

COMMITTEE DRAFT ISO/IEC CD 15408-1, revision		Reference document: SC 27 N18700	
Date: 2018-06-25		Supersedes document WG 3 N1463	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: 2018-08-20 Please submit your comments via the online balloting application by the due date indicated.		
ISO/IEC CD 15408-1, revision Title: IT Security techniques – Evaluation criteria for IT security — Part 1: Introduction and general model Project: ISO/IEC 15408-1 (revision)			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
For details regarding previous development stages refer to 2 nd page of this explanatory report.			
ISO/IEC NP 15408-1 (revision) Evaluation criteria for IT security -- Part 1 NWIP	53 rd WG 3 meeting, Oct. 2016, Recommendations 5, 6, 15, 19 (N16607 = WG 3 N1364).	Expert contr. (WG 3 N1368, N1371, N1373).	SP report (WG 3 N1363); Call f. editor (WG 3 N1387 = N16886); Liaisons to: CCDB (WG 3 N1330); The Open Group (WG 3 N1332); Text f. NWIP (N16963 [replaces N16883]).
ISO/IEC 15408-1 1 st WD	54 th WG 3 meeting, April 2017, Recommendations 5,10, 11, 14 (N17041 = WG 3 N1413).	Results of call f. editor (N17276); SoV (N17025).	PL NB endorsement of co-editor (N17549); Liaisons to: CCDB (WG 3 N1391); The Open Group (WG 3 N1394); ISO/TC 22/SC 32 (N17373); Text f. 1 st WD (WG 3 N1435).
ISO/IEC 15408-1 2 nd WD	55 th WG 3 meeting, October / November 2017, Recommendations 8, 10 (N17666 = WG 3 N1494).	SoCom (WG 3 N1461); Draft DoC (WG 3 N1501).	Editor's report (WG 3 N1465); Liaisons to: CCDB (WG 3 N1455); ISO/TC 22/SC 32 (N18103); DoC (WG 3 N1462); Text f. 2 nd WD (WG 3 N1463)
ISO/IEC 15408-1 1 st CD	56 th WG 3 meeting, April 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30 th SC 27 Plenary, April 2018, Resolution 6 (N18710).	SoCom (WG 3 N1526); Late Com (WG 3 N1562); Draft DoC (WG 3 N1501).	Liaison to: CCDB (WG 3 N1521); DoC (WG 3 N1527); Text f. 1 st CD (N18700).
CD Registration and Consideration In accordance with resolution 6 (see SC 27 N18710) of the 30 th SC 27 Plenary meeting held in Wuhan, China, 2018-04-23/24 the hereby attached document has been registered with the ISO Central Secretariat (ITTF) as 1st Committee Draft (CD) and is being circulated for a 1st CD 8 weeks letter ballot closing by 2018-08-20 Medium: http://isotc.iso.org/livelink/livelink/open/jtc1sc27 No. of pages: 2 + 138			

Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period IT security testing, evaluation and assurance standards and techniques	51 st WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1 st /2 nd call f. contr. (WG 3 N1259 /1317).
	52 nd WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3 rd call f. contr. (WG 3 N1377); Rapporteur's report (WG 3 N1320). Liaison to: CCDB (WG 3 N1266).

ISO/IEC JTC 1/SC 27/WG 3 N18700

Date: 2018-06-22

ISO/IEC WD 15408-1:####(EN)

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

**IT security techniques — Evaluation criteria for IT security — Part 1:
Introduction and general model**

***Techniques de sécurité IT — Critères d'évaluation pour la sécurité des technologies de
l'information — Partie 1 : Introduction et modèle général***

CD stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and **may** not be referred to as an International Standard.

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.

READ ME FIRST

Editors general notes for this draft.

Red text in a box are the Editors' comments.

In this draft the editors highlighted the keywords relating to the ISO verbal forms, *shall, should, may, can and must* using green text in order to highlight these words. This convention will be removed before the FDIS level documents.

In this first CD the editors have reviewed the use of the above verbal forms and have made a few recommended changes that reflect the correct usage within ISO documents. Reviewers should pay attention to this in case the editors have made mistakes in their determination. These have been indicated with the old form in *strikeout* and the suggested change. E.g. "*shall must*" Indicating that the editors recommend replacing "shall" by "must"

The Editors are prepared to organize a meeting on this topic, as well as the normative/informative status of the annexes.

Blue text in italics indicate text that was submitted in response to WD2 DE/SG9 (Multiple-SAR packages) during the editing period.

The Editors' had problems incorporating this contribution while maintaining the DoC agreed in Wuhan. Accordingly, the contribution has been presented in part 1 alongside the relevant portions for review.

The editors suggest that this topic needs further discussion by WG 3.

Some editorial changes have also been introduced in order to comply with the [ISO/IEC Directives part 2:2018](#)

The Editors have restructured the document in order to present the information more effectively and simplified the use of English vocabulary and grammar for consistency. This document is read by many people whose first language is not English and that the document will be translated into other languages.

The editors are aware that the figures are of low quality. In the final documents high quality images will be used. The Editors hope that they are legible in this draft.

The Editors thank the WG 3 contributors for their contributions and support during the editing cycle.

Legal Notice:

The text for the legal notice agreed between ISO/IEC and the CCDB will be included here.

46	Contents	
47	Foreword.....	ix
48	Introduction.....	x
49	1 Scope	1
50	2 Normative references.....	1
51	3 Terms and definitions	2
52	3.1 Terms and definitions in alphabetical order.....	2
53	3.2 Hierarchy of concepts	23
54	4 Abbreviated terms	23
55	5 Overview	25
56	5.1 General.....	25
57	5.2 The different parts of ISO/IEC 15408.....	25
58	5.3 Target audience of the ISO/IEC 15408 series	25
59	5.3.1 General.....	25
60	5.3.2 Risk owners.....	25
61	5.3.3 Developers	26
62	5.3.4 Technical working groups.....	26
63	5.3.5 Evaluators	26
64	5.3.6 Others.....	26
65	5.4 The Target of Evaluation (TOE).....	28
66	5.4.1 General.....	28
67	5.4.2 TOE Boundaries	29
68	5.4.3 Different representations of the TOE	29
69	5.4.4 Different configurations of the TOE	30
70	5.4.5 Operational environment of the TOE.....	30
71	5.5 Presentation of material in this document	31
72	6 General model	32
73	6.1 Background	32
74	6.2 Assets and security controls.....	32
75	6.3 Core constructs of the ISO/IEC 15408(all parts) paradigm.....	34
76	6.3.1 General.....	34
77	6.3.2 Security Target.....	35
78	6.3.3 Communicating security requirements.....	37
79	7 Tailoring security requirements.....	38
80	7.1 General.....	38
81	7.2 Operations.....	38
82	7.2.1 The iteration operation.....	39
83	7.2.2 The assignment operation.....	39
84	7.2.3 The selection operation	40
85	7.2.4 The refinement operation.....	40
86	7.3 Dependencies between components.....	41
87	7.4 Extended components	42
88	8 Packages.....	42
89	8.1 Package types.....	42
90	8.1.1 Assurance packages	42
91	8.1.2 Functional packages	42
92	8.2 Using packages	43
93	8.2.1 General.....	43
94	8.2.2 Assurance packages	43
95	8.2.3 Functional packages	43

96	9	Protection Profiles	45
97	9.1	General.....	45
98	9.2	General conformance claims and conformance statements made by PPs	45
99	9.2.1	Security problem definition:	46
100	9.2.2	Security objectives:	47
101	9.3	Additional requirements for PPs with an exact conformance statement.....	47
102	9.3.1	General.....	47
103	9.3.2	Conformance claims and statements for PPs in the exact conformance case	48
104	9.4	Additional requirements for PPs common to strict and demonstrable conformance	48
105	9.4.1	Conformance claims and statements in the strict and demonstrable conformance cases.....	48
106	9.4.2	Package claims.....	48
107	9.4.3	Additional requirements specific to the strict conformance case	48
108	9.4.4	Additional requirements specific to the demonstrable conformance case	49
109	9.5	Using PPs	49
110	9.6	Conformance statements and claims in the case of multiple PPs	50
111	9.6.1	General.....	50
112	9.6.2	Where exact conformance is specified.....	50
113	9.6.3	Where strict or demonstrable conformance is specified	50
114	9.7	Selection-based security functional components and SFRs.....	50
115	10	Modular Protection Profiles.....	51
116	10.1	General.....	51
117	10.2	Base-PPs.....	51
118	10.3	PP-Modules.....	51
119	10.3.1	General.....	51
120	10.3.2	Requirements for PP-Modules	51
121	10.4	PP-Configurations.....	53
122	10.4.1	General.....	53
123	10.4.2	Requirements for a PP-Configuration	53
124	10.4.3	PP-Configuration SAR statement.....	55
125	11	Security Targets	55
126	11.1	General.....	55
127	11.2	Conformance claims and the conformance statement.....	55
128	11.2.1	Conformance claims made by STs.....	55
129	11.2.2	Additional requirements for the SPD in the exact conformance case	57
130	11.2.3	Additional requirements for the Security Objectives in the exact conformance case.....	57
131	11.2.4	Additional requirements for the security requirements in the exact conformance case....	57
132	11.3	Using PP-Configurations in Security Targets.....	58
133	11.3.1	General.....	58
134	12	Evaluation and evaluation results	59
135	12.1	General.....	59
136	12.2	The evaluation context.....	61
137	12.3	Evaluation of PPs and PP-Configurations.....	61
138	12.4	<i>Multi-assurance evaluation</i>	62
139	12.5	Evaluation of STs	62
140	12.6	Evaluation of TOEs	63
141	12.7	Evaluation methods and activities	63
142	12.8	Evaluation results	63
143	12.8.1	Results of a PP-Configuration evaluation	63
144	12.8.2	Results of a PP evaluation.....	63
145	12.8.3	Results of an ST/TOE evaluation	64
146	13	Composition of assurance.....	65
147	Annex A (informative)	Specification of Security Targets and Direct Rationale STs.....	76
148	A.1	Goal and structure of this Annex.....	76

149	A.2	Using an ST	76
150	A.2.1	How an ST should be used.....	76
151	A.2.2	How an ST should not be used	77
152	A.3	Questions that can be answered with an ST.....	77
153	A.4	Mandatory contents of an ST.....	78
154	A.4.1	ST Introduction (ASE_INT).....	79
155	A.4.1.1	ST reference and TOE reference.....	79
156	A.4.1.2	TOE overview	80
157	A.4.1.2.1	Usage and major security features of a TOE	80
158	A.4.1.2.2	TOE type	80
159	A.4.1.2.3	Required non-TOE hardware/software/firmware	81
160	A.4.1.3	TOE description	81
161	A.4.2	Conformance claims (ASE_CCL)	82
162	A.4.3	Security problem definition (ASE_SPD)	83
163	A.4.3.1	Introduction	83
164	A.4.3.2	Threats.....	83
165	A.4.3.3	Organizational security policies (OSPs)	83
166	A.4.3.4	Assumptions	84
167	A.4.4	Security objectives (ASE_OBJ).....	84
168	A.4.4.1	General.....	84
169	A.4.4.2	High-level solution	85
170	A.4.4.3	Part-wise solutions.....	85
171	A.4.4.3.1	Security objectives for the TOE	85
172	A.4.4.3.2	Security objectives for the operational environment	85
173	A.4.4.4	Relation between Security Objectives and the security problem definition.....	86
174	A.4.4.4.1	Tracing between Security Objectives and the security problem definition	86
175	A.4.4.4.2	Providing a justification for the tracing.....	87
176	A.4.4.4.3	On countering threats.....	87
177	A.4.4.5	Security Objectives: conclusion	87
178	A.4.5	Extended Components Definition (ASE_ECD).....	87
179	A.4.6	Security requirements (ASE_REQ)	88
180	A.4.6.1	General.....	88
181	A.4.6.2	Security functional requirements (SFRs)	88
182	A.4.6.2.1	How ISO/IEC 15408 supports this translation.....	89
183	A.4.6.2.2	Relation between SFRs and Security Objectives.....	89
184	A.4.6.2.2.1	Tracing between SFRs and the Security Objectives for the TOE	89
185	A.4.6.2.2.2	Providing a justification for the tracing	89
186	A.4.6.3	Security assurance requirements (SARs).....	89
187	A.4.6.3.1	SARs and the security requirement rationale.....	90
188	A.4.6.4	Security requirements: conclusion	90
189	A.4.7	TOE summary specification (ASE_TSS)	91
190	A.4.8	Referring to other standards in an ST	92
191	A.4.9	Direct Rationale STs.....	93
192	A.4.9.1	General.....	93
193	A.4.9.2	Conformance claims (ASE_CCL) for Direct Rationale STs.....	94
194	A.4.9.3	Security Problem Definition (ASE_SPD) for Direct Rationale STs	94
195	A.4.9.3.1	General.....	94
196	A.4.9.3.2	Tracing between SFRs, Security Objectives and the security problem definition	95
197	Annex B (informative)	Specification of Protection Profiles and Modular PPs	96
198	B.1	Goal and structure of this Annex.....	96
199	B.2	Specification of a PP	97
200	B.2.1	Using a PP.....	97
201	B.2.1.1	How a PP is used.....	97
202	B.2.1.2	How a PP should must not be used.....	97
203	B.2.2	Mandatory Contents of a PP	97

204	B.2.2.1	PP introduction (APE_INT)	98
205	B.2.2.1.1	General.....	98
206	B.2.2.1.2	PP reference.....	98
207	B.2.2.1.3	TOE overview.....	99
208	B.2.2.1.3.1	Usage and major security features of a TOE.....	99
209	B.2.2.1.3.2	TOE Type.....	99
210	B.2.2.1.3.3	Available non-TOE hardware/software/firmware.....	99
211	B.2.3	Conformance claims and conformance statement (APE_CCL).....	100
212	B.2.3.1	General.....	100
213	B.2.3.2	Exact conformance	100
214	B.2.4	Security problem definition (APE_SPD).....	100
215	B.2.5	Security objectives (APE_OBJ).....	100
216	B.2.6	Extended components definition (APE_ECD).....	100
217	B.2.7	Security requirements (APE_REQ).....	100
218	B.2.8	TOE summary specification.....	101
219	B.2.9	Referring to other standards in a PP.....	101
220	B.2.10	Direct Rationale PPs	101
221	B.2.10.1	General.....	101
222	B.2.10.2	Conformance claims (ASE_CCL) for Direct Rationale PPs	102
223	B.2.10.3	Security Problem Definition (ASE_SPD) for Direct Rationale PPs.....	102
224	B.3	Specification of PP-Modules	103
225	B.3.1	Using a PP-Module.....	103
226	B.3.2	Mandatory Contents of a PP Module.....	103
227	B.3.2.1	PP-Module introduction	104
228	B.3.2.1.1	PP-Module reference.....	104
229	B.3.2.1.2	Base-PP identification.....	104
230	B.3.2.1.3	TOE overview	105
231	B.3.2.2	Consistency rationale.....	105
232	B.3.2.3	Conformance claims and conformance statement.....	105
233	B.3.2.3.1	General.....	105
234	B.3.2.3.2	The conformance statement.....	106
235	B.3.2.3.2.1	Exact conformance.....	106
236	B.3.2.4	Security problem definition.....	107
237	B.3.2.5	Security Objectives	107
238	B.3.2.6	Extended functional components definition.....	108
239	B.3.2.7	Security functional requirements.....	108
240	B.3.3	Direct Rationale PP-Modules	108
241	B.3.4	Guidance for inclusion of SPD-elements from Base-PP.....	109
242	B.4	Specification of PP-Configurations.....	109
243	B.4.1	Mandatory content of a PP-Configuration	109
244	B.4.1.1	PP-Configuration reference	110
245	B.4.1.2	PP-Configuration components statement.....	110
246	B.4.1.3	PP-Configuration conformance claims and conformance statement.....	110
247	B.4.1.3.1	General.....	110
248	B.4.1.3.2	Exact conformance.....	110
249	B.4.1.4	PP-Configuration SAR statement.....	112
250	B.4.2	Using a PP-Configuration	112
251	B.4.3	Evaluation of a PP-Configuration.....	112
252	B.4.4	Interpretation of PP-Configuration as a PP	112
253	B.4.4.1	General.....	112
254	B.4.4.2	TOE type.....	112
255	B.4.4.3	Conformance claims and conformance statement.....	112
256	B.4.4.3.1	General.....	112
257	B.4.4.3.2	Exact Conformance	113
258	B.4.4.4	Security problem definition.....	113

259	B.4.4.5	Security Objectives	113
260	B.4.4.6	Extended functional components definition.....	113
261	B.4.4.7	Security functional requirements.....	113
262	Annex C (informative)	Specification of Packages	115
263	C.1	Goal and structure of this Annex.....	115
264	C.2	Structure of packages and package families	115
265	C.2.1	General.....	115
266	C.2.2	Package family name.....	116
267	C.2.3	Package family overview.....	116
268	C.2.4	Package family objectives.....	116
269	C.2.5	Package identification.....	116
270	C.2.6	Package type.....	117
271	C.2.7	Package overview	117
272	C.2.8	Security problem definition.....	117
273	C.2.9	Security objectives.....	117
274	C.2.10	Application notes	117
275	C.2.11	Components (either SFRs or SARs)	117
276	Annex D (informative)	Guidance for Operations.....	118
277	D.1	Introduction	118
278	D.2	Examples of operations.....	118
279	D.2.1	The iteration operation.....	118
280	D.2.2	The assignment operation.....	118
281	D.2.3	The selection operation	118
282	D.2.4	The refinement operation.....	119
283	D.3	Organization of components	119
284	D.3.1	Class	120
285	D.3.2	Family.....	120
286	D.3.3	Component.....	120
287	D.3.4	Element	120
288	D.4	Extended components	120
289	D.4.1	How to define extended components.....	120
290	Annex E (informative)	PP Conformance.....	122
291	E.1	General.....	122
292	E.2	Demonstrable conformance	122
293	E.3	Strict conformance	122
294	E.4	Exact conformance	123
295	Bibliography.....		125
296			
297	Table of Figures		
298	Figure 1 — Security concepts and relationships.....		33
299	Figure 2 — Evaluation concepts and relationships		34
300	Figure 3 — Evaluation flow.....		60
301	Figure 4 — Layered composition.....		65
302	Figure 5 — Network composition.....		66
303	Figure 6 — Embedded composition		67
304	Figure 7 — Composed TOE evaluated using the ACO class.....		68
305	Figure 8 — Composite TOE		70
306			

307	Table of Tables	
308	Table 1— Road map to the “Evaluation criteria for IT security”	27
309	Table 2 — Information to be provided to the Application developer.....	72
310	Table 3 — Information to be provided to the Composite Product evaluator and evaluation authority....	72
311		

312 Foreword

313 ISO (the International Organization for Standardization) and IEC (the International Electrotechnical
314 Commission) form the specialized system for worldwide standardization. National bodies that are
315 members of ISO or IEC participate in the development of International Standards through technical
316 committees established by the respective organization to deal with particular fields of technical activity.
317 ISO and IEC technical committees collaborate in fields of mutual interest. Other international
318 organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the
319 work. In the field of information technology, ISO and IEC have established a joint technical committee,
320 ISO/IEC JTC 1.

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

325 Attention is drawn to the possibility that some of the elements of this document may be the subject of
326 patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.
327 Details of any patent rights identified during the development of the document will be in the
328 Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

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

335 This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology,
336 Subcommittee SC 27, IT Security techniques.

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

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

340 This **fourth** edition cancels and replaces the **third** edition (ISO/IEC 15408-1:2009), which has been
341 technically revised.

342 The main changes compared to the previous edition are as follows:

- 343 — The document has been restructured
- 344 — Technical changes have been introduced:
 - 345 ○ Review of the terminology,
 - 346 ○ The introduction of exact conformance,
 - 347 ○ The removal of low assurance PPs and the introduction of direct rationale PPs,
 - 348 ○ The introduction of PP-Modules.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations. The ISO/IEC 15408 series does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products **may** be implemented in hardware, firmware, or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results **may** help consumers to determine whether these IT products fulfil their security needs.

The ISO/IEC 15408 series is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using The ISO/IEC 15408 series in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, **can** result in meaningless evaluation results.

*The ISO/IEC 15408 series defines a flexible framework for the **multi-assurance evaluation** of IT products using predefined EALs from ISO/IEC 15408-5 or well-formed assurance packages of ISO/IEC 15408-3 components, which allows claiming a global assurance level for the entire TOE, and possibly multiple different assurance levels for different parts of the TOE.*

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties, and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

The ISO/IEC 15408 series address the protection of assets from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The ISO/IEC 15408 series **may** also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series **may** be applied in other areas of IT but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the ISO/IEC 15408 series. Some of these are identified below:

- a) The ISO/IEC 15408 series does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security **can** often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls.
- ~~b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.~~

Editors' Note:

The inclusion of TOE emanation (FPT_EMS) for emanation in part 2 means that the example given in b) is no longer be true.

Please will experts suggest a different example of technology that is not covered by the standard?

If no suggestions are received then item (b) will be removed in the next draft.

- c) The ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied.

NOTE The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 may be used to further derive evaluation activities and methods from ISO/IEC 18045.

- d) The ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria **may** be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series will be used for evaluation purposes in the context of such a framework.
- e) The procedures for use of evaluation results in accreditation are outside the scope of the ISO/IEC 15408 series. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors **must** make separate provisions for those aspects.
- f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the ISO/IEC 15408 series. In the case that independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which the ISO/IEC 15408 series is applied **must** make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. The term "should" has an additional meaning applicable when using this standard. See the note below. The following definition is given for the use of "should" in the ISO/IEC 15408 series.

should

within normative text, "should" indicates "that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required." (ISO/IEC Directives, Part 2).

NOTE The ISO/IEC 15408 series interprets "not necessarily required" to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

1 Scope

This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 *may* be tailored through the use of permitted operations.

It provides guidelines for using ISO/IEC 15408-4 compliant evaluation methods and activities.

NOTE Such methods and activities *may* be included in Protection Profiles, Security Targets, or supporting documents.

It provides guidelines for using ISO/IEC 15408-5, pre-defined compliant packages of security functional or assurance requirements in Protection Profiles and Security Targets.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This document gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation method given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

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 15408-2, *IT security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *IT security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

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

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

ISO/IEC 18045, *IT security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO/IEC/IEEE 24765:2010 and the following apply.

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

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 Terms and definitions in alphabetical order

Editors' Note

The editors are aware that the terminology will evolve throughout the career of this revision.

The editors have removed the previous subdivisions in this draft and presented the terms in alphabetical order. The editors are working hard on grouping terms according to a hierarchy of concepts, but do not plan to present this until the next draft.

Experts are asked:

1) not to comment current order of terms

2) to contribute to the concept-based order of terms see ISO/IEC 22216, Annex XXX

Additionally, editors draw experts' attention to verb functioning as dual-use wording, in particular, these marked as <evaluation verb>. In Editors opinion, they should not exist as vocabulary entries. Instead of which an introductory subclause on specific usage of these word in evaluation context should be created.

Experts are asked to contribute.

Editors note some general terminology issues:

a **sponsor** is the organization that is responsible for the production of a document. (For example the EALs guess the sponsor is the CCDB). Under the CCRA the term "sponsor" is used specifically, and this might be a confusing term to use in regard to identification of PPs, PP-Modules etc?

The **owner** of a document may be a different organization – For example an iTC

The **author** of a document is the entity writing the document. This can be different to the owner organization. e.g. consider a CPP that is sponsored by NIAP and Japan, the owner is the iTC, and the author is a subcontracted organization (that may change).

Editors request proposed definitions of these terms and appropriate use in the main text

3.1

acceptance criteria

criteria to be applied when performing the acceptance procedures

EXAMPLE successful document review, or successful testing in the case of software, firmware or hardware.

3.2

acceptance procedure

procedure followed in order to accept newly created or modified configuration items as part of the 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 **may** overlap:

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

EXAMPLE module, subsystem, quality control of the finished TOE.

508 c) subsequent to transport of configuration items

509 EXAMPLE parts of the TOE or preliminary products between different development sites;

510 d) subsequent to the delivery of the TOE to the consumer;

511 e) subsequent to the integration of the TOE

512 EXAMPLE inclusion of software, firmware and hardware components from other sources into the TOE.

513 3.3

514 action

515 evaluator action element of ISO/IEC 15408-3

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

518 3.4

519 activity

520 application of an assurance class of ISO/IEC 15408-3

521 3.5

522 administrator

523 entity that has a level of trust with respect to all policies implemented by the TSF

524 Note 1 to entry: Not all PPs or STs assume the same level of trust for administrators. Typically, administrators
525 are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies *may* be related to the
526 functionality of the TOE, others *may* be related to the operational environment.

527 3.6

528 adverse action

529 action performed by a threat agent on an asset

530 3.7

531 asset

532 entity that the owner of the TOE presumably places value upon

533 3.8

534 assignment

535 specification of an identified parameter in a functional element of a given functional or assurance
536 component

537 Note 1 to entry: Such functional element is also called a requirement.

538 3.9

539 assurance

540 grounds for confidence that a TOE meets the SFRs

541 **Editors' Note:**

542 Two definitions ie. assurance package (3.10) and functional package (3.94) should be aligned with 3.126
543 (package)

544 3.10

545 Assurance level

546 AL

547 *set of assurance requirements drawn from ISO/IEC 15408-3, representing the assurance activities*
548 *necessary to determine the perceived threats to assets are sufficiently mitigated by the TOE.*

549 3.11

550 assurance package

551 named set of security assurance requirements

552 EXAMPLE "EAL 3".

3.12

attack potential

measure of the effort needed to exploit a vulnerability in a TOE

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (for example: Expertise, resources, and motivation) and properties related to the vulnerability itself (for example: Window of opportunity, time to exposure).

3.13

augmentation

addition of one or more requirements to a package

Note 1 to entry: in case of a functional package augmentation such an augmentation is considered only in the context of one package and is not considered in the context with other packages or PPs or STs.

Note 2 to entry: in case of an assurance package augmentation refers to one or more SAR.

3.14

authentication data

information used to verify the claimed identity of a user

3.15

authorized user

TOE user who **may**, in accordance with the SFRs, perform an operation

3.16

base component

entity in a composed TOE, which has itself been the subject of an evaluation, providing services and resources to a dependent component

Editors' Note:

The notion of "base component" is used in both composition approaches: "composed evaluation" and "composite evaluation". The proposal is to keep the term component without any particular evaluation status, and use TOE when the component has been or requires evaluation. This is in line with the definition of "component TOE"

base component = entity in a multi-component product that provides services and resources to one or more dependent component(s)

3.17

Base Protection Profile

Base-PP

Protection Profile used as a basis to build a Protection Profile Configuration

3.18

base TOE developer

entity developing the base TOE or sponsoring a base TOE evaluation

Editors' Note

The original definition by JIL is "platform developer". The equivalent term would be "base component".

It is not clear that defining the term "base component developer" is necessary.

3.19

base TOE evaluator

entity performing the base TOE evaluation

3.20

base TOE evaluation authority

evaluation authority monitoring the evaluation of the base TOE

3.21

base TOE

TOE comprising the autonomous component(s) of a layered composite TOE

- 600 **3.22**
 601 **check**
 602 <evaluation verb> generate a verdict by a simple comparison
 603 Note 1 to entry: Evaluator expertise is not required. The statement that uses this verb describes what is
 604 mapped.
- 605 **3.23**
 606 **class**
 607 <taxonomy> set of ISO/IEC 15408 families that share a common focus
- 608 **3.24**
 609 **coherent**
 610 logically ordered and having discernible meaning
 611 Note 1 to entry: For documentation, this term addresses both the actual text and the structure of the document,
 612 in terms of whether it is understandable by its target audience.
- 613 **3.25**
 614 **compatible**
 615 <component> property of a component able to provide the services required by another component,
 616 through the corresponding interfaces of each component, in consistent operational environments
- 617 **3.26**
 618 **complete**
 619 property where all necessary parts of an entity have been provided
 620 Note 1 to entry: In terms of documentation, this means that all relevant information is covered in the
 621 documentation, at such a level of detail that no further explanation is required at that level of abstraction.
- 622 **3.27**
 623 **component**
 624 <taxonomy> smallest selectable set of elements on which requirements **may** be based
- 625 **3.28**
 626 **component TOE**
 627 successfully evaluated TOE that is part of another composed TOE
- 628 **3.29**
 629 **composed assurance package**
 630 **CAP**
 631 assurance package consisting of components drawn predominately from the ACO class, representing a
 632 point on the pre-defined scale for composition assurance
- 633 **3.30**
 634 **composed TOE**
 635 TOE comprised solely of two or more components that have been successfully evaluated
- 636 **3.31**
 637 **composite evaluation**
 638 evaluation of a composite TOE
- 639 **3.32**
 640 **composite product**
 641 TOE comprised of two or more component TOEs, at least one of which has been successfully evaluated

Editors' Note:

Avoid defining a product as a TOE. The alternative definition is as follows:

composite product = product comprised of two or more components which can be organized in two layers: a layer of autonomous base component(s) and a layer of dependent components

Note 1 to entry: The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach.

3.33

composite product evaluation authority

evaluation authority monitoring the evaluation of the composite product

3.34

composite product evaluation sponsor

entity in charge of contracting the composite product evaluation

3.35

composite product evaluator

entity performing the composite product evaluation

3.36

composite product integrator

entity installing the dependent components on the base component(s)

3.37

composite TOE

TOE composed of a superposition of two layers

Note 1 to entry: This definition does not preclude products that use 3 layers, for example that include middleware.

Editors' Note:

The following alternate definition is proposed:

composite TOE = TOE composed of two or more components which can be organized in two layers: a layer of already evaluated autonomous base TOE(s) and a layer of dependent components

3.38

configuration item

object managed by the configuration management system during the TOE development

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

[SOURCE: ISO/IEC/IEEE 24765:2010 3.563 modified, specification of TOE development requirement and note 1 to entry added]

3.39

configuration list

configuration management output document listing all configuration items 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. 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 ALC_CMC.

3.40

configuration management

CM

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

[SOURCE: ISO/IEC/IEEE 24765:2010 3.565]

3.41 configuration management documentation CM documentation

all configuration management documentation including configuration management output, configuration management list(s), configuration management system records, configuration management plan and configuration management usage documentation

3.42 configuration management evidence

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

EXAMPLE configuration management output, rationales provided by the developer, observations, experiments, or interviews made by the evaluator during a site visit

3.43 configuration management output

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

Note 1 to entry: These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies, and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle.

3.44 configuration management plan

description of how the configuration management system is used for the 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 **may** 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 **may** be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.

3.45 configuration management system

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

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

3.46 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.

3.47 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 TOE.

3.48

configuration management usage documentation

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

3.49

confirm

<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency

Note 1 to entry: The level of rigour required depends on the nature of the subject matter.

3.50

connectivity

property of the TOE allowing interaction with IT entities external to the TOE

Note 1 to entry: This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

3.51

counter

act on or respond to a particular threat so that the threat is eradicated or mitigated

3.52

covert channel

enforced, illicit signaling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE

3.53

delivery

transmission of the finished TOE from the production environment into the hands of the customer

Note 1 to entry: This product life-cycle phase **may** include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites.

3.54

demonstrable conformance

relation between an ST/PP and a PP, where the ST/PP provides an equivalent or more restrictive solution which solves the generic security problem in the PP

3.55

demonstrate

<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a “proof”

3.56

dependency

relationship between components such that a PP, ST or package including a component **shall** also include any other components that are identified as being depended upon or include a rationale as to why they are not

3.57

dependent component

entity in a composed TOE, which is itself the subject of an evaluation, relying on the provision on services by a base component

Editors' Note:

(see entry “base component”)

The notion of “dependent component” is used in both composition approaches: “composed evaluation” and “composite evaluation”. This definition should be used for “dependent TOE”.

The proposal is to keep the term component without any particular evaluation status, and use TOE when the component has been or requires evaluation. This is in line with the definition of “component TOE”

dependent component = entity in a multi-component product that relies on the provision of services and resources by one or more base components

3.58

dependent TOE

entity in a composed TOE which is itself the subject of an evaluation, relying on the provision on services by one or more base components

Note 1 to entry: applies only to the “composed” evaluation approach (not to the composite approach).

3.59

dependent TOE developer

entity developing the dependent TOE of a composed TOE

3.60

describe

<evaluation verb> provide specific details of an entity

3.61

determine

<evaluation verb> affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms “confirm” or “verify” which imply that an analysis has already been performed which needs to be reviewed

3.62

developer

organization responsible for the development of the TOE

3.63

development

product life-cycle phase which is concerned with generating the implementation representation of the TOE

Note 1 to entry: Throughout the ALC: Life-cycle support requirements, development, and related terms (developer, develop) are meant in the more general sense to comprise development and production.

3.64

development environment

environment in which the TOE is developed

Note 1 to entry: The conditions include physical facilities, security controls, IT systems and development tools.

3.65

development tool

tools, including any applicable test software that support the development and production of the TOE

EXAMPLE for a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.

3.66

direct rationale

type of Protection Profile or Security Target in which the SPD-elements of the SPD are mapped directly to the SFRs and possibly Security Objectives for the operational environment

Note 1 to entry: Direct rationale is an alternative method for specifying SFRs to the regular method of mapping via the SPD and the set of TOE Security Objectives.

