protection Profile Configuration evaluation

	ACE_CCL.1	ACE_ECD.1	ACE_INT.1	ACE_MCO.1	ACE_OBJ.1	ACE_OBJ.2	ACE_REQ.1	ACE_REQ.2	ACE_SPD.1
ACE_CCL.1		X	X		-	-	O ¹	O ¹	-
ACE_CCO.1	X	X	X	X	O ¹	O ¹	O ²	O ²	X
ACE_ECD.1									
ACE_INT.1									
ACE_MCO.1		-	X		O ¹	O ¹	O ²	O ²	X
ACE_OBJ.1									X
ACE_OBJ.2									X
ACE_REQ.1		X			X				X
ACE_REQ.2		X				X			-
ACE_SPD.1									

8.2 PP-Module conformance claims (ACE_CCL)

8.2.1 Objectives

The objective of this family is to determine the validity of the conformance claim and conformance statement. A PP-Module cannot claim conformance to any PP, PP-Configuration, or another PP-Module.

8.2.2 PP-Module conformance claims (ACE_CCL.1)

Dependencies: ACE_INT.1, PP-Module introduction
 ACE_ECD.1, PP-Module extended components definition
 [ACE_REQ.1, PP-Module direct rationale security requirements or
 ACE_REQ.2, PP-Module derived security requirements]

8.2.2.1 Developer action elements

ACE_CCL.1.1D

The developer shall provide a conformance claim.

ACE_CCL.1.2D

The developer shall provide a conformance statement.

8.2.2.2 Content and presentation elements

ACE_CCL.1.1C

The conformance claim shall identify the ISO/IEC 15408 edition to which the PP-Module claims conformance.

ACE_CCL.1.2C

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

ACE_CCL.1.3C

The conformance statement shall describe the conformance type required of any ST to the PP-Module (as part of a PP-Configuration) as one of exact, strict, or demonstrable.

ACE_CCL.1.4C

The conformance claim shall describe the conformance of the PP-Module to ISO/IEC 15408-3 as either “ISO/IEC 15408-3 conformant” or “ISO/IEC 15408-3 extended”.

ACE_CCL.1.5C

The conformance claim shall be consistent with the extended components definition.

ACE_CCL.1.6C

The conformance claim shall identify all functional packages to which the PP-Module claims conformance.

ACE_CCL.1.7C

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

ACE_CCL.1.8C

The conformance claim shall identify all assurance packages to which the PP-Module claims conformance.

ACE_CCL.1.9C

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

ACE_CCL.1.10C

For exact conformance, the PP-Module’s conformance statement shall contain an allowed-with statement that identifies the set of PPs and PP-Modules (exclusive of those PPs and PP-Modules that are included in the PP-Module Base) to which, in combination with the PP-Module under evaluation, exact conformance is allowed to be claimed.

ACE_CCL.1.11C

The conformance statement may identify the set of ISO/IEC 18045-derived Evaluation methods and Evaluation activities that shall be used with the PP-Module under evaluation. This list shall contain any Evaluation methods and Evaluation activities that are specified in the PP-Module but also any Evaluation methods and Evaluation activities specified in the PP-Module Base(s) and/or in the packages (if any) for which conformance is being claimed by the PP-Module under evaluation.

8.2.2.3 Evaluator action elements

ACE_CCL.1.1E

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

8.3 PP-Configuration consistency (ACE_CCO)

8.3.1 Objectives

The objective of this family is to determine the well-formedness and the consistency of the PP-Configuration.

8.3.2 PP-Configuration consistency (ACE_CCO.1)

Dependencies:

- ACE_INT.1, PP-Module introduction
- ACE_CCL.1, PP-Module conformance claims
- ACE_SPD.1, PP-Module security problem definition
- [ACE_OBJ.1, PP-Module security objectives for the operational environment or
ACE_OBJ.2, PP-Module security objectives]
- ACE_ECD.1, PP-Module extended components definition
- [ACE_REQ.1, PP-Module direct rationale security requirements or
ACE_REQ.2, PP-Module derived security requirements]
- ACE_MCO.1, PP-Module consistency

8.3.2.1 Developer action elements

ACE_CCO.1.1D

The developer shall provide the reference of the PP-Configuration.

ACE_CCO.1.2D

The developer shall provide a components statement.

ACE_CCO.1.3D

The developer shall provide a TOE overview.

ACE_CCO.1.4D

The developer shall provide a conformance claim.

ACE_CCO.1.5D

The developer shall provide a conformance statement within the conformance claim.

ACE_CCO.1.6D

The developer shall provide a consistency rationale.

ACE_CCO.1.7D

The developer shall provide a SAR statement.

ACE_CCO.1.8D

The developer shall provide the set of evaluation methods and/or activities that are applicable to the PP-Configuration.