3.67**domain separation****security domain separation**

security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process **can** affect the contents of a security domain of another user or of the TSF

3.68**element**

(taxonomy) most detailed level of definition of a security need

3.69**encountered potential vulnerability**

potential weakness in the TOE identified by the evaluator while performing Evaluation Activities that could be used to violate the SFRs

3.70**ensure**

<evaluation verb> guarantee a strong causal relationship between an action and its consequences

Note 1 to entry: When this term is preceded by the word “help” it indicates that the consequence is not fully certain, on the basis of that action alone.

3.71**entity**

identifiable item that is described by a set or collection of properties

Note 1 to entry: Entities include subjects, users (including external IT products), objects, information, sessions and/or resources

3.72**evaluation**

assessment of a PP, an ST, or a TOE, against defined criteria

Editors' Note:

All terms related to 'evaluation' need to be aligned with section 3.8 (set of definitions taken out from ISO/IEC TR 18045). Experts are asked for contributions to this task, additionally see ISO/IEC 22216, Annex XXX

3.73**evaluation activity****EA**

activity derived from work units defined in ISO/IEC 18045

Note 1 to entry: The concept of evaluation activities, and the combination of evaluation activities into "evaluation methods", is defined in ISO/IEC 15408-4.

3.74**evaluation assurance level****EAL**

set of security assurance requirements defined ISO/IEC 15408-3 and drawn from ISO/IEC 15408-5, representing a point on the ISO/IEC 15408 pre-defined assurance scale that form an assurance package

Editors' Note:

The following alternate definition is proposed:

evaluation assurance level**EAL**

group of packages that specify pre-defined sets of security assurance components

Note 1 to entry: EALs may be referenced in PPs and STs.

Note 2 to entry: These packages specify appropriate security assurances to be provided during an evaluation of a TOE.

Note 3 to entry: The complete set of EALs form a scale of increasing assurance.

3.75

evaluation authority

body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements ISO/IEC 15408 for that community by means of an evaluation scheme

Editors' Note:

The following definitions are proposed to avoid circular definitions for evaluation authority and evaluation scheme:

evaluation authority

body operating an evaluation scheme

Note 1 to entry: By applying the evaluation scheme evaluation authority sets the standards and monitors the quality of evaluations conducted by bodies within a specific community.

evaluation scheme:

rules, procedures, and management to carrying evaluations of IT products security implementing all parts of ISO/IEC 15408

Note 1 to entry: Administrative and regulatory framework is usually a part of an evaluation scheme. Such framework is out of the scope of ISO/IEC 15408.

Note 2 to entry: The objective of evaluation scheme is to ensure that high standards of competence and impartiality are maintained and a consistency of evaluations is achieved.

Note 3 to entry: evaluation scheme is usually established by an evaluation authority, which defines the evaluation environment, including criteria and methodology required to conduct IT security evaluations.

3.76

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

3.77

evaluation evidence

item used as a factual basis for establishing the verdict of an evaluation activity

3.78

evaluation method

set of evaluation activities used to build knowledge and provide assurance that the TOE meets the requirements

Note 1 to entry: in practice defined as a set of work units defined in ISO/IEC 18045 or evaluation activities that derive work units from ISO/IEC 18045 in accordance with ISO/IEC 15408-4.

Editors' Note:

Needs to be resolved with the 'evaluation method' definition in 18045:

evaluation method

set of one or more evaluation activities that are defined in order to interpret and/or refine ISO/IEC 18045 work units for application in a specific context

"Evaluation method" in the framework of 18405 refers to evaluator's work in general, which corresponds to the definition given above. The new proposal is about 15408-4. The term should explicitly gather the two meanings: one in the general context, one in the context of Part 4.

For the meaning in the context of Part-4, the proposal is as follows:

"set of one or more evaluation activities that are derived from ISO/IEC 18045 work units for application in a specific context"

936 **3.79**

937 **evaluation scheme**

938 administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation
939 authority within a specific community

940 **Editors' Note:**

941 Needs to be resolved with "scheme" in 18045 definitions

942 **3.15**

943 **scheme**

944 set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and
945 methodology required to conduct IT security evaluations

947 **3.80**

948 **evaluation technical report**

949 **ETR**

950 report that documents the overall verdict and its justification, produced by the evaluator, and
951 submitted to an evaluation authority

952 **Editors' Note:**

953 Editors propose the following to align to the JTC1 Directives:

954 **evaluation technical report**

955 documentation of the overall verdict and its justification, produced by the evaluator and submitted to an
956 evaluation authority

957 **3.81**

958 **evaluator**

959 individual assigned to perform evaluations in accordance with a given evaluation standard and
960 associated evaluation methodology

961 Note 1 to entry: An example of evaluation standards is The ISO/IEC 15408 series with the associated evaluation
962 methodology given in ISO/IEC 18045.

963 [SOURCE: ISO/IEC 19896-1:2018]

964 **3.82**

965 **exact conformance**

966 **EC**

967 hierarchical relationship between a PP and an ST where all the requirements in the ST are drawn only
968 from the PP

969 Note 1 to entry: an ST is allowed to claim exact conformance to one or more PPs and/or PP configurations.

970 Note 2 to entry: PPs are not allowed to claim exact conformance to other PPs.

971 **3.83**

972 **examine**

973 <evaluation verb> generate a verdict by analysis using evaluator expertise

974 Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is
975 analysed.

976 **3.84**

977 **exhaustive**

978 <evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity
979 according to an unambiguous plan

980 Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is
981 related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has

been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.

3.85

explain

<evaluation verb> give argument accounting for the reason for taking a course of action

Note 1 to entry: This term differs from both “describe” and “demonstrate”. It is intended to answer the question “Why?” without actually attempting to argue that the course of action that was taken was necessarily optimal.

3.86

exploitable vulnerability

weakness in the TOE that **can** be used to violate the SFRs in the operational environment for the TOE

3.87

extended security requirement

security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408

Note 1 to entry: An extended security requirement **may** be either an SAR or an SFR.

Note 2 to entry: Extended security requirements are defined within extended component definitions.

3.88

Extended TOE

text

3.89

Extended TSF

text

3.90

external entity

user

human or IT entity possibly interacting with the TOE from outside of the TOE boundary

Editors' Note:

Proposed

external entity

user

human, technical system or one of its components interacting with the TOE from outside of the TOE boundary

3.91

family

<taxonomy> set of components that share a similar goal but differ in emphasis or rigour

3.92

formal

expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

3.93

functional interface

external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements

Note 1 to entry: In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.

- 1026 **3.94**
 1027 **functional package**
 1028 named set of security functional requirements that **may** be accompanied by an SPD and Security
 1029 Objectives derived from that SPD
- 1030 **3.95**
 1031 **guidance documentation**
 1032 documentation that describes the delivery, preparation, operation, management and/or use of the TOE
- 1033 **3.96**
 1034 ***global Assurance Level***
 1035 *set of assurance requirements drawn from ISO/IEC 15408-3 that are to be applied to the entire TSF in a*
 1036 *multi-assurance evaluation*
- 1037 **3.97**
 1038 **identity**
 1039 representation uniquely identifying an entity within the context of the TOE
- 1040 **EXAMPLE** An example of such a representation is a string.
- 1041 Note 1 to entry: entities **can** be diverse such as a user, process, or disk. For a human user, the representation
 1042 could be the full or abbreviated name or a unique pseudonym.
- 1043 Note 2 to entry: An entity **can** have more than one identity.
- 1044 **3.98**
 1045 **implementation representation**
 1046 least abstract representation of the TSF, specifically the one that is used to create the TSF itself without
 1047 further design refinement
- 1048 Note 1 to entry: Source code that is then compiled or a hardware drawing that is used to build the actual
 1049 hardware are examples of parts of an implementation representation.
- 1050 **3.99**
 1051 **informal**
 1052 expressed in natural language
- 1053 **3.100**
 1054 **installation**
 1055 procedure performed by a human user embedding the TOE in its operational environment and putting
 1056 it into an operational state
- 1057 Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE.
 1058 The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be
 1059 performed by the developer they are denoted as “generation” throughout the class ALC: Life-cycle support. If the
 1060 TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as
 1061 installation.
- 1062 **3.101**
 1063 **inter TSF transfer**
 1064 communication between the TOE and the security functionality of other trusted IT products
- 1065 **3.102**
 1066 **interaction**
 1067 general communication-based activity between entities
- 1068 **3.103**
 1069 **interface**
 1070 means of communication with an entity
- 1071 **3.104**
 1072 **internal communication channel**
 1073 communication channel between separated parts of the TOE

1074	3.105
1075	internal TOE transfer
1076	communicating data between separated parts of the TOE
1077	3.106
1078	internally consistent
1079	no apparent contradictions exist between any aspects of an entity
1080	Note 1 to entry: In terms of documentation, this means that there can be no statements within the
1081	documentation that can be taken to contradict each other.
1082	3.107
1083	interpretation
1084	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045, or scheme requirement
1085	3.108
1086	iteration
1087	use of the same component to express two or more distinct requirements
1088	3.109
1089	justify
1090	<evaluation verb> provide a rationale providing sufficient reason
1091	Note 1 to entry: The term 'justify' is more rigorous than a 'demonstrate'. This term requires significant rigour in
1092	terms of very carefully and thoroughly explaining every step of a logical analysis leading to a conclusion.
1093	3.110
1094	laboratory
1095	organization with a management system providing evaluation and or testing work in accordance with a
1096	defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the
1097	security functionality of IT products
1098	Note 1 to entry: These organizations are often given alternative names by various approval authorities. For
1099	example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial
1100	Evaluation Facility (CLEF).
1101	[SOURCE ISO/IEC 19896-1 ,3.7]
1102	3.111
1103	layering
1104	design technique where separate groups of modules are hierarchically organized to have separate
1105	responsibilities such that a group of modules depends on groups of modules below it in the hierarchy
1106	for services, and provides its services to the group of modules above it
1107	3.112
1108	life-cycle definition
1109	definition of the life-cycle model
1110	3.113
1111	life cycle model
1112	description of the stages and their relations to each other that are used in the management of the life-
1113	cycle of a certain object, how the sequence of stages looks like and which high level characteristics the
1114	stages have
1115	Note 1 to entry: See also Figure 1.
1116	[SOURCE: ISO/IEC/IEEE 24765:2010 3.1587 modified, note 1 to entry added]
1117	3.114
1118	methodology
1119	system of principles, procedures and processes applied to IT security evaluations
1120	Editors' Note:

Having in mind the definition of 'evaluation method' is presented the Editors propose to remove this one as too general hence redundant.

Suggest:

The term should be "evaluation methodology".

3.115

module

TOE-module

small architectural unit that **can** be characterized in terms of the properties discussed in TSF internals (ADV_INT)

3.116

monitoring attack

generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents

3.117

non-bypassability

(of the TSF) security architecture property whereby all SFR-related actions are mediated by the TSF

3.118

object

entity in the TOE, that contains or receives information, and upon which subjects perform operations

3.119

observation report

report written by the evaluator requesting a clarification or identifying a problem during the evaluation

3.120

operation

(on an ISO/IEC 15408 component) modification or repetition of a component by assignment, iteration, refinement, or selection

3.121

operation

(on an object) specific type of action performed by a subject on an object

3.122

operation

usage phase of the TOE including normal usage, administration, and maintenance of the TOE after delivery and preparation

Editors' Note:

Propose

operation

<life-cycle> life-cycle phase of the TOE after delivery and preparation that includes normal usage, administration, and maintenance of the TOE

3.123

operational environment

environment in which the TOE is operated, consisting of everything that is outside the TOE boundary

3.124

organizational security policy

OSP

set of security rules, procedures, or guidelines for an organization

Note 1 to entry: A policy **may** pertain to a specific operational environment.

3.125**overall verdict**

statement issued by an evaluator with respect to the result of an evaluation

Note 1 to entry: The statement **can** be expressed as “pass” or “fail”.

3.126**oversight verdict**

statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities

3.127**package**

named set of either security assurance requirements or security functional requirements possibly including an SPD and Security Objectives derived from that SPD

Editors' Note:

The definitions “functional or security assurance package” were contributed by experts, but that definition is circular and have been amended by the Editors. Additionally, this definition should be integrated with the two ie. assurance package and functional one.

3.128**policy**

set of rules, procedures, and guidelines

3.129**potential vulnerability**

suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.

3.130**preparation**

activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation

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

3.131**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 to the customer

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

3.132**Protection Profile configuration****PP-Configuration**

Protection Profile composed of Base Protection Profile(s) and Protection Profile module(s)

3.133**Protection Profile****PP**

implementation-independent statement of security needs for a TOE type

3.134**Protection Profile module****PP-Module**

implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles

- 1216 **3.135**
 1217 **prove**
 1218 <evaluation verb> show correspondence by formal analysis in its mathematical sense
- 1219 Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to
 1220 show correspondence between two TSF representations at a high level of rigour.
- 1221 **3.136**
 1222 **record**
 1223 <evaluation verb> retain a written description of procedures, events, observations, insights, and results
 1224 in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later
 1225 time
- 1226 **3.137**
 1227 **refinement**
 1228 addition of details to a security component
- 1229 **3.138**
 1230 **report**
 1231 <evaluation verb> include evaluation results and supporting material in the evaluation technical report
 1232 or an observation report
- 1233 **3.139**
 1234 **residual vulnerability**
 1235 weakness that **cannot** be exploited in the operational environment for the TOE, but that could be used
 1236 to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational
 1237 environment for the TOE
- 1238 **3.140**
 1239 **role**
 1240 pre-defined set of rules establishing the allowed interactions between a user and the TOE
- 1241 **3.141**
 1242 **secret**
 1243 information that **shall** be known only to authorized users and/or the TSF in order to enforce a specific
 1244 SFP
- 1245 **3.142**
 1246 **secure state**
 1247 state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs
- 1248 **3.143**
 1249 **security attribute**
 1250 property of subjects, users, objects, information, sessions and/or resources that is used in defining the
 1251 SFRs and whose values are used in enforcing the SFRs
- 1252 Note 1 to entry: Users **can** include external IT products.
- 1253 **3.144**
 1254 **security domain**
 1255 environment provided by the TSF for the use by untrusted entities in such a way that the environment
 1256 is isolated and protected from other environments
- 1257 **3.145**
 1258 **security function policy**
 1259 **SFP**
 1260 set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs
- 1261 **3.146**
 1262 **security objective**
 1263 statement of an intent to counter identified threats and/or satisfy identified organization security
 1264 policies and/or assumptions

3.147**security problem****security problem definition****SPD**

statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

Note 1 to entry: This statement consists of a combination of: threats to be countered by the TOE and its operational environment, the OSPs enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.

3.148**security requirement**

requirement, stated in a standardized language, which is meant to contribute to achieving the Security Objectives for a TOE

Note 1 to entry: Security Functional Requirement (SFR) refers to the TOE security function description.

Note 2: to entry: Security Assurance Function (SAR) refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user.

Editors' Note:

The definition of security requirement seems to come from previous CC (i.e V2). In CC v3.1, the SAR are not mapped to any objective. It's not clear that the definition is needed. If it is, then the proposal is as follows:

security requirement

requirement, stated in 15408 standardized language, which is part of a TOE security specification as defined in a specific ST or in a PP

Introduce top-level terms SFR and SAR**security functional requirement****SFR**

requirement, stated in 15408-2 standardized language, which contributes to fulfil the TOE's Security Objectives as defined in a specific ST or in a PP

SAR

requirement, stated in 15408-3 standardized language, which refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user

or

requirement, stated in 15408-3 standardized language, which describes how the developer ensures that the TOE meets the aforementioned SFRs. In particular, a SAR refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user

3.149**Security Target****ST**

implementation-dependent statement of security requirements for a TOE based on a security problem definition

3.150**selection**

specification of one or more items from a list in a component

3.151**selection-based Security Functional Requirement****selection-based SFR**

SFR in a Protection Profile that contributes to a stated aspect of the PP's security problem definition that **is to** be included in a conformant ST if a selection choice identified in the PP indicates that it has an associated selection-based SFR

3.152**semiformal**

expressed in a restricted syntax language with defined semantics

3.1.53**SPD-element**

threat, organizational security policy, or assumption

Editors' Note:

This term has been introduced as a result of using it in the clauses below in order to make the language more easily understood in the main clauses.

3.154**specify**

<evaluation verb> provide specific details about an entity in a rigorous and precise manner

3.155**ST-Module**

text

3.156**ST-Configuration**

text

3.157**strict conformance**

hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST

Note 1 to entry: This relation **can** be paraphrased as "the ST **shall** contain all statements that are in the PP but **may** contain more". Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

3.158**sub-activity**

application of an assurance component of ISO/IEC 15408-3

Note 1 to entry: Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family.

3.159**Sub-TSF**

notion applied in multi-assurance evaluation to denote a portion of the TSF that provides security functionality requiring a different assurance level to the remainder/other portions of the TSF

3.160**subject**

entity in the TOE that performs operations on objects

3.161**target of evaluation****TOE**

set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

1360 **3.162**
 1361 **threat agent**
 1362 entity that **can** exercise adverse actions on assets protected by the TOE

1363 **Editors' Note:**

1364 The terms below have been introduced as a result of the action agreed at editing meeting

1365 **3.163**
 1366 **time to exposure**
 1367 text

1368 **Editors' Note:**

1369 This term is related to attack potential

1370 Contributions in regard to a definition, or proposal to remove it are requested.

1371 If none are received the editors will remove this term.

1372 **3.164**
 1373 **TOE resource**
 1374 anything useable or consumable in the TOE

1375 **3.165**
 1376 **TOE security functionality**
 1377 **TSF**
 1378 combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the
 1379 correct enforcement of the SFRs

1380 **3.166**
 1381 **TOE type**
 1382 set of TOEs that have common characteristics

1383 Note 1 to entry: The TOE type **may** be more explicitly defined in a PP.

1384 **3.167**
 1385 **trace**
 1386 perform an informal correspondence analysis in both directions between two entities with only a
 1387 minimal level of rigour

1388 **3.168**
 1389 **trace**
 1390 <evaluation verb> simple directional relation between two sets of entities, which shows which entities
 1391 in the first set correspond to which entities in the second

1392 **3.169**
 1393 **transfer outside of the TOE**
 1394 TSF-mediated communication of data to entities not under the control of the TSF

1395 **3.170**
 1396 **translation**
 1397 describes the process of describing security requirements in a standardized language.

1398 Note 1 to entry: Use of the term translation in this context is not literal and does not imply that every SFR
 1399 expressed in standardized language **can** also be translated back to the Security Objectives.

1400 **3.171**
 1401 **trusted channel**
 1402 means by which a TSF and another trusted IT product **can** communicate with necessary confidence

1403 Note 1 to entry: Communication typically implies the establishment of identification and authentication of both
 1404 parties. It **may** also entail other properties such as integrity and/or confidentiality preservation as well as
 1405 protection against replay.

3.172**trusted IT product**

IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly

EXAMPLE An IT product that has been separately evaluated.

Editor s' Note:

A trusted IT product has not necessarily been CC evaluated. Since the term "security functional requirements" has a specific meaning in CC, the definition must be reworked. The proposal is the following:

trusted IT product

IT product, other than the TOE, which has its security administratively coordinated with the TOE and which is assumed to enforce its security correctly

EXAMPLE: An IT product that has been separately evaluated. CC evaluation is not mandated.

If no comments are received on this, the editors' proposal will be accepted and presented in the next draft.

3.173**trusted path**

means by which a user and a TSF **can** communicate with the necessary confidence

Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the concept of a user specific session which is integrity-protected.

Note 2 to entry: When the external entity is a trusted IT product, the notion of trusted channel is used instead of trusted path.

Note 3 to entry: Both physical and logical aspects of secure communication **can** be considered as mechanisms for gaining confidence.

3.174**TSF data**

data for the operation of the TOE upon which the enforcement of the SFR relies

3.175**TSF interface****TSFI**

means by which either external entities or subjects within the TOE but outside of the TSF interact with or supply data to the TSF

3.176**TSF self-protection**

security architecture property whereby the TSF **cannot** be corrupted by non-TSF code or entities

3.177**user data**

data that is stored, processed, or transmitted by the TOE but that the TSF does not depend on

Note 1 to entry: User data **may** include any data that does not affect the operation of the TSF. It **may** be associated with external entities, and administrators.

Editors' Note:

The DoC for part 1 agreed to keep the original definition for this term. However, it is a circular definition and cannot remain "as is" because of the current Directives. The Editors highlight this as a defect in the last DoC and ask for further input in regard to this term.

Editors proposes the following definition, which reuses CC v3.1R5 definition

user data

data received or produced by the TOE, which is meaningful to some external entity but which do not affect the operation of the TSF

Note 1 to entry: this definition assumes that any *user data* that has an actual impact on the operation of the TSF should be regarded as *TSF data* instead.

If no comments are received on this, the editors' proposal will be accepted and presented in the next draft

3.178**verdict**

statement issued by an evaluator with respect to evaluator action element, assurance component, or class

Note 1 to entry: The statement **can** be presented as: pass, fail or inconclusive.

Note 2 to entry: Also see overall verdict.

3.179**verify**

<evaluation verb> rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see "confirm". This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.

3.180**vulnerability**

weakness in the TOE that **can** be used to violate the SFRs in some environment

3.181**window of opportunity**

period of time that an attacker has access to the TOE

3.182**work unit**

most granular level of evaluation work

Note 1 to entry: ISO/IEC 18405 defines the evaluation work units for a subset of ISO/IEC 15408-3 security assurance requirements.

3.2 Hierarchy of concepts**Editors' Note:**

Under development by the Editors

Note that ISO have stated that the terms must be presented using a hierarchy of concepts, and not in alphabetical order.

4 Abbreviated terms**Editors' Note:**

Editors have removed abbreviations from the list that are presented in the clause 3 definitions

Editors still need to check all parts of 15408 and 18045 for abbreviations and update this list accordingly.

The following abbreviations are used in the ISO/IEC 15408 series:

API	Application Programming Interface
CAP	Composed Assurance Package
DAC	Discretionary Access Control
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator

1496	EA	Evaluation Activity
1497	EMS	Electromagnetic spectrum
1498	GUI	Graphical User Interface
1499	HSM	Hardware Security Module
1500	IC	Integrated Circuit
1501	IOCTL	Input Output Control
1502	IP	Internet Protocol
1503	IT	Information Technology
1504	MB	Mega Byte
1505	OR	Observation Report
1506	OS	Operating System
1507	PC	Personal Computer
1508	PCI	Peripheral Component Interconnect
1509	PKI	Public Key Infrastructure
1510	RAM	Random Access Memory
1511	RBG	Random Bit Generator
1512	RNG	Random Number Generator
1513	RPC	Remote Procedure Call
1514	SAR	Security Assurance Requirement
1515	SFR	Security Functional Requirement
1516	SPA	Simple Power Analysis
1517	TCP	Transmission Control Protocol
1518	VPN	Virtual Private Network
1519		
1520		

1521 5 Overview

1522 5.1 General

1523 This clause introduces the main concepts of the ISO/IEC 15408 series. It identifies the concept of the
1524 Target of Evaluation (TOE), the target audience of the ISO/IEC 15408 series, and the approach taken to
1525 present the material in The ISO/IEC 15408 series.

1526 5.2 The different parts of ISO/IEC 15408

1527 The ISO/IEC 15408 series is presented as a set of distinct but related parts as identified below. Terms
1528 used in the description of the parts are explained in 3.1.

- 1529 a) **ISO/IEC 15408-1, Introduction, and general model** is the introduction to The ISO/IEC 15408
1530 series. It defines the general concepts and principles of IT security evaluation and presents a
1531 general model of evaluation.
- 1532 b) **ISO/IEC 15408-2, Security functional components** establishes a set of functional components
1533 that serve as standard templates upon which security functional requirements for TOEs are
1534 based. ISO/IEC 15408-2 catalogues the set of security functional components and organizes
1535 them in families and classes.
- 1536 c) **ISO/IEC 15408-3, Security assurance components** establishes a set of assurance components
1537 that serve as standard templates upon which security assurance requirements for TOEs are
1538 based. ISO/IEC 15408-3 catalogues the set of security assurance components and organizes
1539 them into families and classes. ISO/IEC 15408-3 also defines evaluation criteria for PPs, STs and
1540 TOEs.
- 1541 d) **ISO/IEC 15408-4, Framework for the specification of evaluation methods and activities**
1542 provides a standardized framework for the specification of evaluation methods and activities
1543 that **may** be included in PPs, STs and any documents supporting them, to be used by evaluators
1544 in support of evaluations using the model described in the other parts of ISO/IEC 15408. Part 4
1545 is fundamental to ISO/IEC 18045.
- 1546 e) **ISO/IEC 15408-5, Pre-defined packages of security requirements** provides packages of
1547 security assurance and security functional requirements that have been identified as useful in
1548 support of common usage by stakeholders. Examples of provided packages include the
1549 evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

1550 In support of the ISO/IEC 15408 series, other documents have been published. For example, ISO/IEC
1551 18045 provides the baseline methodology for IT security evaluation. The bibliography provides a list of
1552 supportive documents and it is anticipated that other documents will be published, including technical
1553 rationale material and guidance documents.

1554 5.3 Target audience of the ISO/IEC 15408 series

1555 5.3.1 General

1556 There are four main groups with a general interest in evaluation of the security properties of TOEs:
1557 consumers, developers, and evaluators. The criteria presented in ISO/IEC 15408-1 have been
1558 structured to support the needs of all three groups. They are all considered to be the principal users of
1559 the ISO/IEC 15408 series. The three groups **can** benefit from the criteria as explained in the following
1560 sub-clauses.

1561 5.3.2 Risk owners

1562 The ISO/IEC 15408 series is written to ensure that evaluation fulfils the needs of risk-owners as this is
1563 the fundamental purpose and justification for the evaluation process.

Risk owners **can** use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Risk owners **can** also use the evaluation results to compare different TOEs.

The ISO/IEC 15408 series gives risk owners, especially those in consumer groups and communities of interest, an implementation- independent structure, termed the Protection Profile (PP), in which to express their security requirements in an unambiguous manner.

5.3.3 Developers

The ISO/IEC 15408 series is intended to support IT product developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST **may** be based on one or more PPs to show that the ST conforms to the security requirements from consumers as laid down in those PPs.

The ISO/IEC 15408 series **can** then be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

5.3.4 Technical working groups

The ISO/IEC 15408 series is intended to support technical working groups in preparing and developing PPs, PP-Modules, PP-Configurations and supporting documents or guidance. Technical working groups **can** be composed of stakeholders including risk-owners, developers, evaluators, and academics.

5.3.5 Evaluators

The ISO/IEC 15408 series contains criteria to be used by evaluators when forming judgements about the conformance of TOEs, STs, PPs and PP-Configurations to their security requirements. The ISO/IEC 15408 series describes the general set of actions the evaluator is to carry out.

NOTE The ISO/IEC 15408 series does not specify procedures to be followed in carrying out those actions. More information on these procedures **may** be found in 11.3.

5.3.6 Others

While the ISO/IEC 15408 series is oriented towards specification and evaluation of the IT security properties of TOEs, it **may can** also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that **can** benefit from information contained in the ISO/IEC 15408 series are:

- a) system custodians and system security officers responsible for determining and meeting organizational IT security policies and requirements;
- b) auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution (which **may** consist of or contain a TOE);
- c) security architects and designers responsible for the specification of security properties of IT products;
- d) accreditors responsible for accepting an IT solution for use within a particular environment;
- e) sponsors of evaluation responsible for requesting and supporting an evaluation;
- f) evaluation authorities responsible for the management and oversight of IT security evaluation programmes; and
- g) academia who perform research on the topic of IT security.

1607 Table 1 presents, for the four key target audience groupings, how the parts of The ISO/IEC 15408 series
 1608 are of interest.

1609

Table 1— Road map to the “Evaluation criteria for IT security”

	Risk owners	Developers	Technical working group	Evaluators
Part 1	<p>Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Configurations, STs and composition.</p> <p>Shall use for the development of security specifications and security problem definitions for TOEs.</p>	<p>Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Configurations, STs and composition.</p> <p>Shall use for the development of security specifications for TOEs, Packages, PP-Modules and PP-Configurations.</p>	<p>Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Configurations, STs and composition.</p> <p>Shall use for the development of security specifications for Packages, PPs and PP-Configurations.</p>	<p>Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Configurations, STs and composition.</p> <p>Shall use when evaluating PPs, PP-Configurations and STs.</p>
Part 2	<p>Shall use for guidance and reference when formulating statements of security functional components for their risk-environment.</p>	<p>Shall use for reference when interpreting statements of security functional components in PPs, PP-Modules and PP-Configurations</p> <p>Shall use when developing STs</p> <p>May use when formulating security functionality for IT products.</p>	<p>Shall use for when formulating statements of security functional components in PPs and PP-Configurations.</p>	<p>Shall use for reference when evaluating security functional components given in PPs and PP-Configurations or security functional requirements in STs.</p>
Part 3	<p>Shall use for guidance and reference when determining the security assurance required for their risk-environment.</p>	<p>Shall use for reference when interpreting statements of security assurance components in PPs, PP-Modules and PP-Configurations.</p> <p>Shall use when developing STs</p> <p>May use when formulating or improving development processes.</p>	<p>Shall use for when formulating statements of security assurance components in PPs and PP-Configurations.</p>	<p>Shall use for reference when evaluating security functional components given in PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.</p>

	Risk owners	Developers	Technical working group	Evaluators
Part 4	Should use for reference and background information of any evaluation methods derived from ISO/IEC 18045 applied to the evaluation of TOEs used in their risk-environment.	Should use for reference purposes and for guidance in the structure of evaluation methods derived from ISO/IEC 18045.	Shall use for reference purposes and for guidance in the structure of evaluation methods derived from ISO/IEC 18045.	Should use for reference purposes and for guidance in the structure of evaluation methods derived from ISO/IEC 18045. Shall use when formulating specific evaluation methods.
Part 5	Should use for reference in determining the contents of any claimed pre-defined packages of security requirements.	Shall use when developing STs claiming conformance to pre-defined packages of security requirements.	Shall use when developing PPs claiming conformance to pre-defined packages of security requirements.	Shall use for reference when evaluating PPs or STs claiming conformance to pre-defined packages of security requirements.

5.4 The Target of Evaluation (TOE)

5.4.1 General

The ISO/IEC 15408 series is flexible in what to evaluate and is therefore not tied to the boundaries of IT products as commonly understood. Therefore, in the context of evaluation, The ISO/IEC 15408 series uses the term “TOE” (Target of Evaluation).

While there are cases where a TOE consists of a complete IT product, this need not be the case. The TOE **may** be an IT product, a part of an IT product, a set of IT products, a unique technology that **may** never be made into a product, or a combination of these.

As far as the ISO/IEC 15408 series is concerned, the precise relation between the TOE and any IT products is only important in one aspect: the evaluation of a TOE containing only part of an IT product **should not** be misrepresented as the evaluation of the entire IT product.

Further information on the TOE is given in Annex A.

EXAMPLE

Examples of TOEs include devices characterized by few interfaces, reduced attack surface, and a well-known supply chain:

- A network device;
- A software application;
- An operating system;
- A virtualization system;
- An integrated circuit;
- The cryptographic co-processor of an integrated circuit;
- An application for a mobile device;
- A database application excluding the remote client software normally associated with that database application.

TOEs **can** also be more complex, characterized by large interface and/or number of components, multiple manufacturing/integration phases, field upgradeable products such as:

- A Local Area Network including all terminals, servers, network equipment and software;
- A mobile device;
- Gateways and hubs;
- A software application in combination with an operating system;
- A multi-function device, such as a multi-function printer;
- A Hardware Security Modules (HSM).

5.4.2 TOE Boundaries

The concept of a TOE boundary is fundamental to the specification of the Security Target.

In the case where the TOE is either a complete IT product or is a part of an IT product, the Security Target **shall** clearly outline the physical and logical scope of the TOE in relation to the IT product as it is delivered to the customer.

EXAMPLE 1

Both TOE and non-TOE part as physical components **cannot** be included in one chip.

Editors' Note:

Editors wonder if the above example is still true?

Any parts of the IT product that are not within the TOE boundary are outside the scope of the evaluation and **shall be** are called *non-TOE parts of the IT product*.

5.4.3 Different representations of the TOE

In the ISO/IEC 15408 series, a TOE **can** occur in several representations in relationship with the assurance criteria:

NOTE These assurance criteria including testing (ATE) and vulnerability analysis (AVA) which require TOE samples, some design (ADV) requirements require an implementation representation, for instance source code, and lifecycle (ALC) requires the TOE's configuration list.

EXAMPLE

TOE representations for a software TOE:

- a list of files in a configuration management system;
- a single master copy, that has just been compiled;
- the source code for a specific version of an open-source distribution;
- a box containing physical media and a manual, ready to be shipped to a customer;
- a binary file available for secure download;
- an installed and operational version.

TOE representations for a hardware TOE:

- Integrated circuit layout
- Memory mappings
- Wafers
- Modules

All of these are considered to be a TOE and wherever the term "TOE" is used in the ISO/IEC 15408 series, the context determines the representation that is meant.