8.3.2.2 Content and presentation elements

ACE_CCO.1.1C

The PP-Configuration reference shall uniquely identify the PP-Configuration.

ACE_CCO.1.2C

The PP-Configuration components statement shall uniquely identify the PPs and PP-Modules that compose the PP-Configuration.

ACE_CCO.1.3C

For each PP-Module identified in the PP-Configuration components statement, the components statement shall include the PP-Module Base required by the identified PP-Module. If the PP-Module specifies alternative PP-Module Bases, only one of these PP-Module Bases shall be referred to in the PP-Configuration.

ACE_CCO.1.4C

For a multi-assurance PP-Configuration, the components statement shall describe the organization of the TSF in terms of the sub-TSFs defined in the PPs and PP-Modules defined in the PP-Configuration.

ACE_CCO.1.5C

The TOE overview shall identify the TOE type.

ACE_CCO.1.6C

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

ACE_CCO.1.7C

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

ACE_CCO.1.8C

The conformance claim shall identify the ISO/IEC 15408 edition(s) to which the PP-Configuration components claim conformance.

ACE_CCO.1.9C

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

ACE_CCO.1.10C

The conformance claim shall describe the conformance of the PP-Configuration to ISO/IEC 15408-3 as either “ISO/IEC 15408-3 conformant” or “ISO/IEC 15408-3 extended”.

ACE_CCO.1.11C

The conformance claim shall be consistent with the conformance claims of the PP-Configuration components.

ACE_CCO.1.12C

The conformance claim of a PP-Configuration shall include an assurance package conformance claim consisting of statements describing any conformance of the PP-Configuration to an assurance package as either package-conformant or package-augmented.

ACE_CCO.1.13C

The conformance statement shall specify the required conformance to the PP-Configuration as one of exact, strict, demonstrable, or it shall provide the list of conformance types that are required by each of the PP-Configuration components.

ACE_CCO.1.14C

For the exact conformance case, the allowed-with statement of the conformance statement of each PP included in the components statement of the PP-Configuration shall identify all the PP-Configuration components as being allowed to be used in combination with the PP in a PP-Configuration.

ACE_CCO.1.15C

For the exact conformance case, the allowed-with statement of the conformance statement of each PP-Module included in the components statement of the PP-Configuration shall identify all the PP-Configuration components that are not in the PP-Module Base(s) for that particular PP-Module as being allowed to be used in combination with the PP-Module in a PP-Configuration.

ACE_CCO.1.16C

For PP-Configurations that are not of exact conformance type (i.e. for PP-Configurations of strict or demonstrable conformance type), the conformance statement of a PP-Configuration may include an Evaluation methods and Evaluation activities reference statement that identifies the set of ISO/IEC 18045-derived Evaluation methods and Evaluation activities that are applicable to the PP-Configuration under evaluation.

ACE_CCO.1.17C

The consistency rationale shall demonstrate that the TOE type defined in the PP-Configuration is consistent with the TOE types defined in the PPs and PP-Modules that belong to the PP-Configuration components statement.

ACE_CCO.1.18C

The consistency rationale shall demonstrate that the union of all the SPDs, security objectives and security functional requirements defined in the PP-Configuration components is consistent.

ACE_CCO.1.19C

For a single-assurance PP-Configuration, the SAR statement shall define a single set of SARs that applies to the entire TOE. For strict and demonstrable conformance, the set of SARs shall include the SARs identified in each of the PP-Configuration components. For exact conformance, the set of SARs shall be identical to the set of SARs identified in each of the PP-Configuration components.

ACE_CCO.1.20C

For a multi-assurance PP-Configuration, the SAR statement shall define the global set of SARs that applies to the entire TOE and the SARs that apply to each sub-TSF. For strict and demonstrable conformance, the global assurance set of SARs shall include the set of common SARs among the PP-Configuration components, and each set of SARs that apply to a sub-TSF shall include those identified for the PP-Configuration components associated with that sub-TSF. For exact conformance, the global assurance set of SARs shall be the set of common SARs among the PP-Configuration components, and each set of SARs that apply to a sub-TSF shall be identical to those identified for the PP-Configuration components associated with that sub-TSF.

ACE_CCO.1.21C

The SAR statement of a PP-Configuration shall include an assurance rationale that demonstrates the consistency of the applicable set of SARs with those defined in the components of the PP-Configuration under evaluation and their associated Evaluation methods and Evaluation activities. For a multi-assurance PP-Configuration, the assurance rationale shall demonstrate:

- that the global set of SARs is consistent with the threats as defined in the SPDs of the PP-Configuration components, and
- that the global set of SARs and the sets of SARs for each sub-TSF are consistent with each other.

8.3.2.3 Evaluator action elements

ACE_CCO.1.1E

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

ACE_CCO.1.2E

The evaluator *shall check* that the PP-Configuration consisting of all the PPs and PP-Modules identified in the component statement is consistent.

8.4 PP-Module extended components definition (ACE_ECD)

8.4.1 Objectives

Extended SFRs are requirements that are not based on components from ISO/IEC 15408-2 or this document, but which are based on extended components: components defined by the PP-Module author.

Evaluation of the definition of extended functional 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 document components.

8.4.2 PP-Module extended components definition (ACE_ECD.1)

8.4.2.1 Developer action elements

ACE_ECD.1.1D

The developer shall provide a statement of security requirements for the PP-Module.

ACE_ECD.1.2D

The developer shall provide an extended components definition for the PP-Module.

8.4.2.2 Content and presentation elements

ACE_ECD.1.1C

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

ACE_ECD.1.2C

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

ACE_ECD.1.3C

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

ACE_ECD.1.4C

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

ACE_ECD.1.5C

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

8.4.2.3 Evaluator action elements

ACE_ECD.1.1E

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

ACE_ECD.1.2E

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

8.5 PP-Module introduction (ACE_INT)

8.5.1 Objectives

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

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

8.5.2 PP-Module introduction (ACE_INT.1)

8.5.2.1 Developer action elements

ACE_INT.1.1D

The developer shall provide a PP-Module introduction.

8.5.2.2 Content and presentation elements

ACE_INT.1.1C

The PP-Module introduction shall contain a PP-Module reference, the identification of the PP-Module Base(s) and a TOE overview.

ACE_INT.1.2C

The PP-Module reference shall uniquely identify the PP-Module.

ACE_INT.1.3C

The identification of the PP-Module Base shall consist of a list of at least one PP and possibly other PPs and PP-Modules on which the PP-Module depends.

ACE_INT.1.4C

The identification of the PP-Module Base(s) shall describe the dependency structure of the PP-Module Base(s).

ACE_INT.1.5C

The PP-Module introduction shall contain as many TOE overviews as alternative PP-Module Bases.

ACE_INT.1.6C

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

ACE_INT.1.7C

The TOE overview shall identify the TOE type.

ACE_INT.1.8C

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

ACE_INT.1.9C

The TOE overview shall describe the differences of the TOE with regard to the TOEs defined in the PP-Module Base(s).

8.5.2.3 Evaluator action elements

ACE_INT.1.1E

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

8.6 PP-Module consistency (ACE_MCO)

8.6.1 Objectives

The objective of this family is to determine the consistency of the PP-Module and to state the correspondence between the PP-Module and its PP-Module Base(s).

8.6.2 PP-Module consistency (ACE_MCO.1)

Dependencies:

- ACE_INT.1, PP-Module introduction
- ACE_SPD.1, PP-Module security problem definition
- [ACE_OBJ.1, PP-Module security objectives for the operational environment or
ACE_OBJ.2, PP-Module security objectives]
- [ACE_REQ.1, PP-Module direct rationale security requirements or
ACE_REQ.2, PP-Module derived security requirements]

8.6.2.1 Developer action elements

ACE_MCO.1.1D

The developer shall provide a consistency rationale of the PP-Module for each of the alternative PP-Module Bases identified in the PP-Module introduction.

ACE_MCO.1.2D

The developer shall provide an assurance rationale of the PP-Module for each of the alternative PP-Module Bases identified in the PP-Module introduction.

8.6.2.2 Content and presentation elements

ACE_MCO.1.1C

The consistency rationale shall demonstrate that the TOE type of the PP-Module and the TOE types of its PP-Module Base(s) are consistent.

ACE_MCO.1.2C

The consistency rationale shall identify the assets of the PP-Module's SPD that also belong to some of its PP-Module Bases and amongst them those for which the PP-Module and the PP-Module Base define different security problems.

ACE_MCO.1.3C

The consistency rationale shall demonstrate that:

- the statement of the security problem definition is consistent with the statement of the security problem definition of its PP-Module Base(s);
- the statement of the security problem definition is consistent with the statement of the security problem definition of any functional package for which conformance is being claimed.

ACE_MCO.1.4C

The consistency rationale shall demonstrate that:

- the security objectives are consistent with the security objectives of its PP-Module Base(s);
- the security objectives are consistent with the security objectives of any functional package for which conformance is being claimed.

ACE_MCO.1.5C

The consistency rationale shall demonstrate that:

- the security functional requirements are consistent with the security functional requirements of its PP-Modules Base(s);
- the security functional requirements are consistent with the security functional requirements of any functional package for which conformance is being claimed.

ACE_MCO.1.6C

The assurance rationale shall demonstrate the internal consistency of the set of security assurance requirements of the PP-Module with regard to its security problem definition.