5.4.4 Different configurations of the TOE

In general, IT products **can** be configured in many ways with different options enabled or disabled. During an evaluation performed in accordance with the ISO/IEC 15408 series, it will be determined whether a TOE meets certain requirements, such flexibility in configuration **can** lead to problems since all possible configurations of the TOE **must** meet the requirements. For these reasons, it is often the case that the guidance part of the TOE constrains the possible configurations of the TOE. That is, the guidance for the TOE **may** be different from the general guidance of the IT product.

EXAMPLE 1

An operating system IT product: This product **can** be configured in many ways including the types of users, number of users, types of external connections allowed/disallowed, options enabled/disabled etc..

In general, if an IT product contains, or is, a TOE then the configuration of the product will need to be much more tightly controlled, since some configuration options **can** lead to a TOE not meeting the requirements.

EXAMPLE 2

- allow all types of external connections,
- the system administrator does not need to be authenticated.

For this reason, there would be an expected difference between the guidance of the general IT product, that **may** allow many configurations, and the guidance of the TOE, that **may** allow only one or only a set of configurations that do not differ in security-relevant ways.

NOTE If the guidance of the TOE allows more than one configuration, these configurations are collectively called “the TOE” and each configuration **must** meet the requirements levied on the TOE.

5.4.5 Operational environment of the TOE

Everything outside the TOE boundary belongs to the TOE operational environment. In the case where the TOE is part of an IT product the IT product **can** have non-TOE parts. Such non-TOE parts are also part of the operational environment of the TOE.

The Security Target **shall** describe assumptions and define Security Objectives for the operational environment describing the security controls which together with the security functionality provided by the TOE itself are necessary to mitigate the threats, and to enforce organizational security policies.

The Security Objectives for the operational environment also **may** be necessary for the TOE security services.

Editors' Note

It is not clear what “security services” means. Is it the TSF or the folks administering the TOE?

EXAMPLE 2

An example of a security objective for the operational environment is organizational key management for TOE cryptographic operation.

EXAMPLE 3

An example of security controls in the operation environment is physical protection of the TOE.

An example of an organizational security policy is a policy determining the intended usage of the TOE.

An example of a security objective for the operational environment is organizational key management for TOE cryptographic operation.

The Security Target **shall** formulate clear requirements for the TOE environment in order to provide the user sufficient information to use the evaluated TOE properly.

5.5 Presentation of material in this document

Editors' Note:

Since 5.1 says "and the approach taken to present the material in the ISO/IEC 15408 series"

The editors have proposed the following text to address that statement.

The general model is presented in 6 which explains the concepts relating to the evaluation of the security functionality of IT products, the definition of the security problem and the specification of security requirements addressing the security problem. Concepts relating to the specification of security requirements, packages, PPs, Modular PPs, that relate to the needs of risk-owners with similar security problems are introduced.

The means of specifying security requirements by completing security components provided in ISO/IEC 15408-3 is explained in 7.

The requirements and recommendations for the core constructs of packages, PPs, Modular PPs and Security Targets, are explained in 8,9,10, and 11.

The requirements and recommendations for evaluation and evaluation results for TOEs, STs, PPs and Modular PPs are found in 12.

Finally, the topic of composing assurance is found in 13.

6 General model

6.1 Background

This clause presents the general concepts used throughout the ISO/IEC 15408 series, including the context in which the concepts are to be used and the approach for applying the concepts. ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4, and ISO/IEC 15408-5, which users of this document are obliged to consult, expand on the use of these concepts, and assume that the approach described is used. Further, for users of the ISO/IEC 15408 series who intend to perform evaluation activities, ISO/IEC 18045 is applicable.

The ISO/IEC 15408 series discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of the ISO/IEC 15408 series. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which the ISO/IEC 15408 series is applicable. This clause assumes that the reader has knowledge of IT security and does not propose to act as a tutorial in this area.

6.2 Assets and security controls

Security is concerned with the protection of assets within the operational environment.

EXAMPLE 1

An example of an asset is the contents of a file or a server.

Examples of operational environments are:

- a data center;
- a computer network connected to the Internet;
- a LAN;
- the every-day environment of a user;
- a general office environment.

Many assets are in the form of information that is stored, processed, and transmitted by IT products to meet requirements laid down by owners of the information. Information owners **may** require that availability, dissemination, and modification of any such information are strictly controlled and that the assets are protected from threats by security controls. Figure 1 illustrates these high-level concepts and relationships.

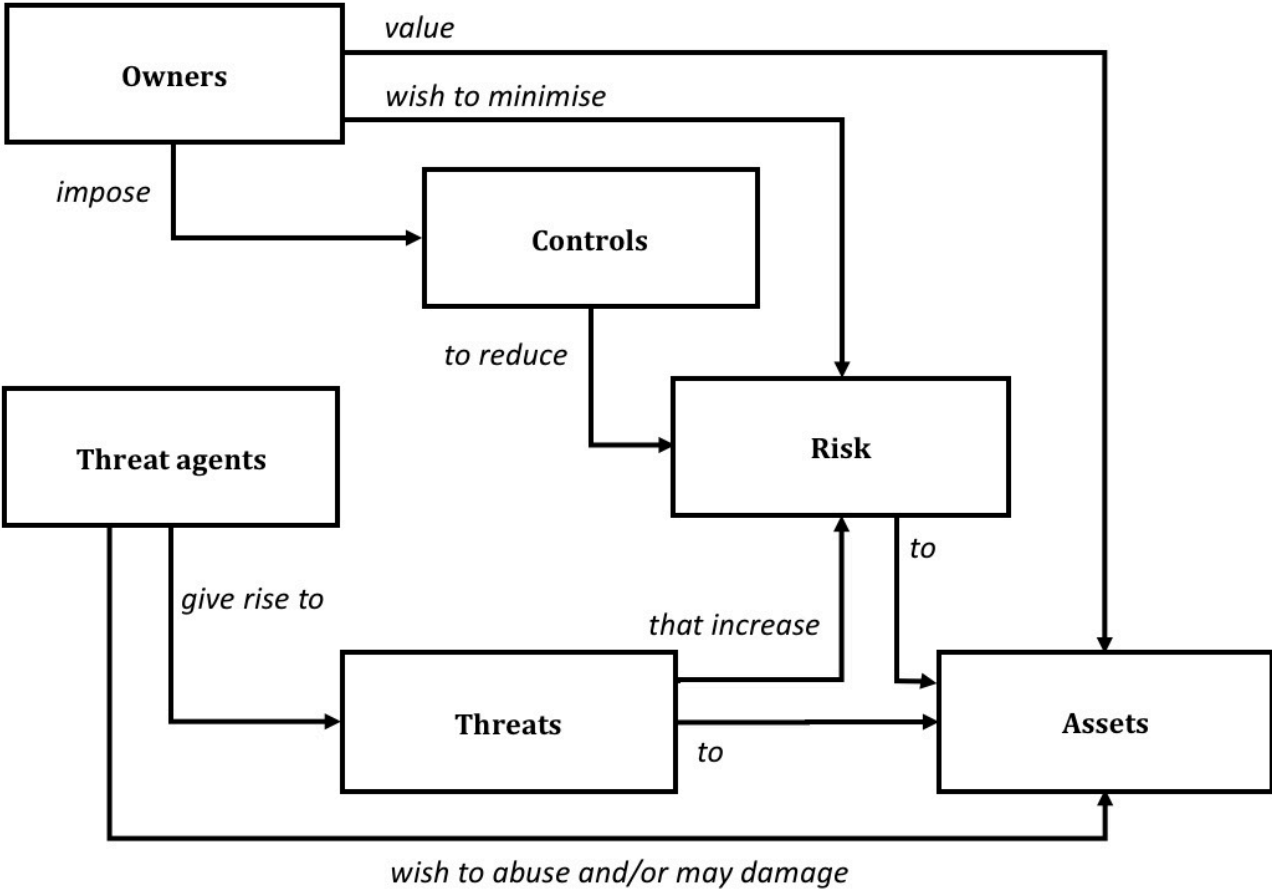


Figure 1 — Security concepts and relationships

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents **may can** also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner.

EXAMPLE
Examples of threat agents include hackers, malicious users, non-malicious users (who sometimes make errors), computer processes and accidents.

The owners of the assets will perceive such threats as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security-specific impairment commonly includes but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realized and the impact on the assets when that threat is realized. Subsequently controls are imposed to reduce the risks to assets. These controls **may can** consist of IT-related controls (such as firewalls and smart cards) and non-IT controls (such as guards and procedures). See also ISO/IEC 27001 and ISO/IEC 27002 for a more general discussion on security controls and how to implement and manage them.

Owners of assets **may can** be held responsible for those assets and therefore **should** be able to defend the decision to accept the risks of exposing the assets to the threats.

Two important elements in defending this decision are being able to demonstrate that:

- the controls are sufficient: if the applied controls do what they claim to do, the threats to the assets are countered;
- the controls are correct: That is, the applied controls do what they claim to do.

ISO/IEC CD1 15408-1: ####(E)

1729

Many owners of assets lack the knowledge, expertise, or resources necessary to judge sufficiency and

1730

correctness of the security controls, and they **may** not wish to rely solely on the assertions of the

1731

developers of the security controls. These consumers **may can** therefore choose to increase their

1732

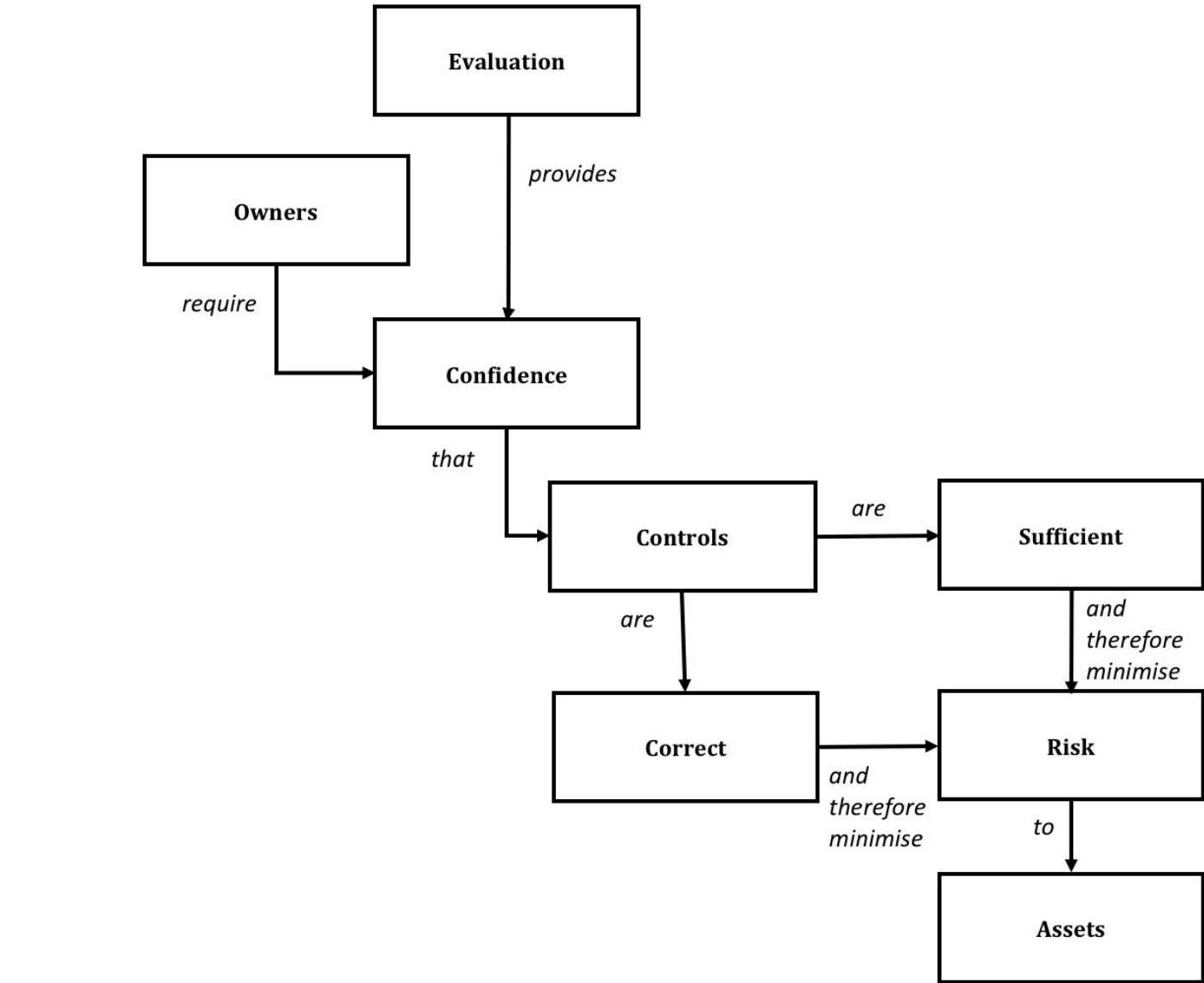
confidence in the sufficiency and correctness of some or all of their security controls by ordering an

1733

evaluation of these security controls.

1734

Figure 2 describes the evaluation concepts and relationships discussed in this section.



1735

1736

In an evaluation, the sufficiency of the security controls is analysed through a construct called the

1737

Security Target. In this subclause a simplified view on this construct is provided: a more detailed and

1738

complete description is found in Annex “A”.

1739

6.3 Core constructs of the ISO/IEC 15408(all parts) paradigm

1740

6.3.1 General

1741

To allow consumer groups and technical communities to express their security needs, and to facilitate

1742

writing PPs and STs, this document provides four constructs: STs, Packages, Protection Profiles (PPs),

1743

and Modular PPs (including the concepts of Base-PPs, PP-Modules and PP-Configurations).

Editors propose the following text to introduce conformance types.

STs, Protection Profiles and Modular PPs require specification of a conformance type in support of the goals of PP and Modular PPs authors.

This document specifies three conformance types; demonstrable, strict, and exact. Conformance types are described in detail in Annex E.

*ISO/IEC 15408 series defines a flexible framework for the **multi-assurance evaluation** of IT products using predefined EALs from ISO/IEC 15408-5 or well-formed assurance packages of ISO/IEC 15408-3 components, which allows claiming a global assurance level for the entire TOE, and possibly multiple different assurance levels for different parts of the TOE.*

6.3.2 Security Target

Editors' Note:

This sub-clause has been renamed to better match the content and to allow including "Security Target" in the titles of the main body (not only in Annex A)

6.3.2.1 General

In this subclause a simplified view of the Security Target construct is provided: a more detailed and complete description is found in Annex A.

Core requirements for STs are found in clause 11. ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs undergoing evaluation.

The Security Target (ST) is a key document that begins with describing the assets and the threats to those assets. The Security Target then describes the security controls (in the form of Security Objectives) and demonstrates that these security controls are sufficient to counter these threats: if the security controls do what they claim to do, the threats are countered.

The Security Target then divides these security controls in two groups:

- a) the Security Objectives for the TOE: these describe the security control(s) for which correctness will be determined in the evaluation;
- b) the Security Objectives for the operational environment: these describe the security controls for which correctness will not be determined in the evaluation.

The reasons for this division are:

- The ISO/IEC 15408 series is only suitable for assessing the correctness of IT security controls. Therefore, the non-IT security controls are always in the operational environment.

EXAMPLE Non-IT security controls include human fences, security guards, procedures.

- Assessing the correctness of security controls costs time and money, possibly making it infeasible to assess the correctness of all IT security controls.

- The correctness of some IT security controls **may** already have been assessed in another evaluation. It is therefore not cost-effective to assess this correctness again.

For the TOE (the IT security controls whose correctness will be assessed during the evaluation), the Security Target requires a further detailing of the Security Objectives for the TOE in Security Functional Requirements (SFRs). These SFRs are formulated in a standardized language (described in ISO/IEC 15408-2) to ensure exactness and facilitate comparability.

In summary, the Security Target demonstrates that:

- The SFRs meet the Security Objectives for the TOE;
- The Security Objectives for the TOE and the Security Objectives for the operational environment counter the threats;

- And therefore, the SFRs and the Security Objectives for the operational environment counter the threats.

From this it follows that a correct TOE (i.e. A TOE that meets the SFRs) in combination with a correct operational environment (i.e. one that meets the Security Objectives for the operational environment) will counter the threats. In the next two subclauses correctness of the TOE and correctness of the operational environment are discussed separately.

In some cases, defining a Security Target that takes an alternative approach to specifying the SFR's is appropriate these STs are known as "Direct Rationale" STs and are explained in the clauses below.

A Security Target **may** be defined as standalone document for a specific TOE or **may** comply with one or more Protection Profile(s) and thereby reuse and specialize their generic definitions to the specific TOE. In the second case, the ST must meet the conformance conditions given in the PPs. The PP constructs and the related concepts of Modular PPs are introduced in 9 and 10.

6.3.2.2 Correctness of the TOE

A TOE **may can** be incorrectly designed and implemented and **may can** therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers **may** be able to damage and/or abuse the assets.

These vulnerabilities **may can** arise from poor design, accidental errors made during development, intentional addition of malicious code, ~~poor testing~~, poor configuration management etc.

Editors' Note:

Poor testing has been removed since is a bad example. Poor testing may neglect to discover vulnerabilities but cannot introduce them.

Poor testing has been replaced by "poor configuration management", since it is more likely to lead to faulty products (compilation of the wrong codebase, mislabeling of open samples leading to releasing vulnerable products, etc.)

Comments are solicited only in the case that there is disagreement on this change.

To determine the correctness of the TOE, various activities ~~can~~ **may** be performed such as:

- testing the TOE;
- examining various design representations of the TOE;
- examining the physical security of the development environment of the TOE.

The Security Target provides a structured description of these activities to determine correctness in the form of Security Assurance Requirements (SARs). These SARs are formulated in a standardized language (described in ISO/IEC 15408-3) to ensure exactness and facilitate comparability.

If the SARs are met, there exists assurance in the correctness of the TOE and the TOE is therefore less likely to contain vulnerabilities that **can** be exploited by attackers. The amount of assurance that exists in the correctness of the TOE is determined by the SARs themselves: a few "weak" SARs will lead to a little assurance, a lot of "strong" SARs will lead to a lot of assurance.

*A Security Target **shall** claim a global set of SARs for the entire TOE and may additionally structure the TOE in various modules and claim a specific set of SARs for each of the modules. The second case can be achieved through the conformance to two or more PPs with different Assurance Levels and/or to multi-assurance PP-Configurations.*

NOTE When multi-assurance is relevant although there is no PP-Configuration to rely on or the pre-defined PP-Configurations do not fully cover the TOE's security problem, the ST writer can take any of the two following paths:

- Define a PP-Configuration that is fully appropriate for the ST. This is not a limitation and does not represent additional effort since an ST is a special type of PP, where all the SFRs are instantiated and the TSS provides the relationship with the actual implementation: If an ST evaluates successfully against ASE requirements then the same ST evaluates successfully against APE requirements.

— Associate the ST specific SFRs to the ST's global Assurance Level (AL), which by definition must be identical or lower than all the global ALs of the PPs/PP-Configurations that are used.

6.3.2.3 Correctness of the operational environment

The operational environment **may** **could** also be incorrectly specified or implemented and **may** therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers' **may** **could** damage and/or abuse the assets.

However, in the ISO/IEC 15408 series, no assurance is obtained regarding the correctness of the operational environment. Or, in other words, the operational environment is not evaluated.

As far as the evaluation is concerned, the operational environment is assumed to be a 100% correct instantiation of the Security Objectives for the operational environment.

This does not preclude a consumer of the TOE from using other methods to determine the correctness of his operational environment.

EXAMPLE

If, for an Operating System TOE, the Security Objectives for the operational environment state "The operational environment **shall** ensure that entities from an untrusted network **can** only access the TOE using the FTP protocol", the consumer could select an evaluated firewall, and configure it to only allow FTP access to the TOE;
NOTE The Internet is an example of an untrusted network

If the Security Objectives for the operational environment state "The operational environment **shall** ensure that all administrative personnel will not behave maliciously", the consumer could adapt his contracts with administrative personnel to include punitive sanctions for malicious behaviour, but this determination is not part of an evaluation using the ISO/IEC 15408 series as a basis.

6.3.3 Communicating security requirements

6.3.3.1 General

Often sets of security requirements are commonly used, ISO/IEC 15408(all parts) also provides a mechanism for identifying sets of security requirements addressing particular TOE types and that share similar security problems. This document introduces three constructs for attaining this, Packages, Protection Profiles and Modular PPs. These are introduced below.

6.3.3.2 Packages

Packages describe a set of related security requirements that are frequently used together. Packages are often designed to be re-used bringing some comparability between those STs that use them.

Security functional packages **may** be used to define security protocols, or other security functional concepts.

Security assurance packages **may** be used to define the conditions and processes such as specification, design, development, testing and delivery under which the TOE is developed and configured

Core requirements for packages are found in 8, Annex C provides additional information about packages and ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs and PPs undergoing evaluation that **may** use packages. ISO/IEC 15408-5 provides some pre-defined packages that **may** be used by PP and ST authors.

6.3.3.3 Protection Profiles (PPs)

Protection Profiles (PPs) describe a TOE type and the security assurance requirements (SAR), security functional requirements (SFRs) expected to be provided for that type of TOE.

PPs based on other PPs **may** be used to further refine a TOE type.

PPs **may** take either a standard or a Direct Rationale approach.

Core requirements for PPs are found in 9, Annex B provides additional information about PPs and ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for PPs undergoing evaluation.

6.3.3.4 Modular PPs

Modular PPs build upon the concept of a PP; introducing the notion of a Base-PP which **may** add one or more PP-Modules. PP-Modules **may** be used to refine the generic TOE type of a Base-PP, or to add security requirements for particular technologies which **may** be optionally associated with the TOE type defined in the Base-PP. Further, PP-Configurations describe which Base-PPs and PP-Modules **may** be legitimately combined whilst maintaining the security assurance specified in the Base-PP. This concept is described in more detail in 10 and 10.4 and further guidance provided in Annex B.

Editors' Note:

Reviewers are invited to consider the next paragraph. Can selection-based SFRs be used in regular PPs as well as modular PPs?

The Editors solicit comment on this issue.

The concept of selection-based SFRs is introduced which expands on the basic use of the selection operation.

Core requirements for Modular PPs are found in 10, Annex B provides additional information about Modular PPs and ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for Modular PPs undergoing evaluation.

Editors' Note:

TO DO: WD2 DE/SF21: Add examples for each construct.

7 Tailoring security requirements

7.1 General

Security Targets specify the security requirements applicable to a TOE. Security functional requirements, and security assurance requirements **may** be drawn from security components which are a template for security requirements. The process of deriving a security requirement from a security component involves tailoring the components for the specific ST and is known as "completion".

7.2 Operations

Functional and assurance components **may** be used exactly as defined in ISO/IEC 15408-2 and ISO/IEC 15408-3, or they **may** be tailored through the use of permitted operations.

NOTE It is important to understand that a PP is intended to describe a TOE type whereas an ST describes a specific TOE. A PP **can** either be used as the basis for another PP, or as a basis for an ST.

When using operations, the PP/ST author **should** be careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components. The operations are described in more detail below.

Editors' Note.

Editors suggest the following correction to the above paragraph.

"The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all security requirements."

If no comments are received on this, the editors' proposal will be accepted and presented in the next draft.

The ISO/IEC 15408-2 annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions **shall** be followed unless the PP/ST author justifies the deviation:

- a) "None" is only available as a choice for the completion of a selection if explicitly provided.

The lists provided for the completion of selections **shall** be non-empty. If a "None" option is chosen, no additional selection options **may** be chosen. If "None" is not given as an option in a selection, it is permissible to combine the choices in a selection with "and"s and "or"s, unless the selection explicitly states "choose one of".

Selection operations **may** be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration **should** not overlap the subject of the other iterated selection, since they are intended to be exclusive

- b) For the completion of assignments, the ISO/IEC 15408-2 annexes **shall** be consulted in order to determine when "None" would be a valid completion.

7.2.1 The iteration operation

The iteration operation **may** be performed on every component. The PP/ST author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component **shall** be different from all other iterations of that component, which is realized by completing assignments and selections in a different way, or by applying refinements to it in a different way.

Different iterations **shall** be uniquely identified to allow clear rationales and tracings to and from these requirements. Iteration identifiers **should** be meaningful to readers.

EXAMPLE

FCS_COP.1(AES data encryption/decryption) and FCS.COP.1(Signature generation) is preferable to FCS.COP.1(a) and FCS.COP.1(b)

NOTE Sometimes an iteration operation **can** be used with components where it is also possible to perform an assignment operation with a range or list of values instead of iterating them. In that case, the author **can** select the most appropriate alternative, considering if there is a necessity of providing a whole rationale for the range of values or if it is necessary to have a separate one for each of them. The author **should** also keep in mind if individual traces are required for those values.

7.2.2 The assignment operation

An assignment operation occurs where a given component contains an element with a parameter that **may** be set by the PP/ST author. The parameter **may** be an unrestricted variable, or a rule that narrows the variable to a specific range of values.

Whenever an element in a PP contains an assignment, a PP author **shall** do one of four things:

- a) leave the assignment uncompleted;

EXAMPLE 1

The PP author could include FIA_AFL.1.2 in the PP.

"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall** [assignment: list of actions]."

In this case, the ST author could complete FIA_AFL.1.2 thus:

"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall** prevent that external entity from binding to any subject in the future."

- b) complete the assignment;

EXAMPLE 2

the PP author could include FIA_AFL.1.2 “When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall** prevent that external entity from binding to any subject in the future.”

- c) narrow the assignment to further limit the range of values that is allowed;

EXAMPLE 3

The PP author could include FIA_AFL.1.1 in the PP

“The TSF **shall** detect when [assignment: positive integer between 4 and 9] unsuccessful authentication attempts occur ...”

In this case, the ST author could complete FIA_AFL.1.1 thus:

“The TSF **shall** detect when 7 unsuccessful authentication attempts occur ...”

- d) transform the assignment to a selection, thereby narrowing the assignment.

EXAMPLE 4

The PP author could include FIA_AFL.1.2 in the PP

“When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall** [selection: **prevent that user from binding to any subject in the future, notify the administrator**].”

In this case, the ST author could complete FIA_AFL.1.2 thus:

“When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall** prevent that user from binding to any subject in the future.”

Whenever an element in an ST contains an assignment, an ST author **shall** complete that assignment, as indicated in b) above. Options a), c) and d) are not allowed for STs.

The values chosen in options b), and c) **shall** conform to the indicated type required by the assignment.

When an assignment is to be completed with a set, a PP author **should** provide a description of the set from which the elements of the set **can** be derived as long as it is clear which subjects are meant.

EXAMPLE 5

Where the set is “subjects”

- all subjects,
- all subjects of type X,
- all subjects except subject a.

7.2.3 The selection operation

7.2.3.1 General

The selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

Whenever an element in a PP contains a selection, the PP author **may** do one of three things:

- a) leave the selection uncompleted,
- b) complete the selection by choosing one or more items,
- c) restrict the selection by removing some of the choices but leaving two or more.

Whenever an element in a PP contains a selection, an ST author **shall** complete that selection, as indicated in b) above. Options a) and c) are not allowed for STs.

The item or items chosen in b) and c) **shall** be taken from the items provided in the selection.

7.2.4 The refinement operation

The refinement operation **can** **may** be performed on every requirement. The PP/ST author performs a refinement by altering that requirement.

The first rule for a refinement is that a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP or ST (i.e. a refined requirement **shall** be “stricter” than the original requirement). If a refinement does not meet this rule, the resulting refined requirement is considered to be an extended requirement and **shall** be treated as such in accordance with 7.3.

The only exception to this rule is that a PP/ST author **may** refine a SFR to apply to some but not all subjects, objects, operations, security attributes and/or external entities. However, this exception does not apply to refining SFRs that are taken from PPs to which conformance is being claimed; these SFRs **shall** not be refined to apply to fewer subjects, objects, operations, security attributes and/or external entities than the SFR in the originating PP.

The second rule for a refinement is that the refinement **shall** be related to the original component.

NOTE 1 A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar, or to make it more understandable to the reader. This change is not allowed to modify the meaning of the requirement in any way.

NOTE 2 A series of refined iteration operations **can** be used to cover all of the subjects, objects, operations, security attributes and/or external entities, but where each individual refinement does not.

7.3 Dependencies between components

Dependencies **may** exist between components. Dependencies arise when a component is not self-sufficient and relies upon the presence of another component to provide security functionality or assurance.

The functional components in ISO/IEC 15408-2 typically have dependencies on other functional components. Some of the assurance components in ISO/IEC 15408-3 also have dependencies, which in turn, **may** have dependencies on other ISO/IEC 15408-3 components.

ISO/IEC 15408-2 dependencies on ISO/IEC 15408-3 components **may** also be defined. However, this does not preclude extended functional components having dependencies on assurance components or vice versa.

Component dependency descriptions are determined by consulting the component definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, or the extended components definition. In order to ensure completeness of the TOE security requirements, dependencies **should** be satisfied when requirements based on components with dependencies are incorporated into PPs and STs. Dependencies **should** also be considered when constructing packages.

In other words: if component A has a dependency on component B, this means that whenever a PP or ST contains a security requirement based on component A, the PP or ST **shall** also contain one of:

- a) a security requirement based on component B, or
- b) a security requirement based on a component that is hierarchically higher than B, or
- c) a justification why the PP/ST does not contain a security requirement based on component B.

In cases a) and b), when a security requirement is included because of a dependency, it **may** be necessary to complete operations (assignment, iteration, refinement, selection) on that security requirement in a particular manner to make sure that it actually satisfies the dependency.

In case c), the justification that a security requirement is not included **should** address either:

- why the dependency is not necessary or useful, or
- that the dependency has been addressed by the operational environment of the TOE, in which case the justification **should** describe how the Security Objectives for the operational environment address this dependency, or
- that the dependency has been addressed by the other SFRs in some other manner (extended SFRs, combinations of SFRs etc.).

7.4 Extended components

In ISO/IEC 15408, requirements **shall** be based on components from ISO/IEC 15408-2 or ISO/IEC 15408-3 with three exceptions:

- a) there are Security Objectives for the TOE that **cannot** be translated to SFRs,
- b) there are third party requirements that **cannot** be translated to SARs,

EXAMPLE

Laws and/or regulation regarding the evaluation of cryptography.

- c) a security objective **can** be translated to SFRs, but only with great difficulty and/or complexity based on components in ISO/IEC 15408-2 and/or ISO/IEC 15408-3.

In these cases, the PP/ST author is required to define new components called extended components. A precisely defined extended component is needed to provide context and meaning to the extended SFRs and SARs based on that component.

After the new components have been defined correctly, the PP/ST author **can** then base one or more SFRs or SARs on these newly defined extended components and use them in the same way as the other SFRs and SARs. From this point on, there is no further distinction between SFRs and SARs drawn from the ISO/IEC 15408 series and SFRs and SARs based on extended components.

Refer to ISO/IEC 15408-3:20XX, Extended components definition (APE_ECD) and Extended components definition (ASE_ECD) for further requirements on extended components. Further information on extended components is given in A.4.5 and in D.4.

8 Packages

8.1 Package types

A package is a named set of security components or security requirements. A package **shall** be either:

- a functional package, containing functional components or requirements, but no assurance components or requirements, or
- an assurance package, containing assurance components or requirements, but no functional components or requirements.

Mixed packages containing both functional and assurance components or requirements **shall not** be specified.

Further information on packages is given in Annex C.

8.1.1 Assurance packages

An assurance package contains a set of assurance components or requirements that **may** be drawn from ISO/IEC 15408-3, **may** be extended assurance requirements, or that **may** be some combination of both.

EXAMPLE

The evaluation assurance levels (EALs) that are defined in ISO/IEC 15408-5 are comprised of SARs drawn from ISO/IEC 15408-3.

Editors' Note:

Why don't we define the structure for assurance packages as we do in the next sub clause?

The Editors propose that we do so and request contribution of text for the structure of assurance packages.

8.1.2 Functional packages

A functional package contains a set of functional components or requirements that **may** be drawn from ISO/IEC 15408-2, or **may** be extended functional components or requirements or some combination of both.

A functional package **may** include a security problem definition (SPD) and Security Objectives derived from that SPD.

At a minimum, a functional package **shall** consist of an identifier, an overview, a conformance claim, and one or more functional components or requirements.

A functional package **may** also include SPD-elements which describe the security problem addressed by the functional package, as well as the Security Objectives derived from them.

NOTE When a Direct Rationale approach is used Security Objectives for the TOE are not included.

A functional package adheres to the following structure:

- a) The functional package identification **shall** be included giving a unique name, short name, version, date, sponsor, and the ISO/IEC 15408 edition;
- b) A functional package overview **shall** be included giving a narrative description of the security functionality;
- c) A functional package conformance claim **shall** be included giving the conformance claim to ISO/IEC 15408-2 and ISO/IEC 15408-3.
- d) The functional package conformance claim **may** include dependencies to other packages;
- e) A functional package SPD **may** be included giving the SPD-elements;
- f) If the package defines an SPD then the functional package Security Objectives **shall** be given. The objectives include the Security Objectives for the TOE and the operational environment, and the Security Objectives rationale;
- g) The functional package functional components or requirements **shall** be included specifying one or more functional components or requirements and **shall** also include an SFR rationale if the package includes any Security Objectives for the TOE.

8.2 Using packages

8.2.1 General

A package **may** be defined by any party and is intended to be re-usable. To this goal, it **should** contain requirements that are useful and effective in combination. Packages **may** be used in the construction of larger packages, PPs, PP-Modules and STs.

NOTE 1 Although no separate criteria are given in the ISO/IEC 15408 series for evaluating packages, once such packages are included in an PP, PP-Module or ST they will be evaluated using the ASE, APE, or ACE criteria.

NOTE 2 ISO/IEC 15408-5 contains commonly used packages, such as Evaluation Assurance Levels (EAL) that have been pre-defined and **can** be used by PP/ST authors.

8.2.2 Assurance packages

Assurance packages **may** be used within PPs and STs.

NOTE PP-Modules do not specify assurance packages.

8.2.3 Functional packages

Functional packages **may** be used within PPs, PP-Modules and STs as a means to structure security functionality into building blocks.

Editors' Note:

Since WD2 US/NIAP 76 removed the notion of mandatory and optional functional packages, the editor has also modified the paragraphs and example below to match.

Functional packages **may** have dependencies on other functional packages. Such dependencies **shall** be documented in the functional package and **may** also be documented in a PP, PP-Module or ST.

EXAMPLE

If a PP contains packages A, B, C and D, and if the following holds: Functional package A is included; functional package C depends on functional package B; and functional package D has no dependencies, then an ST **can** claim conformance to the PP in the following cases:

- the ST only uses functional package A from the PP
- the ST uses functional packages A and B
- the ST uses functional packages A, B and C
- the ST uses functional packages A and D
- the ST uses functional packages A, B, C, and D

The following combinations would not be allowed:

- the ST uses functional packages A and C
since functional package C has a dependency on functional package B, which **must** be included if functional package C is claimed.

2091 Where two or more packages are related to each other, they **may** be presented as part of a package
2092 family, see C.2.

2093

2094 9 Protection Profiles

2095 9.1 General

2096 A PP is intended to describe a general TOE type. Therefore, a PP **may** be used:

- 2097 — as a template for many different STs to be used in different TOE evaluations;
- 2098 — as a template for other PPs in order to further refine the TOE type.

2099 NOTE A Base-PP is a PP used in the modular PP concept described in 10. The requirements of 9 also apply to
2100 Base-PPs.

2101 **Editors' note**

2102 **Editors added the above note to aid in clarification of applicability of 8.3**

2103 A detailed description of PPs is given in Annex B.

EXAMPLE

A TOE type could be "Firewall";

A refined TOE type could be "Stateful inspection firewalls";

A specific TOE related to that TOE type could be the "MinuteGap Firewall v18.5".

2104 A PP describes the general requirements for a TOE type, and is therefore typically sponsored by:

- 2105 — A technical user community seeking to come to a consensus on the requirements for a given
2106 TOE type;
- 2107 — A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum
2108 baseline for that type of TOE;
- 2109 — An organization, such as a government or large corporation, specifying its security
2110 requirements as part of its acquisition process.

2111 NOTE An ST describes requirements for a specific TOE and is typically sponsored by the developer of that
2112 TOE.

2113 9.2 General conformance claims and conformance statements made by PPs

2114 The conformance claims of PPs:

- 2115 a) **shall** state the **edition of ISO/IEC 15408** to which the PP claims conformance;
- 2116 b) **shall** describe the conformance to ISO/IEC 15408-2 (security functional requirements) as
2117 either:
 - 2118 — **ISO/IEC 15408-2 conformant** - A PP is ISO/IEC 15408-2 conformant if all SFRs in that PP
2119 are based only upon functional components in the ISO/IEC 15408-2; or
 - 2120 — **ISO/IEC 15408-2 extended** - A PP is ISO/IEC 15408-2 extended if at least one SFR in that
2121 PP is not based upon functional components in ISO/IEC 15408-2;
- 2122 c) **shall** describe the conformance to ISO/IEC 15408-3 as either:
 - 2123 — **ISO/IEC 15408-3 conformant** - A PP is ISO/IEC 15408-3 conformant if all SARs in that PP
2124 are based only upon assurance components in ISO/IEC 15408-3; or
 - 2125 — **ISO/IEC 15408-3 extended** - A PP is ISO/IEC 15408-3 extended if at least one SAR in that
2126 PP is not based upon assurance components in ISO/IEC 15408-3;
- 2127 d) if evaluation methods and evaluation activities are included in the PP, the conformance claim
2128 **shall** describe the conformance to ISO/IEC 15408-4 as:

- **ISO/IEC 15408-4 conformant** - A PP is ISO/IEC 15408-4 conformant if evaluation methods and activities are supplied in the PP are conformant with the framework described in ISO/IEC 15408-4;

Editors' Note:

See WD2 US/NIAP26 ^

Editors request comments from other NBs in regard to IF evaluation methods and activities may be included in a PP

- e) **may** include a package conformance claim. More than one package **may** be claimed in a PP.

If a package claim is made, it **shall** consist of one of the following statements for each package claim:

- **Package name Conformant** - A PP is conformant to a package if:

- For functional packages, all constituent parts (SPD, Security Objectives, and SFRs) of the functional package are present in the corresponding parts of the PP without modification.

- For assurance packages, the SARs of that PP are identical to the SARs in the assurance package.

- **Package name Augmented** - A PP claims an augmentation of a package if:

- For functional packages, all constituent parts (SPD, Security Objectives, and SFRs) of that PP contain all constituent parts given in the functional package but shall have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package.

- For assurance packages, the SARs of that PP contain all SARs in the assurance package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package;

- f) **may** also include a conformance claim with respect to other PPs:

- **PP Conformant** - A PP meets other specific PP(s);

- g) **shall** provide a Conformance Statement: This statement describes the manner in which other PPs, PP-Modules or STs shall conform to this PP: The conformance statement **shall** be one of:

- **Exact conformance**: If the PP states that exact conformance is required, the PP/ST shall conform to the PP in an exact manner;

- **Strict conformance**: If the PP states that strict conformance is required, the PP/ST shall conform to the PP in either an exact or a strict manner;

- **Demonstrable conformance**: If the PP states that demonstrable conformance is required, the PP/ST shall conform to the PP in either an exact, strict, or demonstrable manner.

NOTE 1 Restating this in other words, a PP/ST is only allowed to conform to a PP in a demonstrable manner if the PP explicitly allows this.

NOTE 2 A set **can** include the null set.

NOTE 3 Either an PP/ST conforms to a PP or it does not. The ISO/IEC 15408 series does not recognize "partial" conformance. It is therefore the responsibility of the PP author to ensure the PP is not overly onerous, prohibiting PP/ST authors from claiming conformance to the PP.

For more information on the conformance statements and claims for PPs, see [Annex B](#).

9.2.1 Security problem definition:

The conformance rationale in the PP/ST **shall** demonstrate that the security problem definition in the PP/ST is equivalent or more restrictive than the security problem definition in the PP. This means that:

— all TOEs that meet the security problem definition in the PP/ST also meet the security problem definition in the PP;

— all operational environments that meet the security problem definition in the PP also meet the security problem definition in the PP/ST.

9.2.2 Security objectives:

The conformance rationale in the PP/ST **shall** demonstrate that the Security Objectives in the PP/ST are equivalent or more restrictive than the Security Objectives in the PP. This means that:

— all TOEs that meet the Security Objectives for the TOE in the PP/ST also meet the Security Objectives for the TOE in the PP;

— all operational environments that meet the Security Objectives for the operational environment in the PP also meet the Security Objectives for the operational environment in the PP/ST.

9.3 Additional requirements for PPs with an exact conformance statement

9.3.1 General

Exact conformance is used to allow a Protection Profile (PP) author to control what an ST can claim conformance to with respect to the PP that they have written. It is used in cases where the PP author requires that STs which claim conformance to the PP do not include additional requirements that have not been considered by the PP author.

A PP with exact conformance type **cannot shall not** build upon PPs with strict or demonstrable conformance type.

NOTE 1: Once a PP has been given exact conformance type, then it will never be possible to use them to build PPs with a different conformance claim. Additionally, it is impossible to claim conformance to both a strict conformance PP and an exact conformance PP, since it would mean adding requirements on top of the exact conformance PP, which explicitly prohibits this operation.

NOTE 2: In a given document D (ST or PP):

— ctype (D) (conformance type, also called conformance statement, the type of conformance that other ST/PPs can claim wrt D): exact, strict, demonstrable

— cclaim (D) (conformance claim wrt a set of PPs): [PPi -> exact, strict, demonstrable]

— cclaim(D,PPi) == exact & ctype(PPi) != exact then FAIL

— cclaim(D,PPi) == (strict or demonstrable) & ctype(PPi) == exact then FAIL

— etc.

In the “simple” case where an ST claims exact conformance to a PP, there is no ambiguity whether the ST is exactly conformant or not because the correspondence between the SPD, Objectives, SFRs, and SARs can be demonstrated during evaluation without the need to seek PP author input.

However, other cases are allowed where multiple sets of SPD-elements, Objectives, and SFRs can be combined, these cases require mechanisms that preserve the ability of the PP/PP-Module authors to control a conformance claim against their PP or PP-Module. These mechanisms are described in the following subclauses.

EXAMPLE

A complex case might be if a PP-Module wishes to use a PP as its Base-PP, or if an ST claims conformance to two PPs.

NOTE 3 If a PP requires exact conformance, then only those SFRs and SARs specified by that PP are allowed in the conformant PP/ST.

9.3.2 Conformance claims and statements for PPs in the exact conformance case

If a PP requires exact conformance in its conformance statement then

- a) the PP **shall** state which other PPs are allowed to be combined with that PP, specifying which, if any, additional PPs are allowed to be claimed in conjunction with the PP by an ST;
- b) **shall** include an “allowed with” list specifying the set of:
 - PPs and packages that **may** be used with the PP;
 - PP-Modules that **may** use this PP as a Base-PP in a PP-Configuration; and
 - other PPs that **may** claim conformance to the PP.
- c) all the additional PPs to which an ST **may** claim exact conformance **shall** also have an exact conformance requirement; and
- d) all PPs to which an ST is claiming exact conformance **shall** be identified by as being “allowed with” by all other PPs in their conformance statement.

9.4 Additional requirements for PPs common to strict and demonstrable conformance**9.4.1 Conformance claims and statements in the strict and demonstrable conformance cases****9.4.1.1 General**

If an PP/ST claims either strict or demonstrable conformance to multiple PPs, it **shall** conform to each PP in the manner stated by that PP; that is, either strictly or demonstrably. This means that the PP/ST **may** conform strictly to some PPs and demonstrably to other PPs.

An PP/ST conforms to a PP if the PP/ST is equivalent or more restrictive than this PP, that is, if:

- all TOEs that meet the PP/ST also meet the PP, and
- all operational environments that meet the PP also meet the PP/ST.

In other words, the PP/ST **shall** levy the same or more, requirements on the TOE and the same or less conditions on the operational environment of the TOE.

This general statement holds for the different constructs of the PP/ST, namely the Security Problem Definition, the Security Objectives for the TOE, the Security Objectives for the Environment, and the security functional and security assurance requirements.

9.4.2 Package claims

*A PP of demonstrable or strict conformance **shall** define its Assurance Level (AL), i.e. the set of SARs that applies to the entire TOE.*

- *If the PP AL is an (augmented) pre-defined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference, then the same name should be used.*
- *Otherwise a new name **shall** be provided for the PP AL.*

9.4.3 Additional requirements specific to the strict conformance case**9.4.3.1 Requirements for the SPD in the strict conformance case:**

The PP/ST **shall** contain the security problem definition of the PP and **may** specify additional threats and OSPs; it **shall** contain all assumptions as defined in the PP, with two possible exceptions as explained in the next two bullets;

- an assumption (or a part of an assumption) specified in the PP **may** be omitted from the PP/ST if all Security Objectives for the operational environment defined in the PP addressing this assumption (or this part of an assumption) are replaced by Security Objectives for the TOE in the PP/ST;

- a new assumption **may** be added in the PP/ST to the set of assumptions defined in the PP, if this new assumption does not mitigate a threat (or part of a threat) meant to be addressed by Security Objectives for the TOE in the PP and if this assumption doesn't fulfil an OSP (or a part of an OSP) meant to be addressed by Security Objectives for the TOE in the PP;

9.4.3.2 Requirements for the Security Objectives in the strict conformance case

The PP/ST:

- **shall** contain all Security Objectives for the TOE of the PP but **may** specify additional Security Objectives for the TOE;
- **shall** contain all Security Objectives for the operational environment as defined in the PP with two exceptions as explained in the next two bullet points;
- **may** specify that certain Security Objectives for the operational environment in the PP are Security Objectives for the TOE in the PP/ST. This is called re-assigning a security objective. If a security objective is re-assigned to the Security Objectives for the TOE the Security Objectives justification has to make clear which assumption or part of the assumption **may** not be necessary anymore;
- **may** specify additional Security Objectives for the operational environment, if these new objectives do not mitigate a threat (or part of a threat) meant to be addressed by Security Objectives of the TOE in the PP and if these new objectives do not fulfil an OSP (or a part of an OSP) meant to be addressed by Security Objectives of the TOE in the PP.

9.4.3.3 Requirements for the security requirements in the strict conformance case

The PP/ST:

- **shall** contain all SFRs and SARs in the PP;
- **may** claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST **shall** be consistent with that in the PP; either the same completion will be used in the PP/ST as that in the PP or one that makes the requirement more restrictive.
NOTE the rules of refinement apply.

9.4.4 Additional requirements specific to the demonstrable conformance case

Demonstrable conformance allows a PP author to describe a common security problem to be solved and provide generic guidelines to the requirements necessary for its resolution, in the knowledge that there is likely to be more than one way of specifying a resolution.

- The PP/ST **shall** contain a rationale on why the PP/ST is considered to be “equivalent or more restrictive” than the PP.

9.5 Using PPs

If a PP/ST claims to be conformant to one or more PPs and possibly one or more packages, the evaluation of that PP/ST will include a demonstration that the PP/ST actually conforms to the claimed PPs and/or packages. Details of this determination of conformance **can** be found in Annex A.

This allows the following process:

- An organization seeking to acquire a particular type of IT security product develops their security needs into a PP, then has this PP evaluated and publishes it;
- A developer takes this PP, writes an ST that claims conformance to the PP and has this ST evaluated;
- The developer then builds a TOE (or uses an existing one) and has this evaluated against the ST.

The result is that the evaluated TOE meets the requirements of the organization as defined in the PP and that the organization **can** therefore have confidence that the TOE meets their security needs. A similar line of reasoning applies to packages.

9.6 Conformance statements and claims in the case of multiple PPs

9.6.1 General

The ISO/IEC 15408 series allows both STs and PPs to claim conformance to multiple PPs. The case for an ST claiming conformance to multiple PPs is covered in 11. This subclause, 9.6 covers the case where a PP claims conformance to multiple PPs.

9.6.2 Where exact conformance is specified

A PP **shall not** claim exact conformance to another PP or combination of PPs. The same effect **may** be achieved by creating PP-Configurations, where PP-Modules are used to specify additional functionality to one or more Base-PPs.

9.6.3 Where strict or demonstrable conformance is specified

Allowing a PP to claim conformance to multiple PPs permits chains of PPs to be constructed, each PP in the chain is based on the previous PP(s).

EXAMPLE

PPs for an Integrated Circuit and for a Smart Card OS, **can** be used to construct a Smart Card PP (IC and OS) that claims conformance to both. In turn, this Smart Card PP could be used to develop a PP on Smart Cards for Public Transport based on the Smart Card PP and a PP on Applet Loading. Finally, a developer could then construct an ST based on these Smart Cards for Public Transport PP.

9.7 Selection-based security functional components and SFRs

Editors' Note:

Can PP-Modules also contain selection based SFRs?

The Editors believe this is true, but request confirmation from commenters.

If PP-Modules can use Selection-based SFRs then this subclause will need to be moved.

A PP **may** define a set of security functional components and/or SFRs called selection-based SFRs. This set of components and/or SFRs is associated with a selection made in another component and/or SFRs in the PP. The related selection-based components and/or SFRs **shall** be included in a PP/ST if:

- a selection choice identified in the PP indicates that it has an associated selection-based SFR, and
- that selection is made by the PP/ST author.

The PP may be organized so that selection-based components and/or SFRs are grouped together.

EXAMPLE

The selection-based SFRs are included in an annex of the PP.

For the case that a PP author needs to leave a selection operation uncompleted, the PP author **shall** leave the selection-based components and/or SFRs that are related to the uncompleted selection operation, unchanged.

For the case in which the PP/ST author needs to complete the selection, authors **should** include the appropriate selection-based components and/or SFRs in the list of SFRs for the PP/ST.

For the case in which the selection operation is to be restricted, i.e. some but not all of the selections are removed, the PP author **should shall** remove any selection-based components and/or SFRs from the list that corresponds to the choices removed from the selection.

10 Modular Protection Profiles

10.1 General

To allow the definition of Protection Profiles that address a TOE's optional security features, this subclause introduces the concept of modular PPs using three constructs: Base-PPs, PP-Modules and PP-Configurations, and describes the way in which they **may** be used.

10.2 Base-PPs

A Base Protection Profile (Base-PP) is a PP that provides a specification of the base TOE type and the mandatory security requirements for that TOE type. A Base-PP is developed with the intention that it **may** be used with PP-Modules.

Editors' Note:

Editors have added the statement below for clarity.

The requirements and recommendations for PPs, given in 9 are applicable to Modular PPs.

10.3 PP-Modules

10.3.1 General

Editors' Note:

Editor has introduced the term "SPD-element" in order to disambiguate from the defined term "element" used in the original text. Further, using this term simplifies the text in several places replacing "assumptions, threats and security policies." and variants thereof some of which were incomplete.

The term SPD-element has been added to the definitions.

A PP-Module is a consistent set of SPD-elements, Security Objectives for the TOE and the operational environment, and security functional requirements.

NOTE 1 In a Direct Rationale PP-Module, Security Objectives for the TOE are not included.

Unlike PPs, PP-Modules address those security features of a given TOE type that **cannot** be required uniformly for all products of this TOE type.

EXAMPLE

Examples of features that **cannot** be required uniformly for all products within a TOE type are authentication using biometrics, Bluetooth security functions, and Wireless Local Area Network clients.

10.3.2 Requirements for PP-Modules

10.3.2.1 General

A PP-Module **shall** be identified with a reference identifier.

NOTE 1 The reference identifier for a PP-Configuration must be unique within a catalogue.

A PP-Module **shall** refer to a set of one or more Base-PP(s), which constitutes the basis of the PP-Module. The PP-Module **may** refer to alternative sets of Base-PPs.

The PP-Module **may** also refer to alternative sets of Base-PPs.

A PP-Module **may** specify a particular TOE type and **shall** specify additional security functional requirements. A PP-Module **may** introduce new SPD-elements to the Base-PPs and **may** also refine or interpret some of the SPD-elements of the Base-PPs.

NOTE 1 In a Direct Rationale PP-Module, Security Objectives for the TOE are not included.

If the PP-Module refers to more than one Base-PP, the set of Base-PPs **shall** be identified in the PP-Module's configuration statement using "and" and "or" statements as described in B.13, in order to identify if they have to be used simultaneously for the evaluation and usage of the PP-Module.

NOTE 2 The evaluation of a PP-Module alone is meaningless. A PP-Module has to be evaluated as part of a PP-Configuration, at least with its mandatory Base-PPs.

Further information on PP-Modules is given in B.3.

10.3.2.2 PP-Module Conformance claims and conformance statements

The conformance claims of a PP-Module:

- a) **shall** state the **edition of ISO/IEC 15408** to which the PP-Module claims conformance;
- b) **shall** describe the conformance to ISO/IEC 15408-2 as either:
 - **ISO/IEC 15408-2 conformant** - A PP-Module is ISO/IEC 15408-2 conformant if all SFRs in that PP-Module are based only upon functional components in the ISO/IEC 15408-2; or
 - **ISO/IEC 15408-2 extended** - A PP-Module is ISO/IEC 15408-2 extended if at least one SFR in that PP-Module is not based upon functional components in ISO/IEC 15408-2;
- c) if evaluation methods and evaluation activities are included in the PP-Module, the conformance claim **shall** describe the conformance to ISO/IEC 15408-4 as:
 - **ISO/IEC 15408-4 conformant** - A PP-Module is ISO/IEC 15408-4 conformant if evaluation methods and activities are supplied in the PP-Module are conformant with the framework described in ISO/IEC 15408-4;

Editors' Note:

See WD2 US/NIAP26 ^

Editors request comments from other NBs in regard to IF evaluation methods and activities may be included in a PP

- d) **may** include a conformance claim made with respect to functional packages. More than one functional package **may** be claimed by a PP-Module.

If a package claim is made, it **shall** consist of one of the following claims for each package:

 - **Package Name Conformant** - PP-Module is conformant to a package if:
 - all constituent parts of the functional package, including the SPD, Security Objectives, and SFRs, of that functional package are present in the corresponding parts of the PP-Module without modification;
 - **Package Name Augmented** - A PP-Module claims an augmentation of a package if:
 - all constituent parts of the functional package, including the SPD, Security Objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but **shall** also contain at least one SFR that is either additional or hierarchically higher than those SFRs contained in the package;

Editors' Note:

The bullet below is proposed by the editor in response to WD2 NIAP/79

- PP-Modules **shall** restate the package conformance claims of their Base-PPs;

NOTE 1 See B.3.2.3.2, that explains that PP-Modules inherit the conformance statement, exact, strict, or demonstrable, from its Base-PPs.
- e) **may** also include a conformance claim with respect to other PPs:
 - **PP Conformant**: The PP-Module conforms with specific PP(s).
- f) In the case of exact conformance, the Conformance Statement:
 - **shall** also include an "allowed with" list specifying any PPs, packages and other PP-Modules that are allowed to be used with the PP-Module;
 - **should not** include the applicable Base-PPs in the "allowed with" list.

NOTE 2 Conformance claims for security assurance packages are inherited from the PP-Module's Base-PP(s).

NOTE 3 The conformance type; i.e. exact, strict, or demonstrable, is inherited from the PP-Module's Base-PP(s).

For more information on the conformance statements and conformance claims for PP-Modules, see Annex B.

A PP-Module shall declare its conformance type, which shall be one of demonstrable, strict, or exact:

- *For demonstrable and strict conformance, there is no restriction on the conformance type of the base PPs. The combination of demonstrable and strict conformance, shall be solved in the PP-Configuration evaluation. The combination of exact with other types of conformance is not allowed.*
- *For exact conformance, the base PPs shall all declare exact conformance type.*

NOTE 1 such explicit declaration of demonstrable or strict conformance allows sponsors to make the most appropriate statement in each PP-Module.

A PP-Module of demonstrable or strict conformance shall define its AL, i.e. the set of SARs that applies to the part of the TOE that is introduced in the PP-Module and the name given to it:

- *If the PP-Module AL is an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference, then the same name should be used.*
- *Otherwise a new name shall be provided for the PP-Module AL.*

A PP-Module of demonstrable or strict conformance shall provide an AL rationale that justifies the adequacy of the PP-Module AL with regard to the underlying threat model as defined in the SPD, and the consistency of the PP-Module AL with all the base PP ALs that are different from the PP-Module AL, if any.

NOTE 2 The PP-Module AL rationale contributes to ensuring that using multiple assurance levels does not undermine the security expected for the assets that are shared between the PP-Module and the base PPs (if shared assets exist).

10.4 PP-Configurations

10.4.1 General

A PP-Configuration is a set of meta-data giving the specification for the use of a Modular PP. A PP-Configuration contains no content such as an SPD, Security Objectives, or security requirements.

A PP-Configuration is an operation on a set of PPs and PP-Modules whose result is semantically equivalent to a PP and intended to be used as such. That is, a PP-Configuration is a way to build a PP from a set of PPs and PP-Modules.

Therefore, unless stated otherwise, a PP denotes either a standard PP that is defined without making use of the configuration operation or a PP-Configuration.

NOTE A Base-PP is a PP that is intended to be used in combination with PP-Modules.

10.4.2 Requirements for a PP-Configuration

10.4.2.1 General

A PP-Configuration:

- may be used in context with the Direct Rationale approach described in B.2.10 and B.3.3. In this case, all of the components of the PP-Configuration shall also use the Direct Rationale approach;
- shall not contain any additional content beyond that described in this document;
- A PP-Configuration should-shall be identified with a reference;

NOTE The reference identifier for a PP-Configuration must be unique within a catalogue.

10.4.2.2 PP-Configuration components statement

A PP-Configuration should be identified with carries a unique reference and

- **shall** identify all the components of the PP-Configuration in a components statement. The components statement shall contain two or more components, at least one of which is a PP.

NOTE 1 These components include the selected Base-PP(s), PP-Module(s) and any other PPs.

NOTE 2 Recall that PP denotes a standard PP or a PP-Configuration; that is, the components list may include PP-Configurations as well. Alternatively, the PP-Configuration may unfold all the component PP-Configurations and include only standard PPs and PP-Modules.

NOTE 3 The components statement is further described in B.4.1.2

- **shall** include the Base-PP(s) of all the PP-Modules included in the PP-Configuration. If the PP-Module defines alternative sets of Base-PPs then only one of these sets **shall** be used in a PP-Configuration;
- **may** select more PPs than the Base-PPs of the PP-Modules;

NOTE 4 An instantiated PP-Configuration is analogous to a PP that includes all the SPD-elements from the Base-PPs, the PP-Modules and any other PPs specified.

10.4.2.3 PP-Configuration conformance statement

The conformance claims of a PP-Configuration;

- shall** state the **edition of ISO/IEC 15408** to which the PP claims conformance;
- shall** provide a **conformance statement** applicable to the ST/PPs that claim conformance to the PP-Configuration, as one of **exact, strict, or demonstrable**, that meet the conformance statements of the PPs and Base-PP(s) in the components statement;

A PP-Configuration must declare its conformance type, which must be one of demonstrable, strict, exact or multiple conformance:

- For demonstrable, strict or exact conformance, all the components of the PP-Configuration must declare the same conformance type, i.e. demonstrable, strict or exact conformance type, respectively.*
- For multiple conformance, the PP-Configuration must provide the list of demonstrable and strict conformance types inherited from each its components. This type of conformance is meaningful when the PP-Configuration contain both demonstrable components and strict components. The combination of demonstrable and strict conformance, must be solved in the ST evaluation. The combination of exact with other types of conformance is not allowed.*

*A PP-Configuration of demonstrable, strict or multiple conformance must define the **PP-Configuration AL**, which consists of:*

- The set of PP ALs and PP-Modules ALs inherited from the PPs and PP-Modules that transitively belong to the PP-Configuration, possibly augmented.*
- The global AL, i.e. the set of SARs that applies to the entire TOE. This can be an (augmented) predefined EAL (EAL1 to EAL7), an (augmented) assurance package defined in an applicable external reference or an assurance package defined within the PP-Configuration.*

*The PP-Configuration AL must carry a new distinctive **name**, unless the global AL and the component ALs are all identical to the same (augmented) predefined EAL (EAL1 to EAL7) or (augmented) assurance package defined in an applicable external reference.*

Editor's Note: Whether the global Assurance Level of a PP-Configuration should include a predefined EAL requires expert discussion.

*A PP-Configuration of demonstrable, strict or multiple conformance must provide an **AL rationale** that justifies*

- The adequacy of the global AL with regard to the threat models as defined in the components' SPD, and*
- The consistency of the global AL and all the component ALs with each other*

Note: The PP-Configuration AL rationale contributes to ensuring that using multiple assurance levels does not undermine the security expected for the assets that are shared between the PPs and PP-Modules that compose the PP-Configuration. The PP-Configuration AL rationale should rely on the PP-Modules AL rationales.

10.4.2.4 PP-Configuration conformance statement in the exact conformance case

In the case that a PP-Configuration contains a PP or Base-PP with an exact conformance statement then:

- a) all PPs/Base-PPs in the PP-configuration **shall** require exact conformance;
- b) all PPs/Base-PPs in the PP-configuration **shall** be specified as being “allowed with” by all other PPs in their conformance statement;
- c) all PP-Modules in the PP-configuration **shall** be specified as being allowed with each of the PPs/Base-PPs in the PP-configuration.

NOTE 1 There are implications for conformance statements in PP-Modules in the exact conformance case that are covered in section B.3.2.3.

NOTE 2 Guidance on the conformance statement is given in B.5.

10.4.2.5 PP-Configuration components statement in the exact conformance case

The components statement of a PP **shall not** include a reference to another PP that specifies exact conformance.

If one Base-PP in a PP-Configuration has a conformance statement of exact conformance, then:

- all other Base-PPs in the PP-Configuration **shall** also have conformance statements of exact conformance;
- **shall** allow the combination of those Base-PPs in the conformance statements for all the referenced Base-PPs; and
- **shall** allow all the PP-Modules given in the PP-Configuration to be used with that Base-PP.

For more information of conformance claims and conformance statements for PP-Configurations see B.4

10.4.3 PP-Configuration SAR statement

- **shall** provide a SAR statement specifying the applicable set of assurance components or requirements.

EXAMPLE

A pre-defined EAL package from ISO/IEC 15408-5 or another assurance package.

11 Security Targets

11.1 General

<introductory material>

11.2 Conformance claims and the conformance statement

11.2.1 Conformance claims made by STs

The conformance claims of an ST:

- a) **shall** state the edition of **ISO/IEC 15408** to which the ST claims conformance.
- b) **shall** describe the conformance to ISO/IEC 15408-2 (security functional requirements) as either:
 - **ISO/IEC 15408-2 conformant** – An ST is ISO/IEC 15408-2 conformant if all SFRs in that ST are based only upon functional components in the ISO/IEC 15408-2, or

- **ISO/IEC 15408-2 extended** – An ST is ISO/IEC 15408-2 extended if at least one SFR in that ST is not based upon functional components in ISO/IEC 15408-2.

NOTE 1 When a TOE is successfully evaluated to an ST, any conformance claims of the ST also hold for the TOE. A TOE **can** therefore also claim to be ISO/IEC 15408-2 conformant.

- c) **shall** describe the conformance to ISO/IEC 15408-3 (security assurance requirements) as either:

- **ISO/IEC 15408-3 conformant** – An ST is ISO/IEC 15408-3 conformant if all SARs in that ST are based only upon assurance components in ISO/IEC 15408-3, or

- **ISO/IEC 15408-3 extended** – An ST is ISO/IEC 15408-3 extended if at least one SAR in that ST is not based upon assurance components in ISO/IEC 15408-3.

- d) if evaluation methods and evaluation activities are included in the document, the conformance claim **shall** describe the conformance to ISO/IEC 15408-4 (framework for the specification of evaluation methods and activities) as:

- **ISO/IEC 15408-4 conformant** – An ST is ISO/IEC 15408-4 conformant if evaluation methods and activities are supplied in the PP or PP-Module is based on the framework described in ISO/IEC 15408-4.

Editors' Note:

See WD2 US/NIAP26 ^

Editors request comments from NBs /liaisons in regard to IF evaluation methods and activities may be included in a PP.

- e) **may** include a claim made with respect to packages.

NOTE 1 More than one package **can** be claimed in an ST.

If the conformance claim is one of exact conformance then a package claim **shall not** be made.

NOTE 2 For exact conformance, any packages included are specified in the PPs or via a PP-Configuration. i.e. in the exact conformance case packages are inherited.

If a package claim is made, it **shall** consist of one of the following claims for each package:

- **Package name Conformant** - An ST is conformant to a package if:

- For functional packages, all constituent parts (security problem definition, Security Objectives, and SFRs) of that ST are identical to the SFRs in the functional package,
- For assurance packages, the SARs of that ST are identical to the SARs in the assurance package.

- **Package name Augmented** – An ST claims augmentation of a package if:

- For functional packages, all constituent parts (SPD, Security Objectives, and SFRs) of that ST contain all constituent parts given in the functional package but **shall** contain at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
- For assurance packages, the SARs of that ST contain all SARs in the assurance package, but **shall** contain at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package;

- f) **may** also include a conformance statement with respect to PPs:

- **PP Conformant** - A PP or TOE meets specific PP(s) or PP-Module(s).

- A Direct Rationale ST **may** only claim conformance to one or more other Direct Rationale PPs (see Annex B).

- g) **may** also include a conformance statement with respect to PP-Configurations

- An ST **may** claim conformance with one or more PP-Configurations when the conformance statement for the PP-Configuration is strict or demonstrable
- An ST **shall not** claim conformance to more than one PP-Configuration when the conformance statement is exact.
- A Direct Rationale ST **shall** only claim conformance to a PP-Configuration if that PP-Configuration uses the Direct Rationale approach.

For more information on the Conformance Statements for STs see Annex A.

For more information on conformance types see Annex E.

11.2.2 Additional requirements for the SPD in the exact conformance case

An ST claiming exact conformance:

- **shall** contain the SPD of all PPs and PP-Modules to which it is claiming exact conformance, including all SPD elements.
- **shall not** include any SPD-elements that are not present in the PP and PP-Modules to which it is claiming exact conformance.

NOTE 1 The combination of PPs and PP-Modules is usually specified as part of a PP-Configuration. See 10.4.

Editors' Note:

Editors noted that PP-Modules may also contain an SPD and therefore added “and PP-Modules” to the above statements.