ACE_MCO.1.7C

The assurance rationale shall demonstrate the consistency of the set of security assurance requirements of the PP-Module with regard to the security assurance requirements of the PP-Module Base(s).

8.6.2.3 Evaluator action elements

ACE_MCO.1.1E

The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence. If the PP-Module specifies alternative PP-Module Bases, the evaluator *shall perform* this action for each consistency rationale.

8.7 PP-Module security objectives (ACE_OBJ)

8.7.1 Objectives

The security objectives are a concise statement of the intended response to the security problem defined through the PP-Module security problem definition (ACE_SPD) (see [8.9](#)) 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.

8.7.2 Component levelling

The components in this family are levelled on whether they prescribe only security objectives for the operational environment (see ACE_OBJ.1, PP-Module security objectives for the operational environment), or also security objectives for the TOE (see ACE_OBJ.2, PP-Module security objectives).

8.7.3 PP-Module security objectives for the operational environment (ACE_OBJ.1)

Dependencies: ACE_SPD.1, PP-Module security problem definition

8.7.3.1 Developer action elements

ACE_OBJ.1.1D

The developer shall provide a statement of security objectives for the operational environment of the PP-Module.

ACE_OBJ.1.2D

The developer shall provide a security objectives rationale for the operational environment of the PP-Module.

8.7.3.2 Content and presentation elements

ACE_OBJ.1.1C

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

ACE_OBJ.1.2C

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.

ACE_OBJ.1.3C

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

8.7.3.3 Evaluator action elements

ACE_OBJ.1.1E

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

8.7.4 PP-Module security objectives (ACE_OBJ.2)

Dependencies: ACE_SPD.1, PP-Module security problem definition

8.7.4.1 Developer action elements

ACE_OBJ.2.1D

The developer shall provide a statement of security objectives for the PP-Module.

ACE_OBJ.2.2D

The developer shall provide a security objectives rationale for the PP-Module.

8.7.4.2 Content and presentation elements

ACE_OBJ.2.1C

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

ACE_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.

ACE_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.

ACE_OBJ.2.4C

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

ACE_OBJ.2.5C

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

ACE_OBJ.2.6C

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

8.7.4.3 Evaluator action elements

ACE_OBJ.2.1E

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

8.8 PP-Module security requirements (ACE_REQ)

8.8.1 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.

8.8.2 Component levelling

The components in this family are levelled on whether the SFRs are derived from SPD (see ACE_REQ.1, PP-Module direct rationale security requirements), or whether the SFRs are derived from the security objectives for the TOE (see ACE_REQ.2, PP-Module derived security requirements.).

8.8.3 PP-Module direct rationale security requirements (ACE_REQ.1)

Dependencies:

- ACE_ECD.1, PP-Module extended components definition
- ACE_OBJ.1, PP-Module security objectives for the operational environment
- ACE_SPD.1, PP-Module security problem definition

8.8.3.1 Developer action elements

ACE_REQ.1.1D

The developer shall provide a statement of security requirements for the PP-Module.

ACE_REQ.1.2D

The developer shall provide a security requirements rationale for the PP-Module.

8.8.3.2 Content and presentation elements

ACE_REQ.1.1C

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

ACE_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.

ACE_REQ.1.3C

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

ACE_REQ.1.4C

All operations shall be performed correctly.

ACE_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.

ACE_REQ.1.6C

The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.

ACE_REQ.1.7C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) counter all the threats for the TOE.

ACE_REQ.1.8C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the operational environment) enforce all the OSPs for the TOE.

ACE_REQ.1.9C

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

ACE_REQ.1.10C

The statement of security requirements shall be internally consistent.

8.8.3.3 Evaluator action elements

ACE_REQ.1.1E

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

8.8.4 PP-Module derived security requirements (ACE_REQ.2)

Dependencies: ACE_ECD.1, PP-Module extended components definition

ACE_OBJ.2, PP-Module security objectives

8.8.4.1 Developer action elements

ACE_REQ.2.1D

The developer shall provide a statement of security requirements for the PP-Module.

ACE_REQ.2.2D

The developer shall provide a security requirements rationale for the PP-Module.

8.8.4.2 Content and presentation elements

ACE_REQ.2.1C

The statement of security requirements shall describe the SFRs and SARs (the SARs that apply to the PP-Module may be explicitly stated or inherited from the PP-Module Base(s)).

ACE_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.

ACE_REQ.2.3C

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

ACE_REQ.2.4C

All operations shall be performed correctly.

ACE_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.

ACE_REQ.2.6C

The security requirements rationale shall **trace each SFR back to** the security objectives for the TOE **enforced by that SFR.**

ACE_REQ.2.7C

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

ACE_REQ.2.8C

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

ACE_REQ.2.9C

The statement of security requirements shall be internally consistent.

8.8.4.3 Evaluator action elements

ACE_REQ.2.1E

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