Editors also added the note in an attempt to clarify the role of a PP-Configuration here.

Editors further note that 11.2.2 is discussing STs and may be misplaced in the PP subclause. Should it be in 12?

11.2.3 Additional requirements for the Security Objectives in the exact conformance case

An ST claiming exact conformance:

- **shall** contain all the Security Objectives for the TOE specified in all of the PPs and PP-Modules to which it claims conformance;
- **shall not** specify additional Security Objectives for the TOE that are not specified in the combination of the PPs and PP-Modules to which it claims conformance;
- **shall** contain all of the Security Objectives for the operational environment that are specified in the combination of PPs and PP-Modules to which it claims conformance; and
- **shall not** specify additional Security Objectives for the operational environment that are not present in the combination of PPs and PP-Modules to which it claims conformance.

NOTE 1 The combination of PPs and PP-Modules is usually specified as part of a PP-Configuration.

Editors' Note:

Editors noted that PP-Modules may also contain Security Objectives and therefore added “and PP-Modules” to the above statements.

Editors also added the note in an attempt to clarify the role of a PP-Configuration here

Editors note that 11.2.3 is discussing STs and may be misplaced in the PP subclause. Should it be in 12?

11.2.4 Additional requirements for the security requirements in the exact conformance case

An ST **shall** contain all the SARs present in the PPs, and all the SFRs present in the PPs and PP-Modules, with the following exception:

- SFRs designated as selection-based SFRs in the PPs or PP-Modules **shall** be excluded if the selection that requires their inclusion is not chosen by the ST author.

NOTE 1 This means that PP/ST authors **cannot** include additional or hierarchically higher security requirements.

2629 NOTE 2 See 9.7 and B.2.7 for further information in regard to selection-based SFRs.

2630 NOTE 3 See Annex E for further information on PP conformance.

2631 11.3 Using PP-Configurations in Security Targets

2632 11.3.1 General

2633 PP-Modules are used to build specific PP-Configurations on top of one or more Base-PPs. Hence, PP-
2634 Modules **shall** only be used by STs as a constituent part of any claimed PP-Configurations.

2635 PP-Configurations **may** be used by STs in a manner similar to that employed by Protection Profiles. An
2636 ST **can may** claim conformity to a PP-Configuration ~~provided that this PP-Configuration has been~~
2637 ~~evaluated~~. See 12.3 for a discussion of the evaluation of PP-Configurations.

2638 Editors' Note:

2639 ISO/IEC 15408 cannot demand that evaluation be performed. (ISO/IEC Directives Part 2, 2018 Section 33.1)

2640 This requirement will be deleted in the next draft

2641 We may be able to make it a recommendation ("should") or a permission ("may") Comments on this are
2642 requested.

2643 NOTE The evaluation of a PP-Configuration **can** be performed upfront, independently of any product
2644 evaluation. Alternatively, the evaluation of a PP-Configuration **can** be performed during the evaluation of a
2645 conformant Security Target, prior to evaluating the ST conformance claim.

2646 *A Security Target may claim conformance with one or more PPs and PP-Configurations, thereby complying*
2647 *with their conformance types. The combination of demonstrable and strict conformance must be solved in the*
2648 *ST evaluation. The combination of exact conformance with other conformance types is not allowed, i.e. an ST*
2649 *cannot claim conformance to an exact PP and to a demonstrable or strict PP.*

2650 *A Security Target that claims conformance with one or more PPs or PP-Configurations of demonstrable, strict*
2651 *or multiple conformance type must define the **ST AL**, which consists of:*

- 2652 • *The set of PP ALs and PP-Modules ALs inherited from the PPs and PP-Configurations the ST*
2653 *claims conformance with, possibly augmented.*
- 2654 • *The global AL, i.e. the set of SARs that applies to the entire TOE. This can be an (augmented)*
2655 *predefined EAL (EAL1 to EAL7), an (augmented) assurance package defined in an applicable*
2656 *external reference or an assurance package defined within the ST.*

2657 *The ST AL must carry a new distinctive **name**, unless*

- 2658 • *The global AL and the component ALs are all identical to the same (augmented) predefined*
2659 *EAL (EAL1 to EAL7) or (augmented) assurance package defined in an applicable external*
2660 *reference.*
- 2661 • *The ST conforms with a standard PP only, and the global ST AL is identical to the PP AL.*
- 2662 • *The ST conforms with a PP-Configuration only, and the ST AL is identical to the PP-*
2663 *Configuration AL.*

2664 *Editor's Note: Whether the global Assurance Level of an ST should include a predefined EAL requires*
2665 *expert discussion.*

2666 *A Security Target that defines an ST AL must provide an **AL rationale** that justifies*

- 2667 • *The adequacy of the global AL with regard to the threat model as defined in the SPD, and*
- 2668 • *The consistency of the global AL and all the component ALs with each other*

2669 *Note: The ST AL rationale contributes to ensuring that using multiple assurance levels does not undermine the*
2670 *security expected for the ST's assets that are shared with the PPs and PP-Configurations to which the*
2671 *ST claims conformance with. The ST AL rationale should rely on the PP-Configurations AL and PP-*
2672 *Modules AL rationales.*

2673 *Note: If the ST global AL is simply the lowest of the components ALs, then the consistency holds implicitly and*
2674 *does not require a rationale.*

2675 **12 Evaluation and evaluation results**

2676 **12.1 General**

2677 This clause 11.3 presents the expected results from PP, PP-Configuration and ST/TOE evaluations
2678 performed according to either ISO/IEC 18045, and/or evaluation methods developed using ISO/IEC
2679 15408-4.

2680 Evaluation **should** lead to objective and repeatable results that **can** be cited as evidence, even if there is
2681 no absolute objective scale for representing the results of a security evaluation.

2682 NOTE The use of evaluated PPs and PP-Configurations along with the use of well-defined evaluation
2683 methodologies is a necessary pre-condition for evaluation that leads to a result that provides a technical basis for
2684 the mutual recognition of evaluation results between evaluation authorities. Recognition criteria are out of the
2685 scope of this standard.

2686 An evaluation result represents the findings of a specific type of investigation of the security properties
2687 of a TOE. Such a result does not automatically guarantee fitness for use in any particular application
2688 environment. The decision to accept a TOE for use in a specific application environment is based on
2689 consideration of many security issues including the evaluation findings.

2690 Figure 3 describes the various evaluations that are needed to provide confidence in the evaluation
2691 results for a TOE.

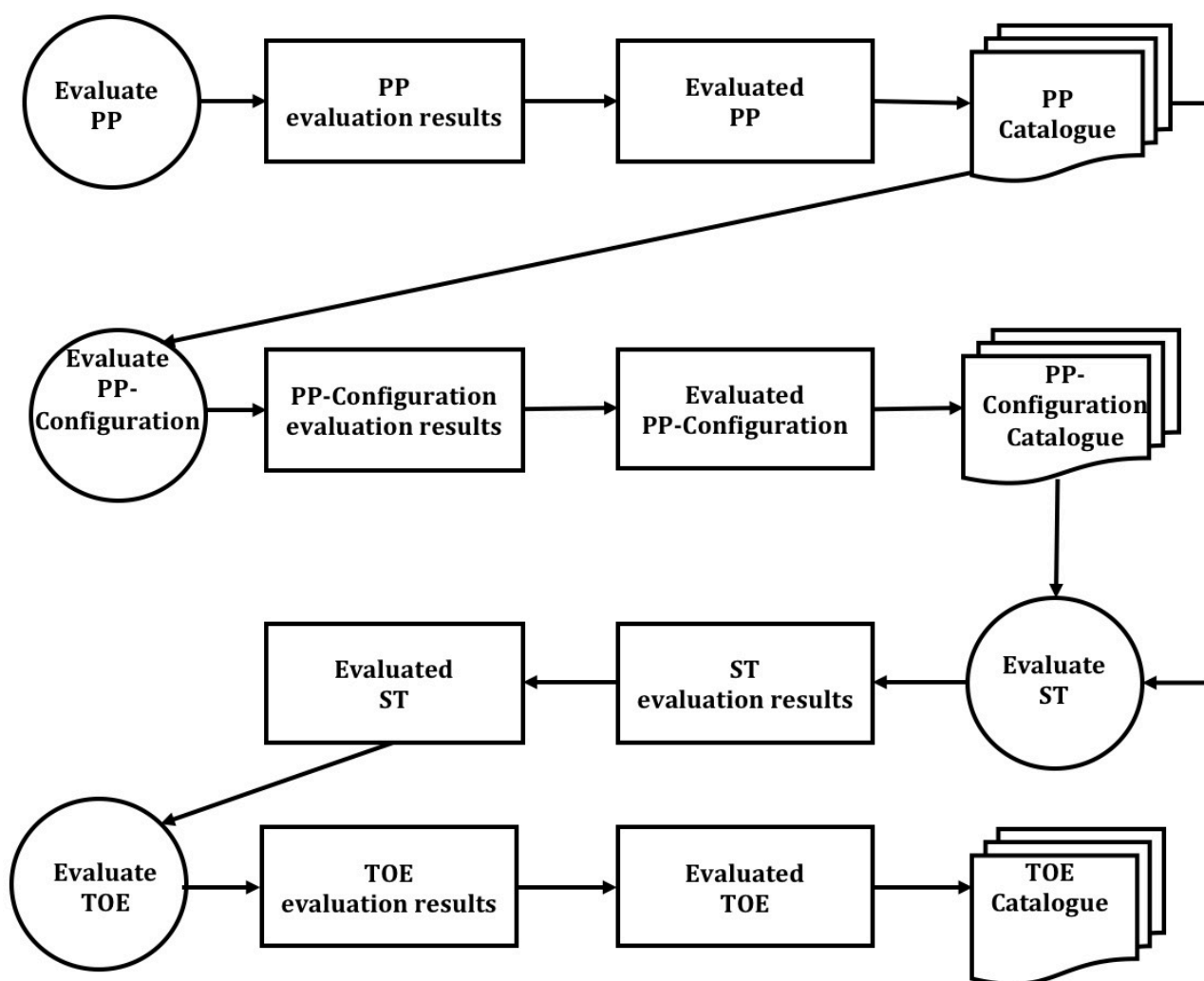


Figure 3 — Evaluation flow

The ISO/IEC 15408 series gives criteria for four types of evaluation:

- a) A PP evaluation which is based on the APE class given in ISO/IEC 15408-3, described in 12.3,
- b) A PP-Configuration evaluation which is based on the ACE class given in ISO/IEC 15408-3, described in 12.3,
- c) An ST evaluation which is based on the ASE class given in ISO/IEC 15408-3, described in 12.5, and
- d) A TOE evaluation, which is based on an evaluated ST and the criteria for evaluating the security requirements claimed by the ST, described in 12.5.

NOTE 1 — ISO/IEC 15408 uses the term *evaluation*, without qualifiers, to refer to an ST/TOE evaluation.

Editors' Note:

Editor proposes to remove NOTE 1 since it is not consistent with the definition of the term “evaluation”.

If no comments are received on this, the editor’s proposal will be accepted and presented in the next draft.

PP and PP-Configuration evaluations provide confidence that the PP and/or PP configuration meets the requirements of the ISO/IEC 15408 series. Catalogues of PPs and PP-Configurations can be maintained by approval authorities or others, criteria for inclusion in the catalogue can include a positive evaluation result as well as other policies of the approval authority.

PP-Modules are only evaluated as part of a PP-Configuration evaluation.

Packages are only evaluated as part of a PP, PP-Configuration, or ST evaluation.

NOTE 2 In practice, a ST that claims conformance with some non-evaluated PP-Configurations **may** still be evaluated by performing the PP-Configuration evaluation first.

An ST evaluation leads to an intermediate result that is used in the frame of a TOE evaluation.

Optionally, STs **may** be developed with conformance claims to packages, PPs and PP-Configurations.

ST/TOE evaluations **can** lead to catalogues of evaluated TOEs. In many cases these catalogues **can** refer to the IT products that the TOEs are derived from rather than the specific TOE. Therefore, the existence of an IT product in a catalogue ~~should not~~ **cannot** be construed as meaning that the whole IT product has been evaluated; instead the actual ST defines the actual extent of the TOE evaluation.

Refer to the bibliography for examples of such catalogues.

12.2 The evaluation context

In order to achieve greater comparability between evaluation results, evaluations **should** be performed within the framework of an evaluation scheme that sets the standards, monitors the quality of the evaluations, and administers the regulations to which the evaluation facilities and evaluators **must** conform.

~~NOTE 1 — The ISO/IEC 15408 series does not state requirements for the regulatory framework. The evaluation schemes and certification processes are the responsibility of the evaluation authorities that run such schemes and processes and are outside the scope of the ISO/IEC 15408 series. However, consistency between the regulatory frameworks of different evaluation authorities is necessary to achieve the goal of mutual recognition of the results of such evaluations.~~

Editors' Note:

The 2018 Directives, and training provided by ISO instructs document editors that regulation, legislation etc shall not be even mentioned in ISO standards (even to say that it is not in scope!). Hence this note will be deleted in the next draft.

Supporting greater comparability between evaluation results is also achieved through the use of common evaluation methods producing these evaluation results. Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results **may** be submitted to a certification process.

NOTE ISO/IEC 19896-3 provides competency requirements for ISO/IEC 15408 evaluators which **can** be used to support conformity in the evaluation process.

For the ISO/IEC 15408 series, the basic common evaluation methodology is given in ISO/IEC 18045 and this **may** be supplemented or replaced by other methodologies derived from ISO/IEC 18045, conforming with the framework given in ISO/IEC 15408-4.

EXAMPLE

It **may** be necessary for PP authors to supplement the basic common evaluation methodology with a method that includes technology-specific evaluation activities.

A certification process, which is outside the scope of the ISO/IEC 15408 series, is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which **can** be publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.

12.3 Evaluation of PPs and PP-Configurations

Basing a PP or an ST on an evaluated PP has two advantages:

- There is much less risk that there are errors, ambiguities, or gaps in the PP. If any problems with a PP, that would have been found during the evaluation of that PP, are found during the writing or evaluation of the new ST, significant time **may can** elapse before the PP is corrected.

- Evaluation of the new PP/ST **can** re-use the evaluation results of the evaluated PP, resulting in less effort being employed in the evaluation of the new PP/ST.

If the evaluation of a PP is required then the APE criteria, given in ISO/IEC 15408-3 **shall** be used.

If the evaluation of a PP-Configuration is required then the ACE criteria given in ISO/IEC 15408-3 **shall** be used.

The goal of such evaluations is to demonstrate that the PP, or PP-Configuration is complete, consistent, and technically sound and suitable for use as a template on which to build an ST or another PP.

The method of stating evaluation results for PPs and PP-Configurations is described in 12.8.

NOTE PP-Modules are not evaluated separately; they are evaluated in the course of evaluating the PP-Configuration that uses them.

For a multi-assurance PP-Configuration, the ACE requirements ensure that the combination of different ALs does not undermine the expected security level of the underlying assets, as defined in the SPDs of the component PPs and PP-Modules.

12.4 Multi-assurance evaluation

The multi-assurance evaluation paradigm allows addressing heterogeneous products/systems, that is,

- *Evaluation of a product/system with security functionality that requires different assurance levels within a single evaluation driven by a security target of the product/system;*
- *Evaluation of complementary security functionality at a given assurance level on top of an evaluated multi-assurance product/system.*

and ensuring that the multiple assurance levels are sound with regard to the security needs for the product/system.

EXAMPLE

Examples where the multi-assurance paradigm is relevant are the following:

- *A device where some security functionality requires higher assurance than the rest, for instance, a key storage and processing unit, a secure boot module, etc.*
- *A device where some parts of the security functionality do not require the same high evaluation assurance as other more exposed parts of the device, for instance an internet gateway with support for personal area network protocols.*
- *A device where some security functionality can be implemented in different ways for different use cases, requiring different levels of assurance for the different implementations, for instance*
 - *tamper-resistant module;*
 - *software module;*
 - *(third-party) black-box components.*

12.5 Evaluation of STs

An ST evaluation determines that the sufficiency of the TOE, the operational environment and the internal consistency of the descriptions and requirements it contains.

The ST evaluation **shall** be carried out by applying the Security Target evaluation criteria, given in the ASE class of ISO/IEC 15408-3 to the Security Target. The precise method to apply the ASE criteria is determined by the evaluation methodology that is associated with the ST, which **may** be either ISO/IEC 18405 or a specific derived methodology defined using ISO/IEC 15408-4.

The method of stating ST evaluation results is described in 12.8. These results also identify any PP(s) and package(s) to which the TOE claims conformance.

For a multi-assurance ST, the ASE requirements ensure that:

- *The combination of different ALs does not undermine the expected security level of the underlying assets, as defined in the SPD.*
- *Each AL belonging to the ST AL is mapped to a well-defined set of SFRs.*

12.6 Evaluation of TOEs

A TOE evaluation determines that the correctness of the TOE against the criteria defined in the Security Target. As said earlier, the TOE evaluation does not assess the correctness of the operational environment.

The TOE evaluation is more complex. The principal inputs to a TOE evaluation are the evaluation evidence, which includes the TOE and the ST, but will usually also include input from the development environment, such as design documents or developer test results.

The TOE evaluation consists of applying the SARs (from the Security Target) to the evaluation evidence. The precise method to apply a specific SAR is determined by the evaluation methodology that is associated with the ST, either ISO/IEC 18405 or a specific derived methodology defined using ISO/IEC 15408-4.

How the results of applying the SARs are documented, and what reports need to be generated and in what detail, is determined by both the evaluation methodology that is used and the evaluation scheme under which the evaluation is carried out.

The TOE evaluation **may** be carried out after TOE development has finished, or in parallel with TOE development, provided that the appropriate assurance components are chosen for this evaluation.

The method of stating ST/TOE evaluation results is described in 12.8.

12.7 Evaluation methods and activities

Basic evaluation methods and activities for each of the security assurance classes given in ISO/IEC 15408-3 are provided in ISO/IEC 18045. These are high level and often need to be supplemented by more specific evaluation methods and activities depending on the technology type, the assurance level needed or the security problem described.

Methods and activities derived from ISO/IEC 18045 **may be** conformant with ISO/IEC 15408-4. Such methods and activities are generally published either as additions to PPs, PP-Modules or as separate supporting documents.

12.8 Evaluation results

12.8.1 Results of a PP-Configuration evaluation

The results of a PP-Configuration evaluation **shall** also include a “conformance claim” in accordance with 10.4.

Once a PP-Configuration has been evaluated, an ST evaluation **may** rely on the results of the PP-Configuration evaluation.

NOTE 1 ISO/IEC 15408-3 provides evaluation criteria for PP-Configurations in the ACE class.

NOTE 2 The evaluation of a PP-Configuration **can** arise in two situations, with no impact on the evaluation methodology:

- Independently of any product evaluation, or
- As the first step of the evaluation of a Security Target that claims conformity with the PP-Configuration. Otherwise the conformance claim is meaningless and the ST evaluation would fail in this aspect.

12.8.2 Results of a PP evaluation

The results of the PP evaluation **shall** also include a “Conformance Claim” in accordance with 9.

NOTE 1 ISO/IEC 15408-3 provides evaluation criteria for PPs in the APE class.

12.8.3 Results of an ST/TOE evaluation

Evaluation of the TOE **shall** therefore result in a pass/fail statement for the ST. If both the ST and the TOE evaluation have resulted in a pass statement, the underlying product **can** be eligible for inclusion in a catalogue.

The results of an ST evaluation **shall** also include a “Conformance Claim” as defined in 11.2.1.

The result of the TOE evaluation process is either:

- A statement that not all SARs have been met and that therefore there is not the specified level of assurance that the TOE meets the SFRs as stated in the ST;
- A statement that all SARs have been met, and that therefore there is the specified level of assurance that the TOE meets the SFRs as stated in the ST.

NOTE 1 In some cases the evaluation results are subsequently used in a certification process, but this certification process is outside the scope of ISO/IEC 15408.

NOTE 2 ISO/IEC 15408-3 provides evaluation criteria for STs in the ASE class.

12.8.3.1 Use of ST/TOE evaluation results

Once an ST and a TOE have been evaluated, asset owners can have the assurance, as defined in the ST, that the TOE, together with the operational environment, counters the stated threats. The evaluation results **may** be used by the asset owner as part of a risk-acceptance decision related to exposing the assets to the threats.

Editors' Note:

Unless comments are received to the contrary, the editor proposes to make the following change, adding “deployed TOE”:

b) the operational environment of the deployed TOE asset owner conforms....

However, risk owners **should** carefully check whether:

- a) the SPD in the ST matches their own security problem;
- b) the operational environment of the asset owner conforms (or **can** be made to conform) to the Security Objectives for the operational environment described in the ST;
- c) any guidance documents provided by the developer in the context of the TOE evaluation are followed during the installation, configuration, and operation of the TOE.

If either one of these conditions do not hold, the assurance **may** not hold true and the evaluation results **should** not be relied upon in a risk-acceptance decision.

Additionally, once an evaluated TOE is in operation, it is probable that previously unknown errors or vulnerabilities in the TOE will be identified. In that case, the developer **may** correct the TOE (to address the vulnerabilities) or change the ST in a way that excludes the newly identified vulnerabilities from the scope of the evaluation. In either case, the old evaluation results **may** no longer be valid

NOTE If assurance is to be maintained, re-evaluation is needed. The ISO/IEC 15408 series **may** be used for this re-evaluation, but detailed procedures for re-evaluation are outside the scope of this document.

2866 **13 Composition of assurance**

2867 **13.1 General**

2868 IT Products are almost always composed from several components. Some of which **may** be evaluated
 2869 and some which are not.

EXAMPLE
 evaluated software is composed with hardware to create an IT product.

2870 Independent product components are often evaluated separately and the problem of composing the
 2871 security assurance to determine the assurance of the entire product arises.

2872 This section describes methods by which security assurance for a multi-component product can be
 2873 provided, and how much can be re-used from the evaluation of individual components. It also discusses
 2874 the important considerations when re-using evaluation results.

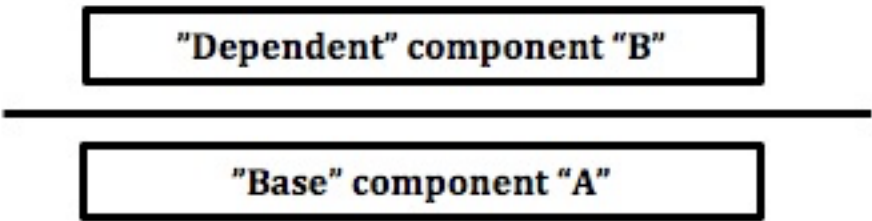
2875 Composition of assurance is dependent upon:

- 2876 — the type of composition,
- 2877 — the security function policies, and organizational security policies that the component
 2878 evaluation was based on,
- 2879 — the claimed security assurance, for example the assurance level,
- 2880 — the overall security policies for the entire product.

2881 **13.2 General composition models**

2882 **13.2.1 Layered**

2883 In this type of layered composition, one component is built on top of another component, as pictured in
 2884 Figure 4.



2885 **Figure 4 — Layered composition**

2886 The following assumptions are made in regard to the layered assurance composition model:

- 2887 — The base component is independent from the dependent component
- 2888 — The base component is not modified by the dependent component
- 2889 — The dependent component uses the functions of the base component and not vice versa

2890 Those performing such a composition should consider that:

- 2891 — The dependent component **may** depend on functions not considered to be security functions in
 2892 the evaluation of the base component. In particular, for
 - 2893 — Hardware/software layering: Almost all instructions of the hardware are used to
 2894 implement the security functions
 - 2895 — Software layering: the dependent component layer **may** depend on some functions not
 2896 considered in the evaluation of base component layer.

EXAMPLE 2

access control **may** be based on different objects.

- 2915 — Assumptions made on a component **may** not be valid,

EXAMPLE 3

assumption on the protection of critical data transferred to another component.

- 2916 — Security functions **may** have unwanted side effects.

EXAMPLE 4

A covert channel leaking cryptographic keys

- 2917 If these kinds of issues are identified then they should be clearly documented along with the
2918 determination of appropriate mitigating controls.

Editors' Note

The items above and the final remarks are vague and give the impression that it is possible to evaluate all these cases, when they are actually quite different:

- when assumptions do not hold, the situation seems very hard to manage

- when security functions have unwanted side effects, countermeasures on one part might fix the problem

It is also not clear who implements the "mitigation controls" : any/both components?

We should consider editing this in a way that clearly states that not all cases can be addressed, and that a defined method must be created for such composition activities, as it has been done with composite evaluation for layered models.

13.2.3 Embedded

In this type of composition, a component is used as part of a larger component or product. See Figure 6.

EXAMPLE

A library or subsystem providing specific security functions as part of a larger product.

The following assumptions are made in regard to the embedded assurance composition model:

- There is usually no separation between the composed parts,
- Each part **may** influence the other via channels and interfaces other than the intended ones.

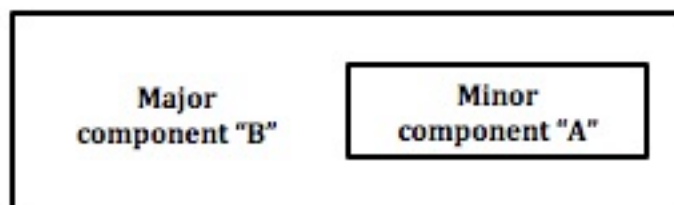


Figure 6 — Embedded composition

Those performing such a composition should consider that due to the lack of separation, components may:

- bypass security functions of the other components,
- modify the security functionality and security policy of other components and the whole product,
- introduce a number of critical side effects.

NOTE If separation is specified ADV_ARC given in ISO/IEC 15408-3 describes criteria for evaluation

Editors' Note

Same as before. The definition of is not clear, we should consider clarify main cases (that can/cannot be addressed) and clarify that the standard currently provides no method, so it is up to the user to create it.

13.3 Evaluation techniques for providing assurance in composition scenarios

13.3.1 Using the ACO class

The ACO class specified in ISO/IEC 15408-3, addresses a TOE composed of two TOEs, both of which have been separately evaluated, and that are composed using a layered technique. These TOEs can be described as a base TOE and a dependent TOE, see Figure 7. An evaluation of the composed TOE consists of evaluating the interaction between both TOEs, reusing evaluation results from both the base TOE and the dependent TOE.

ISO/IEC 15408-5 provides pre-defined composed assurance packages (CAP) that **may** be used for rating the composed TOE's assurance. CAPs provide an alternative approach to obtaining higher levels of assurance for a composed TOE than application of the EALs above EAL1.

The ACO class is applicable up to Extended-Basic assurance level.

Figure 7 shows a typical scenario where the ACO class can be used for evaluating a composition.

Editors' Note:

The following figure corresponds to the definition of composed TOE, not to a typical scenario. A concrete example is welcome

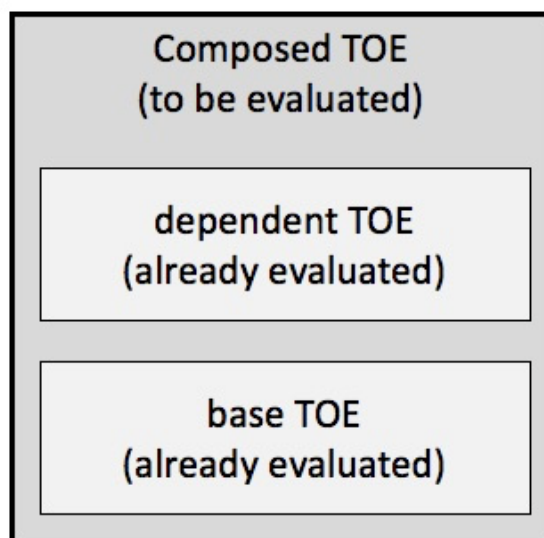


Figure 7 — Composed TOE evaluated using the ACO class

13.3.2 Composite product evaluation using a layered composition model

Editors' Note:

Note to experts: This text is drawn from JIL Composite product evaluation for smart cards and similar devices (V1.5 October 2017). It has been modified to be more generic (as it must be for inclusion in part 1), but provides copious examples for the smart card technology domain. Note that the source document itself states that :

“, this document is not restricted to smart cards and similar devices only and can be applied in principle (possibly with adequate adaptations, as far as necessary) for any other secure IT product where an independently evaluated component is part of a final composite product to be evaluated.”

The composite product evaluation technique was devised to meet different types of objectives:

- independently perform one evaluation of a platform to address several applications and customers;

- create one or several applications to load on one or several certified platforms;
- install one or several applications onto one already certified platform to reduce the evaluation effort keeping a high level of confidence.

The evaluation technique describes a way to perform a transfer of knowledge and a reuse of evidence, in order to meet these objectives.

13.3.2.1 Objective

This method for composition of assurance applies to layered composite IT products that comprise one or more base TOE(s) evaluated independently and one or more dependent component(s). In the composite evaluation approach, the evaluation of the dependent component is performed within the evaluation of the composite product (that is, the composite TOE is made of the integration of the base TOE and the dependent component). Therefore, assurance level is claimed for and applies to the composite TOE as a whole and not to the dependent component alone.

Unlike ACO-based evaluation, this allows a direct comparison with similar products that are evaluated at once without using composition techniques. Moreover, there is no limitation in the assurance level, i.e. the composite TOE can claim any predefined EAL or well-defined assurance package, including resistance up to 'high attack potential' such as those defined in ISO/IEC 15408-3 AVA_VAN.5, whereas ACO is limited by CAP requirements up to 'enhanced-basic' attack potential.

EXAMPLE

Examples of smart card devices requiring high-level assurance include banking (finance) and digital-signature applications.

Smart cards and similar devices are built up with a combination of two parts: a hardware integrated circuit (IC) part and a software part often developed by different actors with specific objectives.

The software part **may** be layered itself, consisting of an "Operating System layer" with possibly integrated applicative functions and an "Application layer" on top of it that **may** contain different applications.

13.3.2.2 Concept of composite TOE

A Composite TOE is composed of a base component and a supplementary layer. The base component is identified as "Platform TOE" in Figure 8, and will be identified as the 'Platform' in the remainder of this document. The supplementary layer is identified in Figure 8 as the 'Application TOE' and will be identified as the 'Application' in the remainder of this document.

- The Platform is the underlying layer. This layer shall have already been evaluated. Therefore, it has a sponsor, a developer, an evaluator, and an evaluation authority;
- The Application is the supplementary layer that is dependent on the Platform. This layer shall also be evaluated.
- The Composite Product includes the Platform and the Application. The composite evaluation technique is intended to optimize the evaluation of this Composite Product;
- Non-TOE parts of the Composite Product, the Platform and the Application are considered part of the operational environment of the Composite Product TOE.

Several composition steps can follow each other. In other terms, the Platform can itself be a composite product.

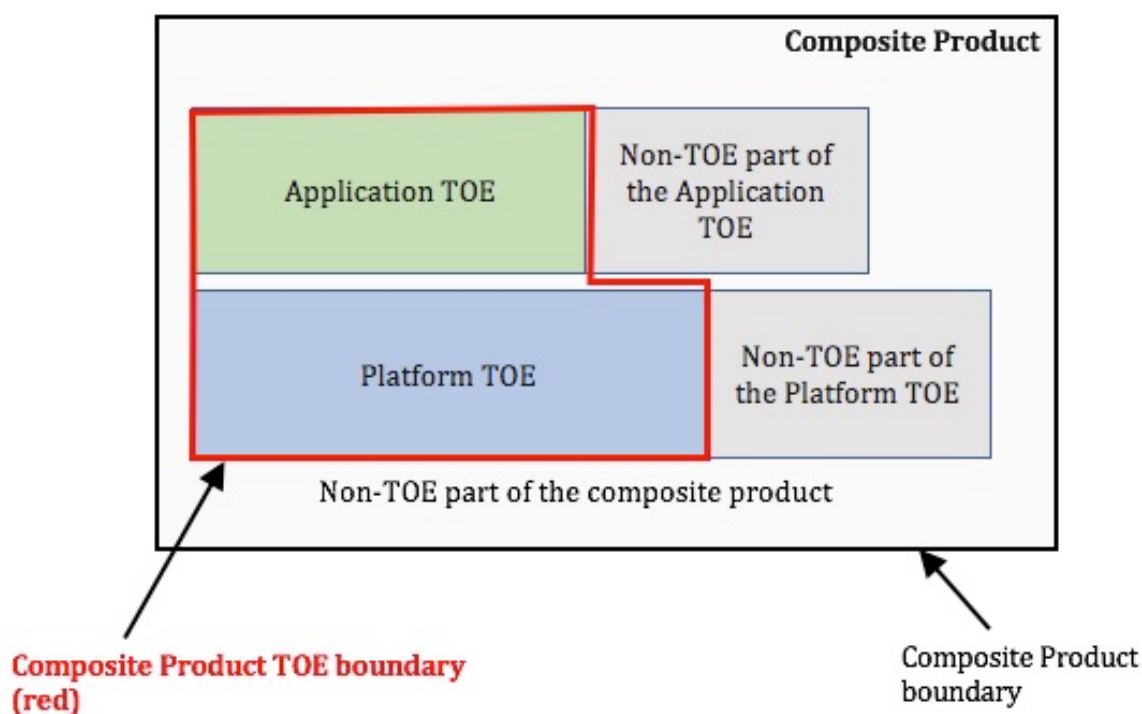


Figure 8 — Composite TOE

Some rules apply when defining the Composite Product TOE:

- The application TOE cannot rely on platform functionalities that are outside the platform TOE, in the Non-TOE parts. This is depicted in grey layer 'Non-TOE part of the Platform TOE';
- The composite TOE is composed with a superset of the entire application TOE, and a superset of the minimum platform TOE functionalities required for the correct execution of the composite product;
- The non-TOE subset of the application can use platform TOE functionalities. As usual, the composite evaluation needs to determine that this non-TOE application part is non-interfering with the application TOE – neither directly nor through the usage of the platform functionalities.

NOTE 1: Composite evaluation can be applied independent of the evaluation assurance level (EAL) for the composite product aimed. Where some evaluation activities are not applicable due to the EAL chosen, they are also not expected to be applied.

NOTE 2: This standard only addresses cases where the level of assurance of the platform is equivalent or higher compared to the composite product evaluation level. Other cases will require dedicated techniques defined by evaluation authorities.

NOTE 3: In the case where both platform and application have already been evaluated using ISO/IEC 15408, a partial evaluation work may be performed regarding the results already obtained from previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

Editors' Note :

Figure 8 was a bit misleading and described incorrectly scenario 2 as a “composed TOE”, since this term is reserved for ACO usage.

Also, this second scenario is possible in theory, and allowed by JIL, but is not used in practice since it would be very impractical. We suggest to remove completely this second scenario from the standard.

13.3.2.3 Roles

The Platform and the Application are all undergoing an evaluation. Therefore, both of them have a sponsor, a developer, an evaluator, and an evaluation authority.

The Composite Product also undergoes an evaluation, and also has a sponsor, an evaluator, and an evaluation authority. However, the composite evaluation performs the evaluation of the Application during the evaluation of the Composite Product. Consequently:

- the Application sponsor is, in practice, the Composite Product sponsor;
- the Application evaluation authority is, in practice, the Composite Product evaluation authority;
- the Application evaluator is, in practice, the Composite Product evaluator;
- there is no Composite Product developer in practice since the Composite Product is resulting from the integration of the Application and the Platform. Instead, the composite evaluation technique defines additional evaluation activities for:
 - the Application developer and the Platform developer;
 - the Composite Product Integrator.

NOTE 1 As already mentioned, the Application **may** have undergone a separate evaluation, but the evaluator and evaluation authority of this previous evaluation are not considered here. Notably, the terms Application evaluator and Application evaluation authority do not refer to this previous evaluation.

NOTE 2 As in the general cases, some other actors involved **may** be the same. The composite evaluation context also leads to specific cases of actors having several roles. Each evaluation will associate particular organizations or persons to these generic roles.

EXAMPLE:

- The Platform developer **may** also be the Platform sponsor;
- The Platform evaluation authority **may** also be the Composite Product evaluation authority.

NOTE 3 The Composite Product Integrator is a different concept than the developer. While this integrator may, in some cases, also be one of the developers defined previously, this is not always true. An example taken from [21] illustrates the role of the Composite Product Integrator:

- Native Smart cards: The 'underlying platform' is an integrated circuit and the Platform Developer is the integrated circuit (chip) manufacturer; the 'application' is a card operating system and its application(s) and the Application Developer is the developer of the smart card software and the application(s). In this case, the role of the Composite Product Integrator is played by (i) the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by (ii) the card manufacturer usually loading some parts of the operating system and the applications into NV-Memories (EEPROM and/or Flash) of the chip.
- Java Card technology-enabled devices: The 'underlying platform' is the Java Card runtime Environment (Java Card RE) on chip and the Platform Developer is the card manufacturer/issuer; the 'application' is the Java Card applet and **may** be developed by the Application Developer. In this case, another role is the Composite Product Integrator who **may** be played by the domain/application service provider or by a trust centre loading the applet and often personalizing the card electronically.

Editors' Note

The Editors do not know to what [21] refers.

13.3.2.4 Actions elements and required information

To allow the evaluation of this Composite Product, the composite evaluation technique identifies two main sets of issues, leading to two sets of rules:

- The Composite Product might be insecure due to gaps in the definition, integration or test of the Platform and Application security mechanisms. In particular, the following properties are to be enforced:
 - The assets to be protected are the final composite product assets defined in a dedicated composite product Security Target;

- The security mechanisms involved in the protection of these assets are those provided by the Platform and by the Application;
- Some of the security mechanisms and security services provided by the Platform **may** require configuration, programming, or activation by the Application;
- Evaluation is performed and validated on the final composite product.

To this effect, the composite evaluation technique defines specific action elements to be performed by the actors involved in the evaluation of the Platform, as well as the evaluation of the Application and Composite Product;

- The aforementioned action elements **may** be impossible to perform due to a lack of information sharing between actors. To avoid this, the composite evaluation technique explicitly defines which information is required for each action element.

Table 2 and Table 3 define which SARs **must** be selected in the Composite Product Security Target, and which information is required to allow a composite evaluation.

Table 2 — Information to be provided to the Application developer

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	Security target of the Platform Information (usually in the form of a guidance or user's manual) related to the platform's security mechanisms and security services that the application has to manage.	Platform developer
Composite design compliance (ADV_COMP)	Information (usually in the form of a guidance or user's manual) related to the platform's security mechanisms and security services that the application has to manage.	Platform developer

Table 3 — Information to be provided to the Composite Product evaluator and evaluation authority

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	Security target of the Platform Information related to the platform's security mechanisms and security services that the application has to manage.	Platform developer
	Security target of the Composite Product	Application developer
Integration of composition parts and consistency check of delivery procedures (ALC_COMP)	Organizational evidence of version correctness, on the basis of configuration lists containing unambiguous version information of the platform and the application having been composed into the final composite product.	Composite Product Integrator
	Organizational evidence that components (Application or Platform) transmitted from an actor to another is securely received, accepted and parameterized.	Composite Product Integrator Platform developer Application developer
Composite design compliance (ADV_COMP)	Platform-related integration recommendations, typically including the user guidance.	Platform developer
	Evidence that the composite product meets the platform-related integration recommendations.	Composite Product Integrator
	Certification Report for the platform	Platform evaluation authority

SAR defining the action elements	Information required	Originator of the information
Composite functional testing (ATE_COMP)	Composite product samples suitable for testing, that allow to load any Application	Composite Product Integrator
Composite vulnerability assessment (AVA_COMP)	Evidence allowing the Composite Product Evaluator and the respective Evaluation Authority to understand the considered attack paths, the performed tests, the effectiveness of countermeasures implemented by the platform, and explanation related to residual vulnerability linked to integration recommendations included in the user guidance.	Platform evaluator
	Certification Report for the platform	Platform evaluation authority

NOTE 1: ~~the mutual recognition of the composite evaluation technique can require refinements of the above rules by Evaluation Authorities and MRAs. In particular, the notion of ETR for composition can be used to clarify the amount and presentation of evidence required (see for example [21] for the domain of smartcards and similar products).~~

Editors' Note

ISO will not accept a reference to an MRA. This note will be removed in the next draft.

NOTE 2: In the case of composition, the term "developer" needs further clarification in order to distinguish the different actor involved. Here, the base TOE developer, the dependent TOE developer and the composite product TOE integrator can be different entities. Similarly, for the terms "evaluator", "evaluation authority (evaluation scheme)" and "validator" further distinguishing of the different entities involved needs to be made.

NOTE 3: In the case where both base and dependent TOEs have already been evaluated, a reduced set of evaluation activities **may** be performed taking into account the evaluation results already obtained from the previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

NOTE 4: The composite product TOE evaluator **may** not need all the detailed results of the base and dependent TOEs evaluations. See subclause 13.4 for more detail on re-using evaluation results.

Editors' Note:

Editors note that the JIL document stated that the detailed evaluation results are NOT needed, but editor observes this is only true in the context of the JIL organization, for other actors the trust level may not be the same.

Note also that part 1 can only refer to evaluation results, and not reference certification since that is a policy outside of the scope of the standard.

EXAMPLE

Smart Card

Smart card architecture is composed of a hardware platform (base TOE) and a software application (dependent TOE). In a Composite TOE evaluation, the platform is already evaluated, the application is evaluated and the results of the platform evaluation are reused. In this case, the platform is the base component, and the application is the dependent component.

The hardware platform has no 'strictly functional' properties related to the security of the composite TOE. It provides functionality supporting the protection of the composite product assets, but the composite product behaviour depends on the software application having to use, configure, and activate these security functions.

Therefore, the hardware platform evaluation results must provide specific security recommendations and conditions for the software application implementation. The composite product evaluation includes examination that the combination of both component TOEs does not lead to any exploitable vulnerability.

A smart card composite evaluation method and associated evaluation activities is developed that includes precise work units with clear statements on the information required from the platform developer and

provides an agreed “framework” for information transfer from the platform evaluator to the composite product evaluator.

The information required is already available from the platform evaluation tasks and no additional work is required from the platform developer.

There are no further requirements for the development class ADV.

The user guidance (AGD) of the platform is considered early in the development of the composite product and provides all of the interfaces on which information is needed.

The development and the evaluation of the composite TOE rely on the proper implementation of the evaluated interfaces of the platform.

The proper use of all relevant interfaces between the platform and the application is in the scope of the composite product evaluation.

Test (ATE) and vulnerability assessment (AVA) are performed on the composite product taking advantage of the available platform evaluation results.

3116

3117 **13.3.3 Composition using packages**

3118 In some cases, PPs can be developed in a modular way using functional packages to define the core
3119 functional elements that are then used as structural elements (building blocks) of PPs.

EXAMPLE

An operating system protection profile has defined “extended packages” to supplement the core operating system protection profile security functional requirements with additional functionality groups for cryptographic service providers, extended I&A, labeled security, integrity verification and others.

3120

Editors’ Note:

3121

This text does not give rise to a composition evaluation approach.

3122

Editors recommend removing it, since packages are now discussed at length in clause 8.

3123

If no comments are received on this, the editors’ proposal will be accepted and presented in the next draft.

3124

13.4 Requirements for evaluations using composition techniques

3125

13.4.1 Re-use of evaluation results

3126

When composing components into an IT product, it is possible that components have already been evaluated and that existing evaluation results could be reused. However, further evaluation of the TOE shall be performed to confirm the security assurance of the entire IT product.

3127

3128

3129

If the evaluation results and evidence for TOE components are not available then they cannot be re-used.

3130

3131

The re-use of evaluation results and evaluation evidence is dependent upon:

3132

- the assurance to be claimed for the TOE;

EXAMPLE 1

the evaluation assurance level.

3133

- the type of composition performed;

3134

- if security properties for the TOE are claimed or not.

EXAMPLE 2

Security properties include, but are not limited to

- Separation;
- Information Flow Control;
- Fault tolerance.

— evaluation scheme policy.

13.4.2 Composition conformance claim

Support Multi-EAL may applicable if the chosen EAL are the higher value.

EXAMPLE

If the highest is EAL4, it may also comply with EAL1 till EAL3, where the SARs aspects of evaluation are varying through type of EAL being chosen, whilst the components such as SPD, SO, SOOE, SFRs are still applicable for the lower EAL from the recommended PP EAL.

Yet, if the EAL chosen for evaluation are lower the stated EAL in the Base-PP, some mapping requires under Rational Section of the PP, whilst describing the applicability of lower EAL than stated from the aspects of Risk Analysis, Threat Mitigations, Evaluation Criteria in ATE+AVA and etc.

13.4.3 Composition rationale

When composing an IT product from components, a composition rationale shall be provided. This includes analyses of the:

- a) composition type (or types);
- b) interfaces and dependencies of the functions;
- c) composability of the security function policies, and organizational security policies;
- d) preservation of security properties;
- e) for the embedded type of composition, aspects of correctness.

13.4.3.1 Use of the ACO class

Part 3 of this standard, describes the ACO class which provides security assurance components that **may** be used in support of the evaluation of composed TOEs.

Part 5 of this standard, provides a family of pre-defined assurance packages for composition which provide packages (composed assurance packages (CAP)) which balance the level of assurance obtained with the cost and feasibility of acquiring such assurance for composed TOEs.

NOTE the composed assurance packages are designed to provide assurance that the composition was performed to a specified rigour, and do not imply any evaluation assurance level for the composed IT product.

13.4.3.2 Vulnerability analysis

The composed IT product shall have a vulnerability analysis, in accordance with the AVA class, performed on the composed IT product at a level commensurate with the required security assurance for the composed IT product. The vulnerability analysis is more difficult when security properties are claimed.

The vulnerability analysis shall be designed in consideration of the composition analysis.

13.4.3.3 Testing

Additional testing, using the ATE and IND classes given in ISO/IEC 15408-3, of the composed product shall be performed. It **may** be possible to re-use the testing evaluation results from the components, but additional tests for the composed product shall be designed and performed.

The testing shall be designed in consideration of the composition analysis.

Annex A (informative)

Specification of Security Targets and Direct Rationale STs

Editors' Note:

The 2018 Directives have clarified the normative/informative status of Annexes

Note that informative annexes may contain **optional** requirements, however the main clauses would then describe in which case the option could be taken.

This Annex is informative. The various requirements and permissions appearing in this annex,

Either need to be moved in the corresponding normative clauses of 15408-1, -2 or -3;

or the verbal form needs to be changed.

The verbal forms used by ISO are very specific.

— Requirement: shall or shall not

— Recommendation: should or should not

— Permission: may or may not

— Possibility and capability: can or cannot

— External constraint: "must"

Additionally, we should consider verifying that any requirements, recommendations, and permissions are actually present as SARs or CEM activities.

More information on verbal forms and the annex statuses are found in the latest directives at:

<http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype>

A.1 Goal and structure of this Annex

The goal of this annex is to explain the Security Target (ST) concept and is supported by the documents given in the bibliography.

NOTE This annex does not define the ST evaluation criteria requirements which are found in the ASE class in ISO/IEC 15408-3.

This annex consists of four major parts:

- How an ST **should be** used.* This is summarized in A.2 and A.3. These sections describe how an ST **should be** used, and some of the questions that can be answered with an ST.
- What an ST **must** contain.* This is summarized in A.4 and is described in more detail in A.5 - A.11. These sections describe the mandatory contents of the ST, the interrelationships between these contents, and provide examples.
- Claiming conformance with standards.* A.12 describes how an ST writer **can** claim that the TOE meets a particular standard.
- Direct Rationale STs.* Direct Rationale STs are STs in which the SPD-elements are mapped directly to the SFRs, and possibly to Security Objectives for the operational environment. A.4 through A.12 are applicable to Direct Rationale STs with the differences given in A.13.

A.2 Using an ST

A.2.1 How an ST **should be** used

A typical ST fulfils two roles:

- Before and during the evaluation, the ST specifies “what is to be evaluated”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role. A.7 describes how the ST is used in this role.
- After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumer **can** rely on this description because the TOE has been evaluated to meet the ST. Ease of use and understandability are major issues for this role. A.11 describes how the ST is used in this role.

A.2.2 How an ST **should not** be used

One role, among many, that an ST **should not** fulfil is:

- *a complete specification*: An ST is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size, and weight, required voltage etc. **should not** be part of an ST. This means that in general an ST **may** be a part of a complete specification, but not a complete specification itself.

A.3 Questions that **can** be answered with an ST

After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST **can** therefore answer the following questions (and more):

- a) *How can I find the ST/TOE that I need given the multitude of existing STs/TOEs?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;
- b) *Does this TOE fit in with my existing IT-infrastructure?* This question is addressed by the TOE overview, which identifies the major hardware/firmware/software elements needed to run the TOE;
- c) *Does this TOE fit in with my existing operational environment?* This question is addressed by the Security Objectives for the operational environment, which identifies all constraints the TOE places on the operational environment in order to function;
- d) *What does the TOE do (interested reader)?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;
- e) *What does the TOE do (potential consumer)?* This question is addressed by the TOE description, which gives a less brief (several pages) summary of the TOE;
- f) *What does the TOE do (technical)?* This question is addressed by the TOE summary specification which provides a high-level description of the mechanisms the TOE uses;
- g) *What does the TOE do (expert)?* This question is addressed by the SFRs which provide an abstract highly technical description, and the TOE summary specification which provide additional detail;
- h) *Does the TOE address the problem as defined by my government/organization?* If your government/organization has defined packages and/or PPs to define this solution, then the answer can be found in the Conformance Claims section of the ST, which lists all packages and PPs that the ST conforms to;
- i) *Does the TOE address my security problem (expert)?* What are the threats countered by the TOE? What organizational security policies does it enforce? What assumptions does it make about the operational environment? These questions are addressed by the security problem definition;
- j) *How much trust can I place in the TOE?* This can be found in the SARs in the security requirements section, which provide the assurance requirements that were used to evaluate the TOE, and hence the trust that the evaluation provides in the correctness of the TOE.

A.4 Mandatory contents of an ST

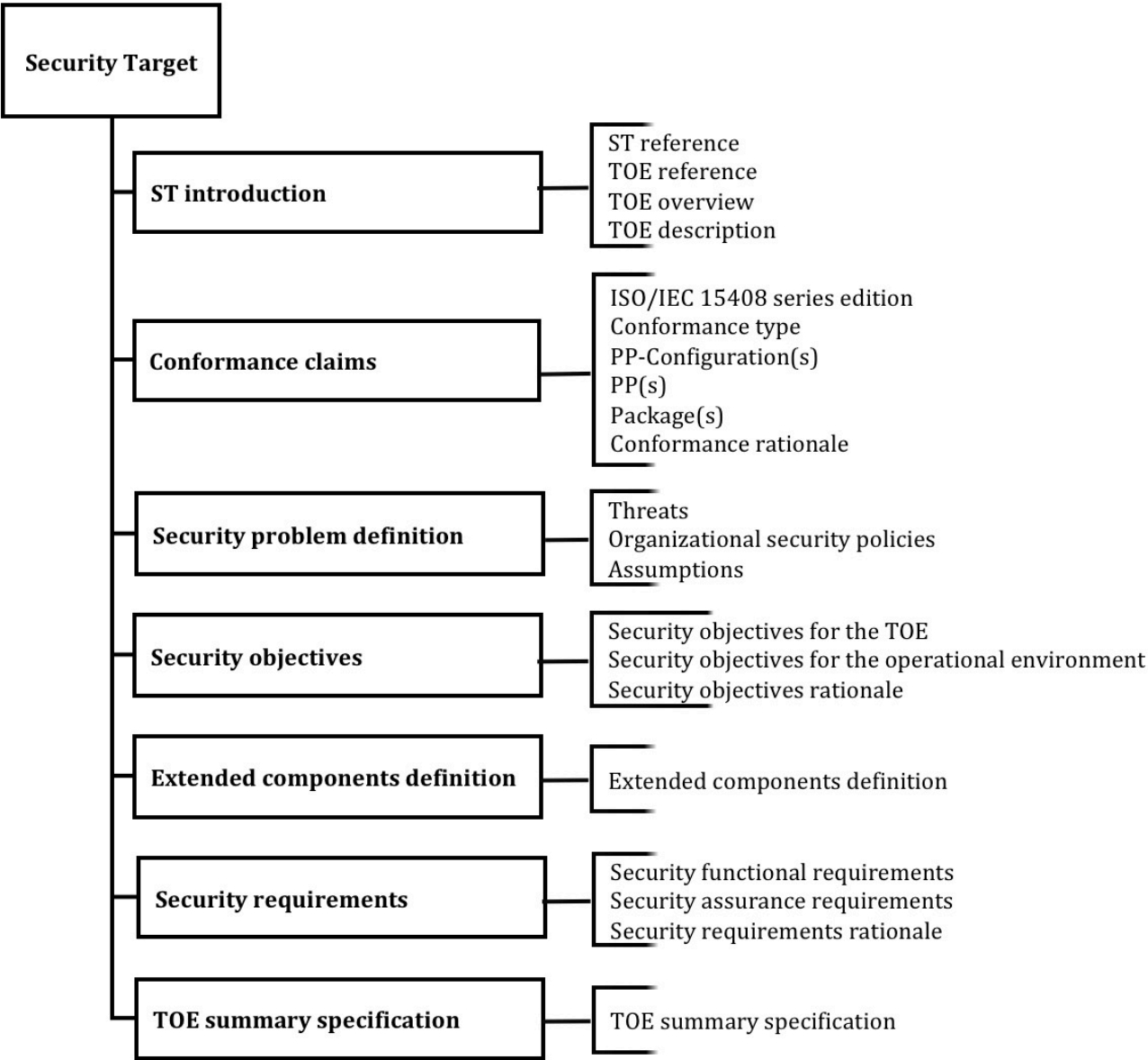
There are two types of ST. Firstly the “regular” ST which is an ST that contains the full contents as described in A.5 through A.12. Secondly, in some cases an ST author can use a Direct Rationale ST which has different contents compared to STs that contain Security Objectives for the TOE. Direct Rationale STs, and the reasons and circumstances in which they are used are described in detail in A.13 All other parts of this Annex assume an ST with full contents.

Figure A.1 — Contents of an ST, portrays the-contents of an ST that are given in ISO/IEC 15408- 3. Figure A.1 **can** also be used as a structural outline of the ST, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the ST instead of in the security requirements section. The separate sections of an ST and the contents of those sections are briefly summarized below and explained in much more detail in A.5 to A.12. An ST **normally** contains:

NOTE In Direct Rationale STs no Security Objectives for the TOE are included: See A.4.9.

- a) *an ST introduction* containing three narrative descriptions of the TOE on different levels of abstraction;
- b) *a conformance claim*, stating the ST’s conformance to 15408-2 and 15408-3; showing whether the ST claims conformance to any PPs, PP-Configurations, and/or packages; and if so identifying the specific PPs, PP-Configurations, and/or packages, and the type of conformance claimed;
- c) *a security problem definition*, showing threats, OSPs and assumptions;
- d) *Security Objectives*, showing how the solution to the security problem is divided between Security Objectives for the TOE and Security Objectives for the operational environment of the TOE;
- e) *extended components definitions* (optional), where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) **may** be defined. These new components are needed to define extended functional and extended assurance requirements;
- f) *security requirements*, where a translation of the Security Objectives for the TOE into a standardized language is provided. This standardized language is in the form of SFRs. Additionally, this section defines the SARs;

3283 g) a TOE summary specification, showing how the SFRs are implemented in the TOE.



3284 **Figure A.1 — Contents of an ST**

3285 **A.4.1 ST Introduction (ASE_INT)**

3286 The ST introduction describes the TOE in a narrative way on three levels of abstraction:

- 3287 a) the ST reference and the TOE reference, which provide identification material for the ST and the
- 3288 TOE that the ST refers to;
- 3289 b) the TOE overview, which briefly describes the TOE;
- 3290 c) the TOE description, which describes the TOE in more detail.

3291 **A.4.1.1 ST reference and TOE reference**

3292 The ST reference and the TOE reference facilitate indexing and referencing the ST and TOE and their

3293 inclusion in catalogues.

3294 An ST contains a clear ST reference that identifies that particular ST. A typical ST reference consists of

3295 title, version, sponsors, and publication date.

3296 NOTE Here a distinction is made between the sponsor of an ST, i.e. the entity responsible for its development,

3297 and the author of an ST which is the entity responsible for its production.

EXAMPLE 1

An example of an ST reference is “MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2017”.

3298 An ST also contains a TOE reference that identifies the TOE that claims conformance to the ST. A typical
 3299 TOE reference consists of developer name, TOE name and TOE version number. As a single TOE **may** be
 3300 evaluated multiple times, for instance by different consumers of that TOE, and therefore have multiple
 3301 STs, this reference **may** not be unique.

EXAMPLE 2

An example of a TOE reference is “MauveCorp MauveRAM Database v5.12”.

3302 If the TOE is constructed from one or more well-known products, it is allowed to reflect this in the TOE
 3303 reference, by referring to the product name(s). However, this **should** not be used to mislead consumers:
 3304 situations where major parts or security functionalities were not considered in the evaluation, yet the
 3305 TOE reference does not reflect this are not allowed.

3306 **A.4.1.2 TOE overview**

3307 The TOE overview is aimed at potential consumers of a TOE who are looking through catalogs of
 3308 evaluated TOEs/Products to find TOEs that **may can** meet their security needs, and are supported by
 3309 their hardware, software, and firmware. The typical length of a TOE overview is several paragraphs.

3310 To this end, the TOE overview briefly describes the usage of the TOE and its major security features,
 3311 identifies the TOE type, and identifies any major non-TOE hardware/software/firmware required by
 3312 the TOE.

3313 **A.4.1.2.1 Usage and major security features of a TOE**

3314 The description of the usage and major security features of the TOE is intended to give a very general
 3315 idea of what the TOE is capable of in terms of security, and what it can be used for in a security context.
 3316 This section **should be** is written for (potential) TOE consumers, describing TOE usage and major
 3317 security features in terms of business operations, using language that TOE consumers understand.

EXAMPLE

“The MauveCorp MauveRAM Database v5.12 is a multi-user database intended to be used in a networked environment. It allows 1024 users to be active simultaneously. It allows password/token and biometric authentication, protects against accidental data corruption, and **can** roll-back ten thousand transactions. Its audit features are highly configurable, so as to allow detailed audit to be performed for some users and transactions, while protecting the privacy of other users and transactions.”

3318 **A.4.1.2.2 TOE type**

3319 The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smart card, crypto-
 3320 modem, intranet, web server, database, web server and database, LAN, LAN with web server and
 3321 database, etc.

3322 It **may can** be the case that the TOE is not of a readily available type, in which case “none” would be
 3323 acceptable.

3324 In some cases, a TOE type **can** mislead consumers. This is to be avoided by ST authors.

EXAMPLE

Examples of misleading TOE types include:

- certain functionality **can** be expected of the TOE because of its TOE type, but the TOE does not have this functionality. Examples include:

- an ATM-card type TOE, which does not support any identification/authentication functionality;
- a firewall type TOE, which does not support protocols that are almost universally used;
- a PKI-type TOE, which has no certificate revocation functionality.
- the TOE **can** be expected to operate in certain operational environments because of its TOE type, but it **cannot** do so.
 - a PC-operating system type TOE, which is unable to function securely unless the PC has no network connection, floppy drive, and CD/DVD-player;
 - a firewall, which is unable to function securely unless all users that **can** connect through that firewall are benign.

A.4.1.2.3 Required non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify such non-TOE hardware, software and/or firmware. A complete and fully detailed identification of the additional hardware, software and/or firmware is not necessary, but the identification **should-must** be complete and detailed enough for potential consumers to determine the major hardware, software and/or firmware needed to use the TOE.

EXAMPLE

Example hardware/software/firmware identifications are:

- a standard PC with a dual core 2.10 GHz or faster processor and 4GB or more RAM, running the Yaiza operating system for professionals, version 53.0 Update 6b, c, or 7, or version 54.0;
- a standard 64-bit server with a 2xQuad-Core core processor and 16GB or more RAM, running the Yaiza operating system, server edition version 7.0 Update 6d, and the WonderMagic 12.0 Graphics card with the 1.0 WM Driver Set;
- a CleverCard SB17067 integrated circuit;
- a CleverCard SB17067 integrated circuit running v12.0 of the QuickOS smart card operating system;
- the December 2019 installation of the LAN of the Director-General's Office of the Department of Traffic.

A.4.1.3 TOE description

A TOE description is a narrative description of the TOE, likely to run to several pages. The TOE description **should** provides evaluators and potential consumers with a general understanding of the security capabilities of the TOE, in more detail than was provided in the TOE overview. The TOE description **may can** also be used to describe the wider application context into which the TOE will fit.

The TOE description discusses the physical scope of the TOE: a list of all hardware, firmware, software, and guidance parts that constitute the TOE. This list **should-must** be described at a level of detail that is sufficient to give the reader a general understanding of those parts.

The TOE description **should-must** also discuss the logical scope of the TOE, including the major TOE functions and provide a brief description of the security features of the TSF in the context of these functional features. The description provided **should-must be** at a level of detail that is sufficient to give the reader a general understanding of those features. This description is expected to be in more detail than the major security features described in the TOE overview.

An important property of the physical and logical scopes is that they describe the TOE in such a way that there remains no doubt on whether a certain part or feature is in the TOE or whether this part or feature is outside the TOE. This is especially important when the TOE is integrated with and **cannot** be easily separated from non-TOE entities.

EXAMPLE

Examples where the TOE is integrated with non-TOE entities are:

- the TOE is a cryptographic co-processor of a smart card IC, instead of the entire IC;
- the TOE is a smart card IC, except for the cryptographic processor;
- the TOE is the Network Address Translation part of the MinuteGap Firewall v28.2.

Editors' Note:

The following text was included in response to WD2 SE/JJ2:

Evaluation at EAL 4 and higher is often impossible when third party components need to be present in the TOE. Access to source code is mandatory at EAL 4+ and many component vendors does not share source code with the component integrators or the evaluators.

Most schemes accept that compiler libraries, operating systems, and processors in the operational environment are implicitly involved in executing TOE source code.

The implementation representation for Windows or the microprocessors performing the TSF functionality is most likely not available during an evaluation.

Some schemes accept that validated crypto modules are used by the TOE, where the source code is not available during the CC evaluation at EAL 4+, and where cryptographic SFRs are executed by the crypto module.

Since a third-party component where source code is unavailable would have a well-defined interface (boundary) it is feasible to separate the functionality of the TOE and of the module. Here the TOE is responsible for using correct syntax while calling the intended functionality (this is what should be part of the TOE evaluation), while the third-party component is responsible for performing the functions called by the TOE and is placed in the environment.”

When third-party components, providing security functionality upon which the TOE depends but for which sufficient evidence is not available for evaluation, are specified to be in the TOE's operational environment the TOE description **should must** include a description of the third-party components and how they are used. Such third-party components **should can** be either very well known (OS), evaluated in conformance with the ISO/IEC 15408 series, or tested by a party with sufficiently good standing (specific requirements TBD).

EXAMPLE

An example of where sufficient evidence for evaluation is not available from third-parties includes when source code **cannot** be made available to the developer of the TOE.

A.4.2 Conformance claims (ASE_CCL)

This section of an ST describes how the ST conforms with:

- The edition of the ISO/IEC 15408 series used;
- ISO/IEC 15408-2 and ISO/IEC 15408-3;
- Protection Profiles (if any);
- PP-Configuration(s) (if any);
- Packages (if any).

The description of how the ST conforms to The ISO/IEC 15408 series consists of two items: the edition of ISO/IEC 15408 that is used and whether the ST contains extended security requirements or not (see 11.2. and A.4.5).

The description of conformance claimed by the ST to Protection Profiles and PP-Configurations means that the ST lists the PPs, and any PP-Configurations to which conformance is being claimed to. The type of conformance being claimed is also identified. For an explanation of this, see 11.2.

NOTE In the exact conformance scenario, an ST ~~can~~ conforms to only one PP-Configuration.

The description of conformance of the ST to packages means that the ST lists the packages to which conformance is being claimed. For an explanation of this, see 11.2.

A.4.3 Security problem definition (ASE_SPD)

A.4.3.1 Introduction

The security problem definition defines the security problem that is to be addressed. The security problem definition is, as far as ISO/IEC 15408 is concerned, axiomatic. That is, the process of deriving the security problem definition falls outside the scope of ISO/IEC 15408.

NOTE 1 The usefulness of the results of an evaluation strongly depends on the ST, and the usefulness of the ST strongly depends on the quality of the security problem definition. It is therefore often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good security problem definition.

NOTE 2 According to ISO/IEC 15408-3 it is not mandatory to have statements in all sections, an ST with threats does not need to have OSPs and vice versa. Also, any ST ~~may~~ could omit assumptions.

NOTE 3 Where the TOE is physically distributed, it ~~can~~ be better to discuss the relevant threats, OSPs and assumptions separately for distinct domains of the TOE operational environment.

A.4.3.2 Threats

This section of the security problem definition shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

A threat consists of an adverse action performed by a threat agent on an asset.

Adverse actions are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value.

Threat agents ~~may~~ can be described as individual entities, but in some cases, it ~~may~~ can be better to describe them as types of entities, groups of entities etc.

EXAMPLE

Examples of threat agents are hackers, users, computer processes, and accidents. Threat agents ~~may~~ can be further described by attributes such as expertise, resources, opportunity, and motivation.

Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network;
- a worm seriously degrading the performance of a wide-area network;
- a system administrator violating user privacy;
- someone on the Internet listening in on confidential electronic communication.

A.4.3.3 Organizational security policies (OSP)

This section of the security problem definition shows the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

OSP are security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organization in the operational environment. OSPs ~~may~~ can be made by an organization controlling the operational environment of the TOE, or they ~~may~~ can be made by legislative or regulatory bodies. OSPs ~~can~~ apply to the TOE and/or the operational environment of the TOE.

EXAMPLE

Examples of OSPs are:

- All products that are used by the Government **must** conform to the National Standard for password generation and encryption;
- Only users with System Administrator privilege and clearance of Department Secret **shall** be allowed to manage the Department Fileserver.

3416 A.4.3.4 Assumptions

3417 This section of the security problem definition shows the assumptions that are made on the operational
3418 environment in order to be able to provide security functionality. If the TOE is placed in an operational
3419 environment that does not meet these assumptions, the TOE **may could** not be able to provide all of its
3420 security functionality anymore. Assumptions can be on physical, personnel and connectivity of the
3421 operational environment.

EXAMPLE

Examples of assumptions are:

- Assumptions on physical aspects of the operational environment:
 - It is assumed that the TOE will be placed in a room that is designed to minimize electromagnetic emanations;
 - It is assumed that the administrator consoles of the TOE will be placed in a restricted access area.
- Assumptions on personnel aspects of the operational environment:
 - It is assumed that users of the TOE will be trained sufficiently in order to operate the TOE;
 - It is assumed that users of the TOE are approved for information that is classified as National Secret;
 - It is assumed that users of the TOE will not write down their passwords.
- Assumptions on connectivity aspects of the operational environment:
 - It is assumed that a PC workstation with at least 10GB of disk space is available to run the TOE on;
 - It is assumed that the TOE is the only non-OS application running on this workstation;
 - It is assumed that the TOE will not be connected to an untrusted network.

3422 NOTE During an evaluation these assumptions are considered to be true: they are not tested in any way. For
3423 these reasons, assumptions **can** only be made on the operational environment. Assumptions **can** never be made on
3424 the behaviour of the TOE because an evaluation consists of evaluating assertions made about the TOE and not by
3425 assuming that assertions on the TOE are true.

3426 A.4.4 Security objectives (ASE_OB)

3427 A.4.4.1 General

3428 The Security Objectives are a concise and abstract statement of the intended solution to the problem
3429 defined by the security problem definition. The role of the Security Objectives is threefold:

- provide a high-level, natural language solution of the problem;
- divide this solution into two part-wise solutions, that reflect that different entities each have to address a part of the problem;
- demonstrate that these part-wise solutions form a complete solution to the problem.

A.4.4.2 High-level solution

The Security Objectives consist of a set of short and clear statements without overly much detail that together form a high-level solution to the security problem. The level of abstraction of the Security Objectives aims at being clear and understandable to knowledgeable potential consumers of the TOE. The Security Objectives are in natural language.

A.4.4.3 Part-wise solutions

In an ST the high-level security solution, as described by the Security Objectives, is divided into two part-wise solutions. These part-wise solutions are called the Security Objectives for the TOE and the Security Objectives for the operational environment. This reflects that these part-wise solutions are to be provided by two different entities: the TOE, and the operational environment.

A.4.4.3.1 Security objectives for the TOE

The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This part-wise solution is called the Security Objectives for the TOE and consists of a set of objectives that the TOE ~~should~~ **must** achieve in order to solve its part of the problem.

NOTE In Direct Rationale STs Security Objectives for the TOE are not included: See A.4.9.

EXAMPLE

Examples of Security Objectives for the TOE are:

- The TOE **shall** keep confidential the content of all files transmitted between it and a Server;
- The TOE **shall** identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE;
- The TOE **shall** restrict user access to data according to the Data Access policy described in Annex 3 of the ST.

If the TOE is physically distributed, it ~~may~~ **can** be better to subdivide the ST section containing the Security Objectives for the TOE into several subsections to reflect this.

A.4.4.3.2 Security objectives for the operational environment

The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the Security Objectives for the TOE). This pair-wise solution is called the Security Objectives for the operational environment and consists of a set of statements describing the goals that the operational environment ~~should~~ **must** achieve.

EXAMPLE

Examples of Security Objectives for the operational environment are:

- The operational environment **shall** provide a workstation with the OS Inux version 3.01b to execute the TOE on;
- The operational environment **shall** ensure that all human TOE users receive appropriate training before allowing them to work with the TOE;
- The operational environment of the TOE **shall** restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel;
- The operational environment **shall** ensure the confidentiality of the audit logs generated by the TOE before sending them to the central Audit Server.

If the operational environment of the TOE consists of multiple physical sites, each with different properties, it ~~could~~ ~~may~~ be better to subdivide the ST section containing the Security Objectives for the operational environment into several sub-sections to reflect this.

Editors' Note:

The following text was included in response to WD2 SE/JJ2

Third party components that **cannot** be evaluated due to unavailability of evaluation evidence are included in the operational environment, and the Security Objectives for the operational environment **must** include that the third-party component works as intended.

A.4.4.4 Relation between Security Objectives and the security problem definition

The ST also contains a Security Objectives rationale containing two sections:

- a tracing that shows which Security Objectives address which SPD-elements (threats, OSPs and assumptions);
- a set of justifications that shows that all SPD-elements are effectively addressed by the Security Objectives.

NOTE In Direct Rationale STs a Security Objectives Rationale is not included: See A.4.9.

EXAMPLE

A threat “T17: Threat agent X reads the Confidential Information in transit between A and B”, a security objective for the TOE: “OT12: The TOE **shall** ensure that all information transmitted between A and B is kept confidential”, and a demonstration “T17 is directly countered by OT12”.

A.4.4.4.1 Tracing between Security Objectives and the security problem definition

The tracing shows how the Security Objectives trace back to the threats, OSPs and assumptions as described in the security problem definition (SPD).

- a) *No spurious objectives*: Each security objective traces to at least one SPD-element (threat, OSP or assumption).
- b) *Complete with respect to the security problem definition*: Each SPD-element has at least one security objective tracing to it.
- c) *Correct tracing*: Since assumptions are always made by the TOE on the operational environment, Security Objectives for the TOE do not trace back to assumptions. The tracings allowed by ISO/IEC 15408-3 are depicted in Figure A.2.

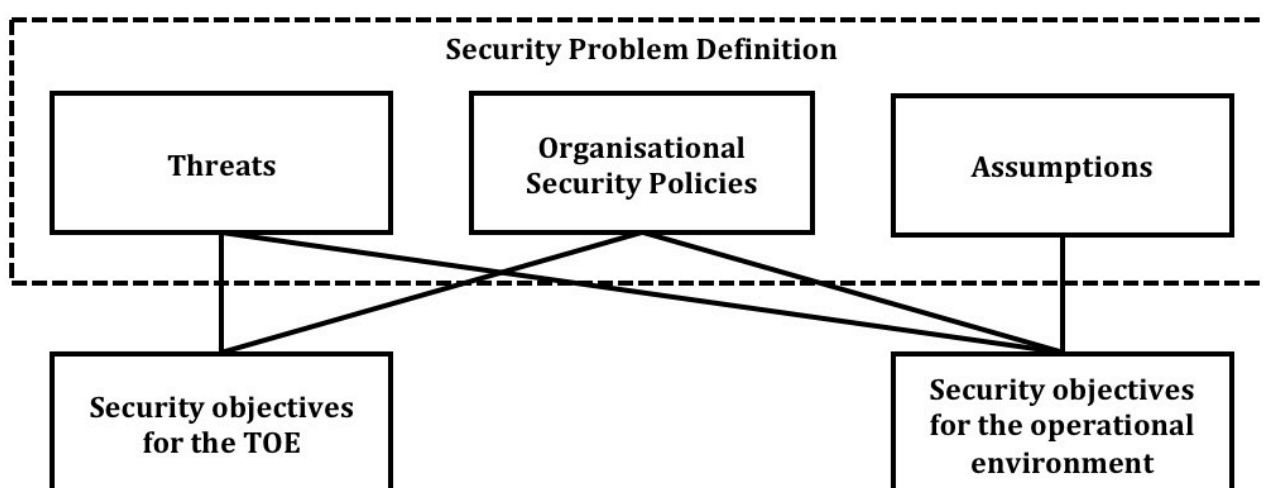


Figure A.2 — Tracings between Security Objectives and the SPD

Multiple Security Objectives **may can** trace to the same threat, indicating that the combination of those Security Objectives counters that threat. A similar argument holds for OSPs and assumptions.

A.4.4.4.2 Providing a justification for the tracing

The Security Objectives rationale also demonstrates that the tracing is effective: All the given threats, OSPs and assumption are addressed (i.e. countered, enforced, and upheld respectively) if all Security Objectives tracing to a particular threat, OSP or assumption are achieved.

This demonstration analyses the effect of achieving the relevant Security Objectives on countering the threats, enforcing the OSPs and upholding the assumptions and leads to the conclusion that this is indeed the case.

In some cases, where parts of the SPD very closely resemble some Security Objectives, the demonstration **can** be much simpler.

A.4.4.4.3 On countering threats

Countering a threat does not necessarily mean removing that threat, it **can** also mean sufficiently diminishing that threat or sufficiently mitigating that threat.

EXAMPLE

Examples of removing a threat are:

- removing the ability to execute the adverse action from the threat agent;
- moving, changing, or protecting the asset in such a way that the adverse action is no longer applicable to it;
- removing the threat agent;
EXAMPLE removing machines from a network that frequently crash that network.

Examples of diminishing a threat are:

- restricting the ability of a threat agent to perform adverse actions;
- restricting the opportunity to execute an adverse action of a threat agent;
- reducing the likelihood of an executed adverse action being successful;
- reducing the motivation to execute an adverse action of a threat agent by deterrence;
- requiring greater expertise or greater resources from the threat agent.

Examples of mitigating the effects of a threat are:

- making frequent back-ups of the asset;
- obtaining spare copies of an asset;
- insuring an asset;
- ensuring that successful adverse actions are always timely detected, so that appropriate action **can** be taken.

A.4.4.5 Security Objectives: conclusion

Based on the Security Objectives and the Security Objectives rationale, the following conclusion **can** be drawn: if all Security Objectives are achieved then the security problem as defined in Security problem definition (ASE_SPD) is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

A.4.5 Extended Components Definition (ASE_ECD)

In many cases the security requirements in an ST are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3, see A.4.6. However, in some cases, there **may** **might** be requirements in an ST that

are not based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3. In these cases, new components, i.e. extended components, **must** be defined, and the definition ~~should be~~ provided in the Extended Components Definition section of the ST. For more information on this, see D.4

NOTE This section of an ST is intended to contain only the extended components and not the extended requirements which are based on the extended components. The extended requirements ~~should can~~ be included in the security requirements section of the ST as described in A.4.6 and are then for all purposes treated identically to the requirements that are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3.

A.4.6 Security requirements (ASE_REQ)

A.4.6.1 General

The security requirements consist of two groups of requirements:

- a) *the security functional requirements* (SFRs): a translation of the Security Objectives for the TOE into a standardized language;
- b) *the security assurance requirements* (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

These two groups are discussed in the following two subclauses:

A.4.6.2 Security functional requirements (SFRs)

The SFRs are a translation of the Security Objectives for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the Security Objectives **must** be completely addressed) and be independent of any specific technical solution (implementation). ISO/IEC 15408 requires this translation into a standardized language for several reasons:

- to provide an exact description of what is to be evaluated. As Security Objectives for the TOE are usually formulated in natural language, translation into a standardized language enforces a more exact description of the functionality of the TOE.
- to allow comparison between two STs. As different ST authors ~~may can~~ use different terminology in describing their Security Objectives, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

There is no translation required in ISO/IEC 15408 for the Security Objectives for the operational environment, because the operational environment is not evaluated and does therefore not require a description aimed at its evaluation. See the bibliography for items relevant to the security assessment of operational systems.

It ~~may can~~ be the case that parts of the operational environment are evaluated in another evaluation, but this is out of scope for the current evaluation.

EXAMPLE

An OS TOE **may** require a firewall to be present in its operational environment. Another evaluation **may** subsequently evaluate the firewall, but this evaluation has nothing to do with the evaluation of the OS TOE.

Editors' Note:

The following text is included in response to WD2 SE/JJ2

When third-party components are included in the operational environment as described in A.4.1.3:

- The functionality, where the third-party component is involved, is represented by SFRs in the PP/ST, and will be tested during the evaluation.
- Application notes **can** be provided in the ST for SFRs partly implemented in a third-party component.
- Internal design review, source code review, and testing of the internal interfaces of the third-party component is not performed.

A.4.6.2.1 How ISO/IEC 15408 supports this translation

ISO/IEC 15408(all parts) supports this translation in three ways:

- a) by providing a pre-defined precise “language” designed to describe exactly what is to be evaluated. This language is defined as a set of components defined in ISO/IEC 15408-2. The use of this language as a well-defined translation of the Security Objectives for the TOE to SFRs is mandatory, though some exceptions exist and are given in 7.4.
- b) by providing operations: mechanisms that allow the ST writer to modify the SFRs to provide a more accurate translation of the Security Objectives for the TOE. This document defines the four allowed operations: assignment, selection, iteration, and refinement. These are described further in 7.2.
- c) by providing dependencies: a mechanism that supports a more complete translation to SFRs. In ISO/IEC 15408-2 language, an SFR **can** have a dependency on other SFRs. This signifies that if an ST uses that SFR, it generally needs to use those other SFRs as well. This makes it much harder for the ST writer to overlook including necessary SFRs and thereby improves the completeness of the ST. Dependencies are described further in 7.3.

A.4.6.2.2 Relation between SFRs and Security Objectives

The ST also contains a security requirements rationale, consisting of two sections about SFRs:

- a tracing that shows which SFRs address which Security Objectives for the TOE;
- a set of justifications that shows that all Security Objectives for the TOE are effectively addressed by the SFRs.

A.4.6.2.2.1 Tracing between SFRs and the Security Objectives for the TOE

The tracing shows how the SFRs trace back to the Security Objectives for the TOE as follows:

- a) *No spurious SFRs*: Each SFR traces back to at least one security objective.
- b) *Complete with respect to the Security Objectives for the TOE*: Each security objective for the TOE has at least one SFR tracing to it.

Multiple SFRs **may can** trace to the same security objective for the TOE, indicating that the combination of those security requirements meets that security objective for the TOE.

A.4.6.2.2.2 Providing a justification for the tracing

The security requirements rationale demonstrates that the tracing is effective: if all SFRs tracing to a particular security objective for the TOE are satisfied, that security objective for the TOE is achieved.

This demonstration analyses the effects of satisfying the relevant SFRs on achieving the security objective for the TOE and lead to the conclusion that this is indeed the case.

In cases where SFRs very closely resemble Security Objectives for the TOE, the demonstration **can** be much simpler.

A.4.6.3 Security assurance requirements (SARs)

The SARs are a description of how the TOE is to be evaluated. This description uses a standardized language for two reasons:

- to provide an exact description of how the TOE is to be evaluated. Using a standardized language assists in creating an exact description and avoids ambiguity.
- to allow comparison between two STs. As different ST authors **may could** use different terminology in describing the evaluation, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

This standardized language is defined as a set of components defined in ISO/IEC 15408-3. The use of this language is mandatory, though some exceptions exist. ISO/IEC 15408 enhances this language in two ways:

- a) by providing operations: mechanisms that allow the ST writer to modify the SARs. ISO/IEC 15408 has four operations: assignment, selection, iteration, and refinement. These are described further in 7.2.
- b) by providing dependencies: a mechanism that supports a more complete translation to SARs. In ISO/IEC 15408-3 language, an SAR **can** have a dependency on other SARs. This signifies that if an ST uses that SAR, it generally needs to use those other SARs as well. This makes it much harder for the ST writer to overlook including necessary SARs and thereby improves the completeness of STs. Dependencies are described further in 7.3.

Editors' Note:

The following text is included in response to WD2 SE/JJ2

When third-party components are included in the operational environment as described in A.4.1.3:

- some assurance components from the ADV class given in ISO/IEC 15408-3 **cannot** be evaluated due to insufficient evidence.

EXAMPLE

Examples of the ADV components that **may** not be evaluable for third-party provided TOE components include ADV_IMP.1, ADV_INT.2, ADV_SPM.1 and ADV_TDS.3

- components of AVA_VAN.3 and above also **cannot** be evaluated.

A.4.6.3.1 SARs and the security requirement rationale

The ST also contains a security requirements rationale that explains why the chosen set of SARs was deemed appropriate. There are no specific requirements for this explanation. The goal for this explanation is to allow the ST readers to understand the reasons why this particular set was chosen.

SARs contribute to the confidence that a risk owner **can** place in an evaluation. Many SARs given in ISO/IEC 15408-3 relate to the design and development processes used in the implementation of a TOE by a developer. Some SARs relate to an operational TOE such as secure delivery process and flaw remediation.

EXAMPLE

An example of an inconsistency in the selection of SARs is if the security problem definition mentions threats where the threat agent is very capable, and a low (or no) vulnerability analysis (AVA_VAN) is included in the SARs.

A.4.6.4 Security requirements: conclusion

In the Security Problem Definition section of the ST, the security problem is defined as consisting of threats, OSPs and assumptions. In the Security Objectives section of the ST, the solution is provided in the form of two sub-solutions:

- Security Objectives for the TOE;
- Security Objectives for the operational environment.

Additionally, a Security Objectives rationale is provided showing that if all Security Objectives are achieved, the security problem is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

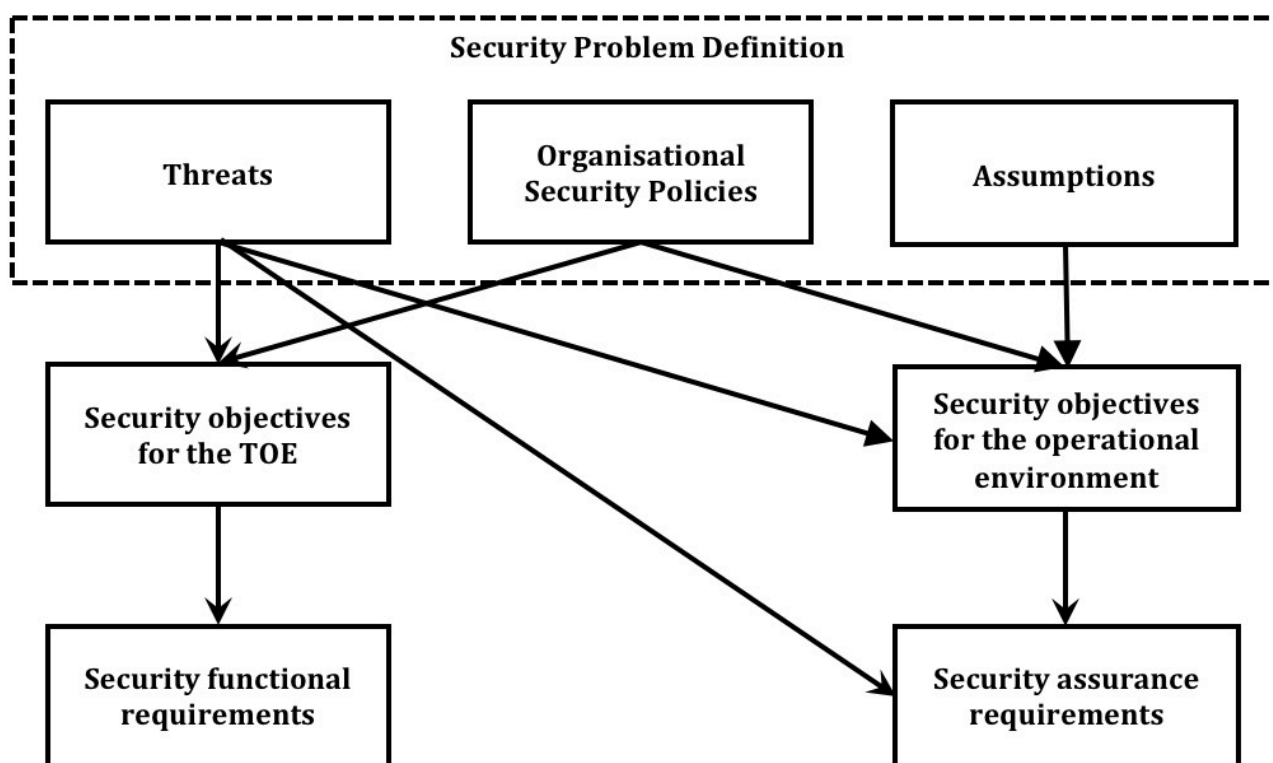


Figure A.3 — Relations between the SPD, the Security Objectives, and the security requirements

In the security requirements section of the ST, the Security Objectives for the TOE are translated to SFRs and a security requirements rationale is provided showing that if all SFRs are satisfied, all Security Objectives for the TOE are achieved.

Additionally, a set of SARs is provided to show how the TOE is evaluated, together with an explanation for selecting these SARs.

All of the above **can** be combined into the statement: If all SFRs and SARs are satisfied and all Security Objectives for the operational environment are achieved, then there exists assurance that the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld. This is illustrated in Figure A.3.

The amount of assurance obtained is defined by the SARs, and whether this amount of assurance is sufficient to risk-owners using the ST is described in the explanation given for choosing these SARs.

A.4.7 TOE summary specification (ASE_TSS)

The objective for the TOE summary specification (TSS) is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification **should** provides the general technical mechanisms that the TOE uses for this purpose. The level of detail of this description **should-must** be sufficient to enable potential consumers to understand the general form and implementation of the TOE.

The statement of security requirements includes a natural language description, part of which describes how the SFRs combine together to provide security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

EXAMPLE 1:

The following are examples of internal features:

- Unavailability of residual data upon reallocation of a resource;
- Hidden failure conditions of login/password-authentication;
- Hidden biometric comparison score.

EXAMPLE 2:

If the TOE is an Internet PC and the SFRs contain FIA_UAU.1 to specify authentication, the TOE summary specification **should** indicate how this authentication is done: password, token, iris scanning etc. More information, like applicable standards that the TOE uses to meet SFRs, or more detailed descriptions **may** also be provided.

A.4.8 Referring to other standards in an ST

In some cases, an ST writer **may needs** to refer to an external standard, such as a particular cryptographic standard or protocol. ISO/IEC 15408(all parts) allows three ways of doing this:

- a) As an organizational security policy (or part of it).

EXAMPLE 1

There exists a government standard defining how passwords have to be chosen, this **may** be stated as an organizational security policy in an ST. This **may** lead to an objective for the environment (e. g. if users of the TOE need to choose passwords accordingly), or it **may** lead to Security Objectives for the TOE and then to appropriate SFRs (likely of the FIA class), if the TOE generates passwords. In both cases the rationale of the developer needs to make plausible that the Security Objectives for the TOE and the SFRs are suitable to fulfil the OSP. The evaluator will examine if this is in fact plausible (and **may** decide to look into the standard for this), if the OSP is implemented by SFRs, as explained below.

- b) As a technical standard used in a refinement of ~~an SFR~~ component or security requirement.

Editors' Note

Editors have corrected b) since it could apply also to assurance components and SARs.

EXAMPLE 2

FCS_CKM.1.1 Refinement: The [selection: **TSF, TOE platform**] **shall** generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection:

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: [selection:
 - **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;**
 - **ANSI X9.31-1998, Section 4.1];**
- ECC schemes using "NIST curves" P-256, P-384 and [selection: **P-521, no other curves**] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1

].

Conformance to the standard as part of the fulfilment of the SFR by the TOE is then assessed in one of the following ways:

- 1) If an explicit Evaluation Activity has been defined for the SFR in accordance with ISO/IEC 15408-4, then the evaluator actions in that Evaluation Activity are carried out;
- 2) If no explicit Evaluation Activity has been defined for the SFR then conformance is subsequently determined as if the full text of the standard is included as part of the SFR. This means that, as with any other aspect of an SFR during ADV: Development and ATE: Tests it is analysed, by design analysis and tests, to determine that the SFR is completely and fully implemented in the TOE."

If reference to only a certain part of a standard is desired, that part **should must** be unambiguously stated in the SFR refinement.

- c) As a technical standard referenced in the TOE summary specification.

The TOE summary specification is only considered as an explanation of how the SFRs are realized and is not strictly used as a strict implementation requirement like the SFRs or the documents delivered for ADV: Development. So, the evaluator **may could** detect an inconsistency if the TSS references a technical standard and this is not reflected in ADV: Development documentation, but there is no routine activity to test fulfilment of the standard.

EXAMPLE

TSS content

"The TOE provides cryptographic functionality to perform an AES encryption and decryption with 128,192 or 256 bits keys to the embedded software. The AES algorithm conforms with ISO/IEC 18033-3:2010, 5.2."

NOTE The ST author is reminded that referring to a standard in SFRs **may can** impose a significant burden on a developer developing a TOE to meet that ST (depending on the size and complexity of the standard and the assurance required), and that it **may can** be more suitable to require alternative (non-CC related) ways to assess conformance to that standard.

A.4.9 Direct Rationale STs

A.4.9.1 General

~~In some situations, it is appropriate to include a security problem definition, that omits the definition of the TOE Security Objectives, but includes a rationale that directly maps the threats, organizational security policies and where appropriate, Security Objectives for the operational environment given in the SPD. The rationale demonstrates that the threats are countered and the organizational security policies are implemented.~~

In some situations, it is appropriate to omit the definition of the TOE Security Objectives, in this case the Security Requirements rationale directly maps the SPD and, where appropriate, Security Objectives for the operational environment, to the SFRs. The Security Objectives rationale demonstrates that the threats are countered and the organizational security policies are implemented.

~~The intention of this type of ST is to minimize the level of indirection between threats or OSPs, Security Objectives for the operational environment, and the SFRs, based on an enhanced description of the SFRs.~~

The intention of the Direct Rationale ST is to minimize the level of indirection between the SPD, any Security Objectives for the operational environment, and the SFRs, based on an enhanced description of the SFRs.

Editors' Note:

Editors amended the above text since the Security Objectives are not part of the SPD

Because of its directness and additional description of SFRs in natural language, this type of ST can be easier for end-users and risk owners to understand and use.

~~ISO/IEC 15408(all parts) allows the use of a Direct Rationale ST for either~~

~~— an EAL 1 evaluation; or~~

~~— where the ST specifies a set of assurance components that are not the EAL2 through EAL7 packages given in ISO/IEC 15408-5.~~

Editors' Note:

Do we want ISO to make these requirements? – That is usually in the domain of scheme / MRA policy.

Editors request comments on this issue. In the absence of comments about this issue, the Editors will delete requirements in the next draft.

The differences found in a Direct Rationale ST are in the conformance claims and in the SPD sections. These are described in A.4.9.2 and A.4.9.3, below.

The content of a Direct Rationale ST is shown in Figure A.4

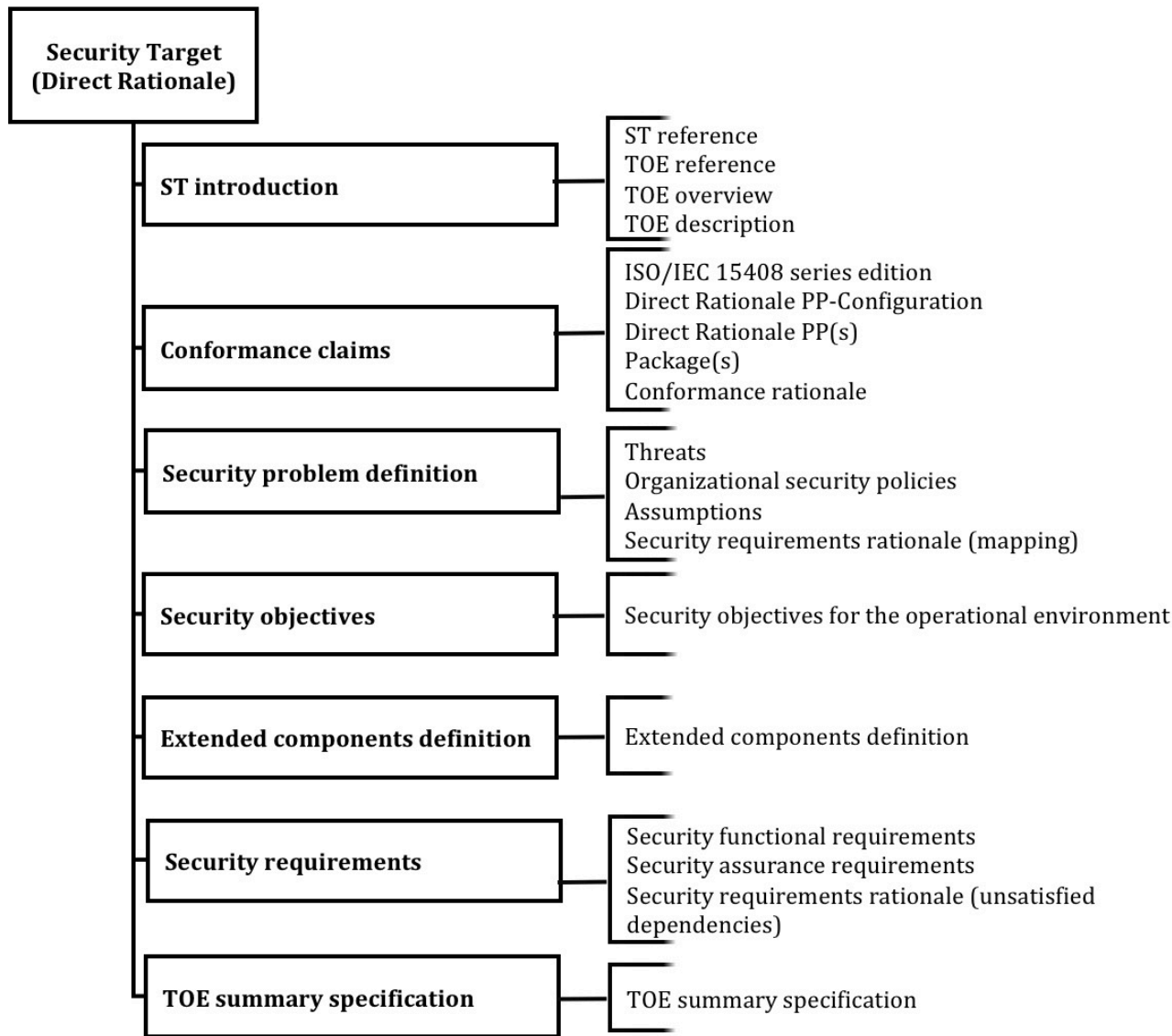


Figure A.4 — Contents of a Direct Rationale ST

A.4.9.2 Conformance claims (ASE_CCL) for Direct Rationale STs

A Direct Rationale ST **can** only claim conformance to one or more other Direct Rationale PPs (see 11.2.1 and Annex B).

A Direct Rationale ST **can** only claim conformance to a PP-Configuration if that PP-Configuration also uses the Direct Rationale approach. (see 11.2.1)

A.4.9.3 Security Problem Definition (ASE_SPD) for Direct Rationale STs

A.4.9.3.1 General

A Direct Rationale ST has the following differences when compared to an ST that contains Security Objectives for the TOE:

- Security Objectives for the TOE are not included.

- A Security Objectives rationale is not included as there are no TOE Security Objectives in the ST;
- A Security Requirements rationale that directly maps the SPD-elements to the SFRs and to any Security Objectives for the operational environment is included. It is recommended that this part of the security requirements rationale is located directly under each of the threats, OSPs and assumptions in the SPD section. As in an ST that contain Security Objectives for the TOE, the security requirements rationale also needs to justify any SFR dependencies that are not satisfied; this part of the rationale is typically located after the definition of the SFRs.
- there is a requirement, given in ISO/IEC 15408-3, to provide a natural language description of the SFRs and their relationship to security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

EXAMPLE:

The following are examples of internal features:

- Unavailability of residual data upon reallocation of a resource;
- Hidden failure conditions of login/password-authentication;
- Hidden biometric comparison score.

A.4.9.3.2 Tracing between SFRs, Security Objectives and the security problem definition

The tracing between SFRs, Security Objectives and the SPD becomes more straightforward in a Direct Rationale ST. Figure A.5 shows the more direct specification of the SFRs that is used in the Direct Rationale approach.

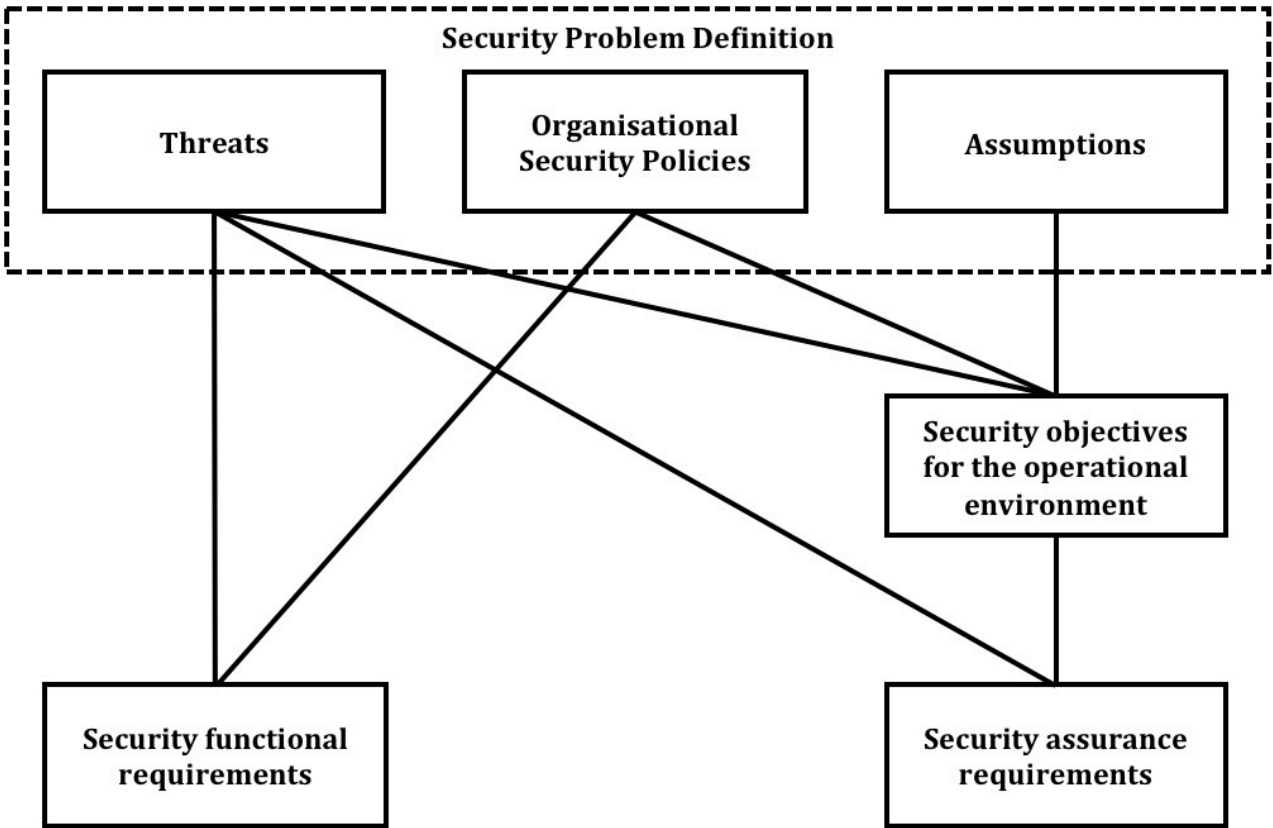


Figure A.5 — Relations between the security problem definition, the Security Objectives, and the security requirements for Direct Rationale STs

Annex B (informative)

Specification of Protection Profiles and Modular PPs

Editors' Note:

The 2018 Directives have clarified the normative/informative status of Annexes

Note that informative annexes may contain **optional** requirements, however the main clauses would then describe in which case the option could be taken.

This Annex is informative. The various requirements and permissions appearing in this annex,

Either need to be moved in the corresponding normative clauses of 15408-1, -2 or -3;

or the verbal form needs to be changed.

The verbal forms used by ISO are very specific.

— Requirement: shall or shall not

— Recommendation: should or should not

— Permission: may or may not

— Possibility and capability: can or cannot

— External constraint: "must"

Additionally, we should consider verifying that any requirements, recommendations and permissions are actually present as SARs or CEM activities.

More information on verbal forms and the annex statuses are found in the latest directives at:

<http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype>

B.1 Goal and structure of this Annex

The goal of this annex is to explain the Protection Profile (PP) concept.

NOTE This annex does not define the APE evaluation criteria; this definition can be found in ISO/IEC 15408-3 and is supported by the documents given in the bibliography.

As PPs and STs have a significant overlap, this annex focuses on the differences between PPs and STs.

The material that is identical between STs and PPs is described in annex A.

This annex consists of six major parts:

a) *The specification of a PP.* This is summarized in B.2. and includes

— *how a PP is used*

— *how a PP is not used.*

— *What a PP must contain.* This is summarized in B.2.2 and is described in more detail in B.2.2.1 to B.2.8. These clauses describe the mandatory contents of the PP, the interrelationships between these contents, and provide examples.

— *Claiming conformance with standards.* B.2.9 describes how a PP writer can claim that the TOE is to meet a particular standard.

— *Direct Rationale PPs.* Direct Rationale PPs are PPs in which the threats and organizational security policies in the SPD are mapped directly to the SFRs and possibly to Security Objectives for the operational environment. They are described in detail in B.2.10.

b) *PP-Modules.* These are described in B.3.

c) *PP-Configurations*. These are described in B.4.

B.2 Specification of a PP

B.2.1 Using a PP

B.2.1.1 How a PP is used

A PP is typically a statement of need where a user community, a regulatory entity, or a group of developers define a common set of security needs. A PP gives consumers a means of referring to this set and facilitates future evaluation against these needs.

A PP is therefore typically used as:

- part of a requirement specification for a specific consumer or group of consumers, who will only consider buying a specific type of IT product if it meets the PP;
- part of a regulation from a specific regulatory entity, who will only allow a specific type of IT product to be used if it meets the PP;
- to address a common security problem presented by a variety of consumers, and often defined by a group including several IT product developers, who then produce IT products of this type in order to meet the needs of their common market.

although this does not preclude other uses.

B.2.1.2 How a PP ~~should~~ **must** not be used

Two roles, among many, that a PP **does not** fulfil are:

- a complete specification: A PP is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size, and weight, required voltage etc. **might not** be part of a PP. This means that in general a PP is a part of a complete specification, but not a complete specification itself.
- a specification of a single product: Unlike an ST, a PP is designed to describe a certain type of IT product, and not a single product. When only a single product is described, it is better to use an ST for this purpose.

B.2.2 Mandatory Contents of a PP

There are two types of PP. Firstly the “regular” PP which is a PP that contains the full contents as described in in B.2.2.1 to B.2.8. Secondly, in some cases a PP author can write a Direct Rationale PP which has different contents compared to PPs that contain Security Objectives for the TOE. Direct Rationale PPs, and the reasons and circumstances in which they are used are described in detail in B.2.10. All other parts of this Annex assume a PP with full contents.

Figure B.1 portrays the content for a PP that is given in ISO/IEC 15408-3. Figure B.1 ~~may~~ **can** also be used as a structural outline of the PP, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the PP instead of in the security requirements section. The separate sections of a PP and the contents of those sections are briefly summarized below and explained in much more detail in B.2.2.1 to B.2.8.

A PP contains:

- a) a *PP introduction* containing a narrative description of the TOE type;
- b) a *conformance claim*, showing which edition of The ISO/IEC 15408 series is applicable, whether the PP claims conformance to any other PPs and/or packages, and if so, to which ones and the type of conformance claimed. The conformance claim also provides a conformance statement showing the type of conformance demanded of STs and other PPs derived from it;

NOTE PP-Modules inherit the type of conformance demanded by the PP in its conformance statement when the PP is used by the PP-Module as a Base-PP;

- c) a *security problem definition*, showing threats, OSPs and assumptions;

- d) *Security Objectives*, showing how the solution to the security problem is divided between Security Objectives for the operational environment and optionally Security Objectives for the TOE;
- e) *extended components definition*, where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) ~~may~~ can be defined. These new components are needed to define extended functional and extended assurance requirements;
- f) *security requirements*, where a translation of the Security Objectives for the TOE into a standardized language is provided. This standardized language is in the form of SFRs. Additionally, this section of a PP defines the SARs;

There also exist Direct Rationale PPs, which have slightly different content; these are described in detail in B.2.10.. With this exception, all other parts of this Annex assume a PP with full contents.

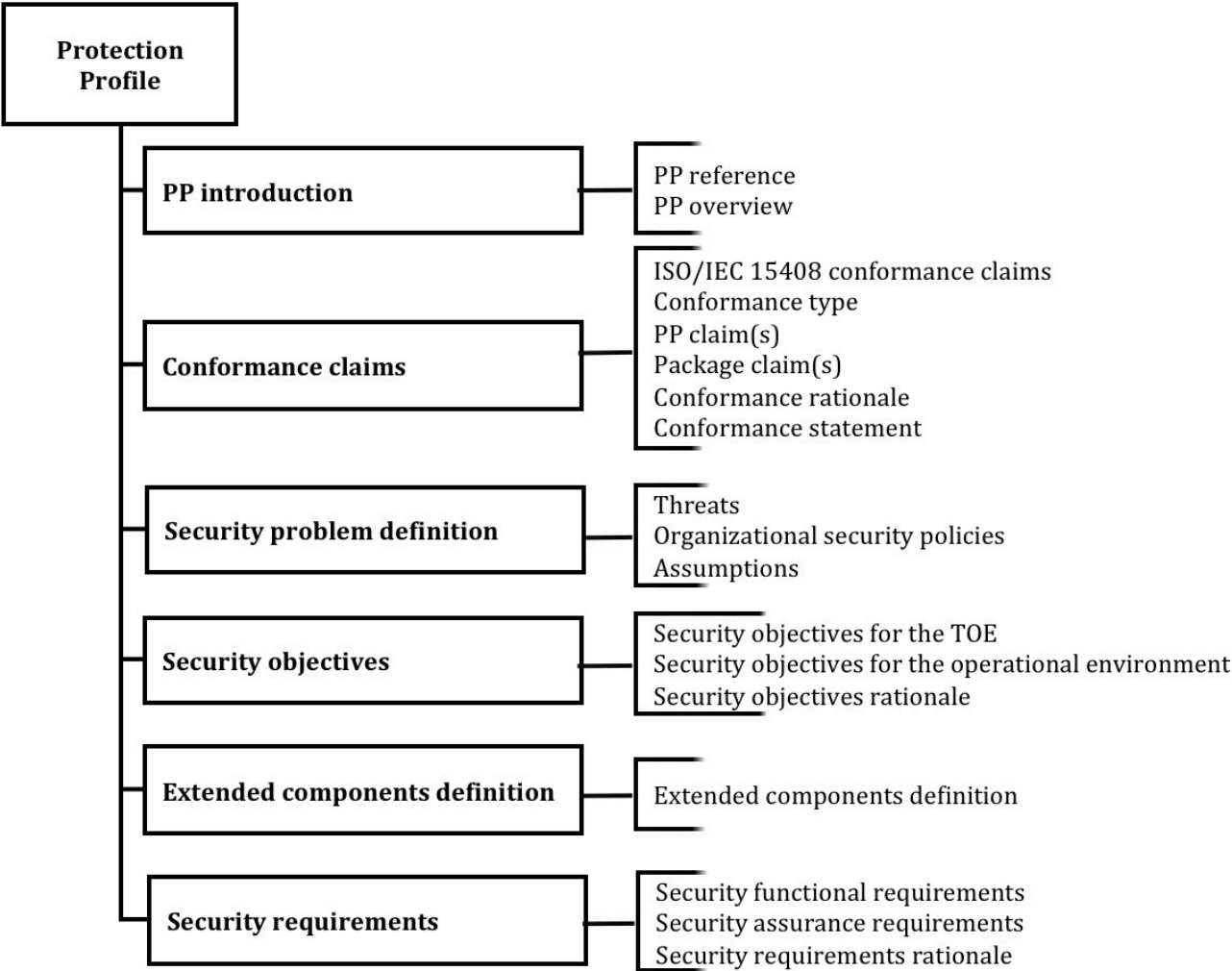


Figure B.1 — Contents of a Protection Profile

B.2.2.1 PP introduction (APE_INT)

B.2.2.1.1 General

The PP introduction describes the TOE in a narrative way on two levels of abstraction:

- a) the PP reference, which provides identification material for the PP;
- b) the TOE overview, which briefly describes the TOE.

B.2.2.1.2 PP reference

A PP contains a clear PP reference that identifies that particular PP. A typical PP reference consists of title, version, sponsors, and publication date.

NOTE Here a distinction is made between the sponsor of an ST, i.e. the entity responsible for its development, and the author of an ST which is the entity responsible for its production.

EXAMPLE

An example of a PP reference is “Atlantean Navy CablePhone Encryptor PP, version 2b, Atlantean Navy Procurement Office, April 1, 2020”.

The reference **must** be unique so that it is possible to tell different PPs and different versions of the same PP apart. The PP reference facilitates indexing and referencing the PP and its inclusion in lists of PPs.

B.2.2.1.3 TOE overview

The TOE overview is aimed at potential consumers of a TOE who are looking through lists of evaluated products to find TOEs that **may can** meet their security needs, and are supported by their hardware, software, and firmware.

The TOE overview is also aimed at developers who **may can** use the PP in designing TOEs or in adapting existing products.

The typical length of a TOE overview is several paragraphs.

To this end, the TOE overview briefly describes the usage of the TOE and its major security features, identifies the TOE type, and identifies any major non-TOE hardware/software/firmware available to the TOE.

B.2.2.1.3.1 Usage and major security features of a TOE

The description of the usage and major security features of the TOE is intended to give a very general idea of what the TOE ~~should be~~ **is** capable of, and what it **can** be used for. This section is written for TOE or potential TOE consumers, describing TOE usage and major security features in terms of business operations, using language that TOE consumers understand.

EXAMPLE

An example of this is “The Atlantean Navy CablePhone Encryptor is an encryption device that **should** allow confidential communication between ships across the Atlantean Navy CablePhone system. To this end it **should** allow at least 1024 different users and support at least 500 Mbps encryption speed. It **should** allow both bilateral communication between ships and broadcast across the entire network.”

B.2.2.1.3.2 TOE Type

The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server, mobile device, and database, etc.

B.2.2.1.3.3 Available non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify the non-TOE hardware/software/firmware.

As a Protection Profile is not written for a specific product, in many cases only a general idea **can** be given of the available hardware/software/firmware. In some other cases, (much) more specific information **may can** be provided

EXAMPLE 1

An example where more specific information is provided would be a requirements specification for a specific consumer where the platform is already known.

EXAMPLE 2

Examples of hardware/software/firmware identifications include:

- None. (for a completely stand-alone TOE);
- a standard PC with a dual core 2.10 GHz or faster processor and 4GB or more RAM, running the Yaiza operating system for professionals, version 53.0 Update 6b, c, or 7, or version 54.0;
- a standard 64-bit server with a 2xQuad-Core core processor and 16GB or more RAM, running the Yaiza operating system, server edition version 7.0 Update 6d, and the WonderMagic 12.0 Graphics card with the 1.01 WM Driver Set;
- a CleverCard SB17067 integrated circuit;
- a CleverCard SB17067 integrated circuit running v12.0 of the QuickOS smart card operating system;
- Yaiza mobile-OS 3.1.6 on smartphone and tablet devices using the FP9 processor.

B.2.3 Conformance claims and conformance statement (APE_CCL)

B.2.3.1 General

The conformance claims section of a PP describes how the PP conforms with the ISO/IEC 15408 series. other PPs, PP-Modules and with packages. It is identical to the conformance claims subclause for an ST described in A.4.2, with one exception, the conformance statement.

The conformance statement in the PP states how ST/PPs **must** conform to that PP. The PP author selects whether “exact”, “strict” or “demonstrable” conformance is required.

NOTE 1 See B.3 for the use of conformance claims in PP modules

NOTE 2 See B.2.10.2 for the use of conformance claims in Direct Rationale PPs

B.2.3.2 Exact conformance

If exact conformance is selected, the PP author also has the option of specifying the following information in the components statement:

- PPs and packages that **can** be used with the PP;
- PP-Modules that **can** use this PP as a Base-PP in a PP-Configuration; and
- other PPs that **can** claim conformance to the PP.

NOTE 1 See 9 (PPs) and 10 (Modular PPs) for the requirements and Annex E for additional description in the exact conformance case.

B.2.4 Security problem definition (APE_SPD)

This subclause is identical to the security problem definition subclause of an ST as explained in A.4.3

B.2.5 Security objectives (APE_OBJ)

This subclause is identical to the Security Objectives subclause of an ST as explained in A.4.4. and A.4.9

B.2.6 Extended components definition (APE_ECD)

This subclause is identical to the extended components subclause of an ST as explained in A.8.

B.2.7 Security requirements (APE_REQ)

This subclause is identical to the security requirements subclause of an ST as explained in A.9. with the exception of

- the rules for completing operations as described in 7.2
- the specification of selection-based SFRs as outlined below.

A PP **may can** identify a set of selection-based SFRs. In this case, the PP author additionally ensures that the PP clearly indicates the dependencies between a particular selection in an security functional

component and/or SFR included in the PP and the associated selection-based SFR(s) that ~~should~~ must be included if that selection is chosen by another PP/ST author. This is explained in 9.7.

B.2.8 TOE summary specification

Unlike an ST, a PP has no TOE summary specification.

B.2.9 Referring to other standards in a PP

This subclause is identical to the subclause on standards for STs as described in A.12, with one exception: Since a Direct Rationale PP has no TOE summary specification, the third option is not valid for Direct Rationale PPs.

B.2.10 Direct Rationale PPs

B.2.10.1 General

Writing a PP includes consideration of the STs that will be written with the PP as a basis. As noted in A.4.9, in some cases it is desired to write a PP that supports the specification of Direct Rationale STs.

~~The intention of this type of PP is to minimize the level of indirection between threats or OSPs, Security Objectives for the operational environment, and the SFRs, based on an enhanced description of the SFRs.~~

The intention of the Direct Rationale PP is to minimize the level of indirection between the SPD, any Security Objectives for the operational environment, and the SFRs, based on an enhanced description of the SFRs.

~~In this case, it is appropriate to include a security problem definition that omits the definition of the TOE Security Objectives, but includes a rationale that directly maps the threats, organizational security policies and where appropriate, Security Objectives for the operational environment given in the SPD. The rationale demonstrates that the threats are countered and the organizational security policies are implemented.~~

In some situations, it is appropriate to omit the definition of the TOE Security Objectives, in this case the Security Requirements rationale directly maps the SPD and, where appropriate, Security Objectives for the operational environment. The Security Objectives Rationale demonstrates that the threats are countered and the organizational security policies are implemented.

Editors' Note:

Editors amended the above text since the Security Objectives are not technically part of the SPD.

Because of its directness and the additional description of SFRs in natural language, this type of PP makes it easier for end-users and risk owners to understand and use.

The ISO/IEC 15408 series allows the use of a Direct Rationale PP for

- an EAL 1 evaluation;
- where the PP specifies a set of assurance components that are not the EAL2 through EAL7 packages given in ISO/IEC 15408-5.

Editors' Note:

Do we want ISO to make these requirements? – That is usually in the domain of scheme / MRA policy

A Direct Rationale PP has the same relationship to a PP that contains Security Objectives for the TOE, as a Direct Rationale ST has to an ST that contains Security Objectives for the TOE. This means that a Direct Rationale PP consists of:

- a) a PP introduction, consisting of a PP reference and a TOE overview;
- b) the conformance claim;
- c) Security Objectives for the operational environment;

- d) the SFRs and the SARs (including the extended components definition) and the security requirements rationale (only if the dependencies are not satisfied).

The content of a Direct Rationale PP is shown in Figure B.2.

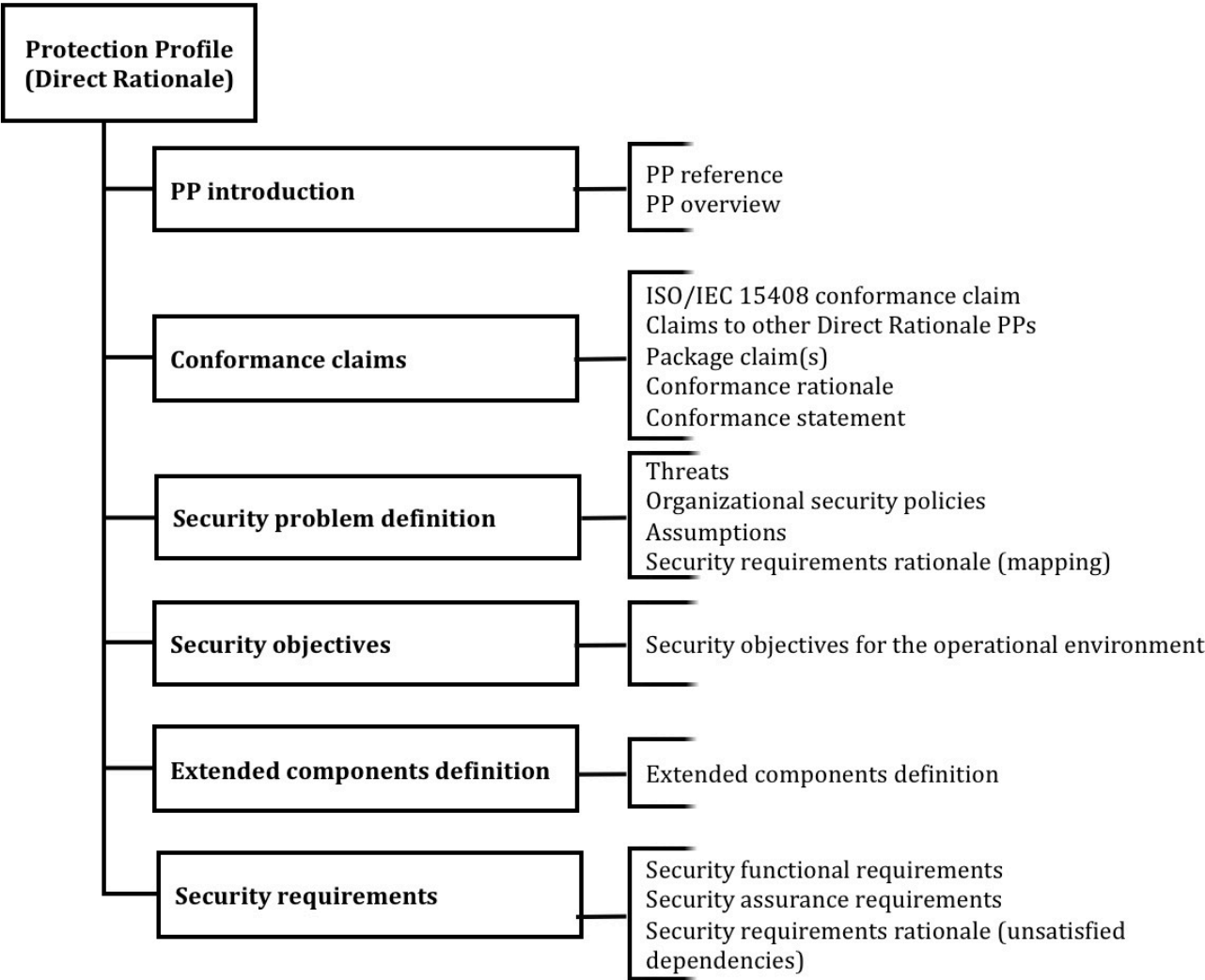


Figure B.2 — Contents of a Direct Rationale PP

B.2.10.2 Conformance claims (ASE_CCL) for Direct Rationale PPs

A Direct Rationale PP **may can** only claim conformance to another Direct Rationale PP (See 9 and B.5). A regular PP **may can** claim conformance with a Direct Rationale PP.

B.2.10.3 Security Problem Definition (ASE_SPD) for Direct Rationale PPs

A Direct Rationale PP has the following differences when compared to an PP that contains Security Objectives for the TOE:

- Security Objectives for the TOE are not included. The Security Objectives for the operational environment **must** still be described;
- a Security Objectives rationale is not included as there are no TOE Security Objectives in the PP;
- a Security Requirements rationale that directly maps the SPD-elements to the SFRs and to any Security Objectives for the operational environment is included. It is recommended that this part of the security requirements rationale is located directly under each of the threats, OSPs and assumptions in the SPD section. As in a PP that contain Security Objectives for the TOE, the security requirements rationale also needs to justify any SFR dependencies that are not satisfied; this part of the rationale is typically located after the definition of the SFRs.

- there is a requirement to provide a natural language description of the SFRs and their relationship to security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

EXAMPLE
The following are examples of internal features:

- Unavailability of residual data upon reallocation of a resource;
- Hidden failure conditions of login/password-authentication;
- Hidden biometric comparison score.

B.3 Specification of PP-Modules

B.3.1 Using a PP-Module

A PP-Module is a security statement of a group of users or developers, regulators, administration, or any other entity that meets specific consumer needs. A PP-Module complements one or more Base-PPs and allows consumers to refer to this statement, facilitates the evaluation against it and the comparison of conformant evaluated TOEs.

NOTE A Base-PP is a PP that is intended to be used with one or more PP-Modules.

B.3.2 Mandatory Contents of a PP Module

Figure B.3 shows the content of a PP-Module.

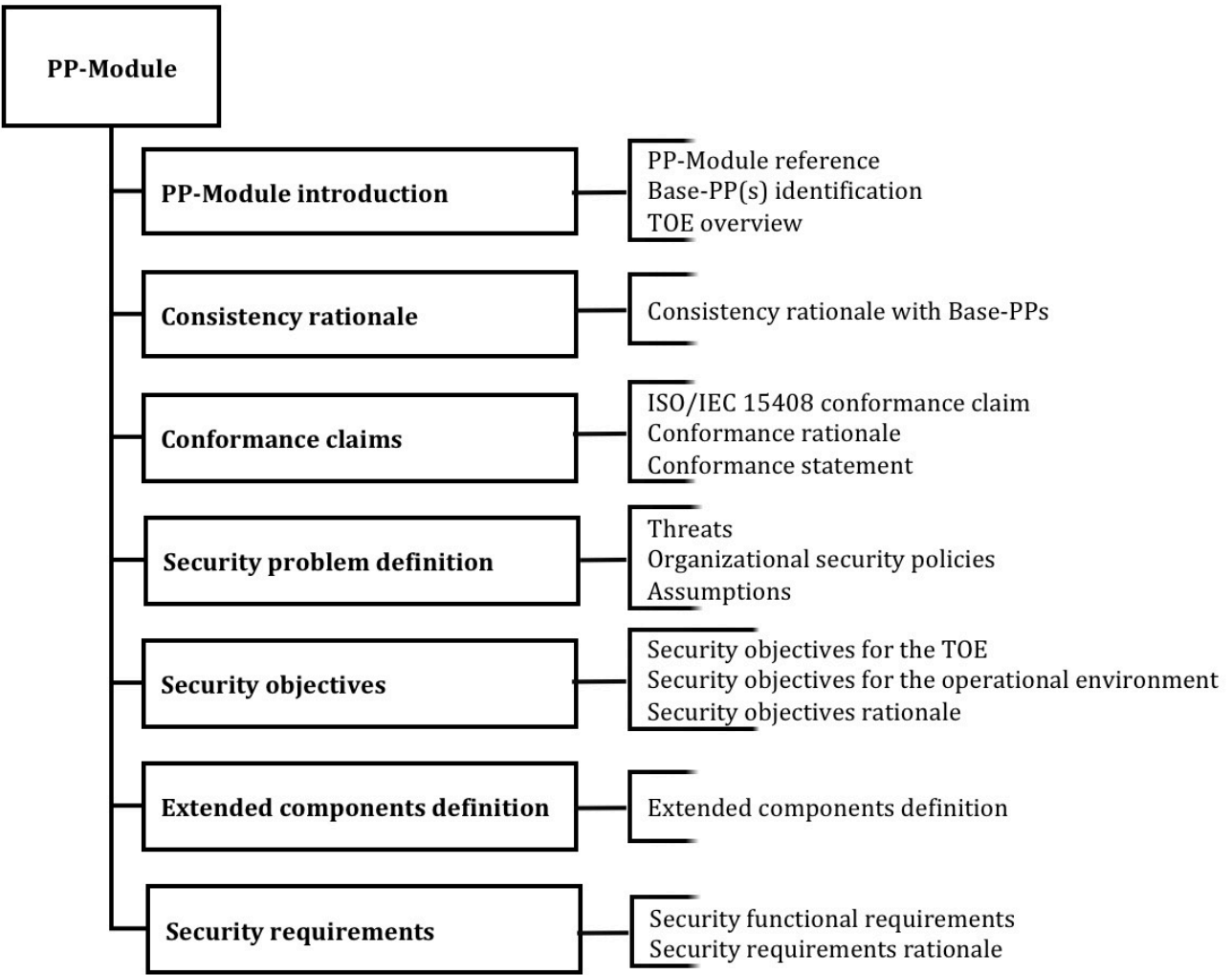


Figure B.3 — Content of a PP-Module

Editors' Note:

Please note that the comment MY/ZM1 highlighted issues in Tables 14 and 15 of 15408-5

The comment MY/ZM2 asked for a figure illustrating the usage of a standard PP. We understand that Figure 1 answers this need. Experts are kindly asked to comment or provide additional details on how this can be improved.

The content of the PP-Module is summarized below and explained in detail in sections from B.3.2.1 to B.3.3. A PP-Module contains:

- an *Introduction* which identifies the PP-Module, identifies the Base-PP(s) which it is based on and states the correspondence rationale, and provides a description of the TOE within its environment that meets the descriptions underlying the Base-PPs,
- a *Consistency rationale* that states the correspondence between the Module and its Base-PP(s),
- a *Conformance claim* regarding the edition of the ISO/IEC 15408 series, the conformance statement and with any applicable inherited EAL,
- a *Security problem definition* with threats, assumptions, and organizational security policies,
- a *Security objectives section* presenting the solution to the security problem in terms of objectives for the TOE and its operational environment,
- an optional *Extended functional components* definition where new functional components not included in ISO/IEC 15408-2 are introduced,
- a *Security functional requirements* section with a standardized statement of the TOE Security Objectives.

B.3.2.1 PP-Module introduction**B.3.2.1.1 PP-Module reference**

The PP-Module introduction provides a clear and unambiguous reference that allows identifying the PP-Module. A typical reference is made of the title of the PP-Module, its version, their sponsors, and the publication date.

The PP-Module reference can be used to index the document in Protection Profiles catalogues.

B.3.2.1.2 Base-PP identification

The PP-Module introduction identifies the Base-PPs that the PP-Module relies on. The identification consists of a list of Base-PP references.

The PP-Module **may could** require that it be used with a set of Base-PPs simultaneously, say $\{PP_1 \dots, PP_n\}$; the identification list states:

$$PP_1 \text{ AND } \dots \text{ AND } PP_n \text{ with } n \geq 1$$

Alternatively, the PP-Module **may could** allow it's use with alternative sets of Base-PPs, say $\{S_1 \dots, S_k\}$; the identification list states:

$$S_1 \text{ OR } \dots \text{ OR } S_k \text{ with } k \geq 1$$

The general form of the Base-PP identification is then:

$$(PP_{1,1} \text{ AND } \dots PP_{1,n_1}) \text{ OR } \dots \text{ OR } (PP_{k,1} \text{ AND } \dots PP_{k,n_k}) \text{ with } n \geq 1, k \geq 1$$

NOTE 1 A PP-Module that states a list with an "OR" **can** be replaced by as many PP-Modules as elements in the list. That is, the list with an "OR" is a means to avoid managing similar PP-Modules for different usages, which does not introduce any complexity to the security specification itself.

NOTE 2 A Base-PP with an exact conformance statement is not allowed to be combined with Base-PPs with other types of conformance in a PP-Module.

B.3.2.1.3 TOE overview

The TOE overview of the PP-Module ~~may~~ completes the TOE overviews of the Base-PPs, provided the supplements do not contradict the Base-PPs:

- The TOE type of the PP-Module **can** be the same of the Base-PPs or introduce specificities that meet the purpose of the PP-Module.
- The PP-Module **can** introduce additional usage and major security features to those stated in the Base-PPs.
- The PP-Module **can** specify particular non-TOE hardware, software and/or firmware compliant with the statement in the Base-PPs.

In a PP-Module, the possibility of supplementing the TOE overview of one or more of the Base-PPs has the same meaning as in an Base-PP or ST that supplements the TOE overview of a Base-PP to which they claim conformance.

The statement of the TOE overview in a PP-Module is necessary whenever the TOE overview of the Base-PPs present different characteristics that need to be consolidated.

The PP-Module ~~may~~ **can** provide as many specific TOE overviews as alternative sets of Base-PPs.

B.3.2.2 Consistency rationale

The PP-Module has to provide a consistency rationale with respect to its Base-PPs.

If the PP-Module specifies alternative sets of Base-PPs, the PP-Module **must** provide as many conformance claims as the number of alternative set of Base-PPs.

If the PP-Module specifies alternative sets of Base-PPs, the PP-Module **must** provide as many consistency rationales as the number of alternative set of Base-PPs.

The consistency analysis **must** be performed on the TOE type, the SPD, the objectives, and the security functional requirements. At the end, the goal is to demonstrate that a TOE can meet the TOE type descriptions provided in the Base-PP(s) and in the PP-Module and that the TOE can satisfy all security functional requirements specified in the Base-PPs and the PP-Module.

The consistency rationale **must** demonstrate that the unions of the SPD, the objectives, and the security functional requirements from the Base-PPs and from the PP-Module do not lead to a contradiction.

The consistency rationale ~~may~~ **can** use correspondence tables between SPD/objectives/SFRs in the PP-Module and SPD/objectives/SFRs in the Base-PPs together with textual justifications whenever needed.

NOTE The consistency at the SFR level implies the consistency of the union of objectives and the union of SPDs provided that the PP-Module does not change the assumptions and objectives for the environment of the Base-PP(s).

B.3.2.3 Conformance claims and conformance statement**B.3.2.3.1 General**

This section of a PP-Module **must** be included for all PP-Modules and describes how the PP-Module conforms to:

- ISO/IEC 15408-2, its edition, and any use of extended security requirements
- functional packages.

A PP-Module **cannot** claim conformance to any PP, PP-Module, or PP-Configuration.

NOTE A PP-Module inherits the SAR packages, including any pre-defined EALs, from its Base-PPs. The issue of ANDed Base-PPs with different EALs must be resolved and is dealt with in the same way that an ST conformant to all those PP deals with the issue.

Editors' Note:

Editors wonder if it is just SAR packages? It may be some set of SARs that is not officially a package. Comments are solicited on this topic.

4068

4069

4070

4071

ISO/IEC CD1 15408-1: ####(E)

Editors suggest the following text:

"A PP-Module inherits the security assurance requirements, including any assurance packages such as the pre-defined EALs"

If no comments are received on this, the editors' proposal will be accepted and presented in the next draft.

4072

B.3.2.3.2 The conformance statement

4073

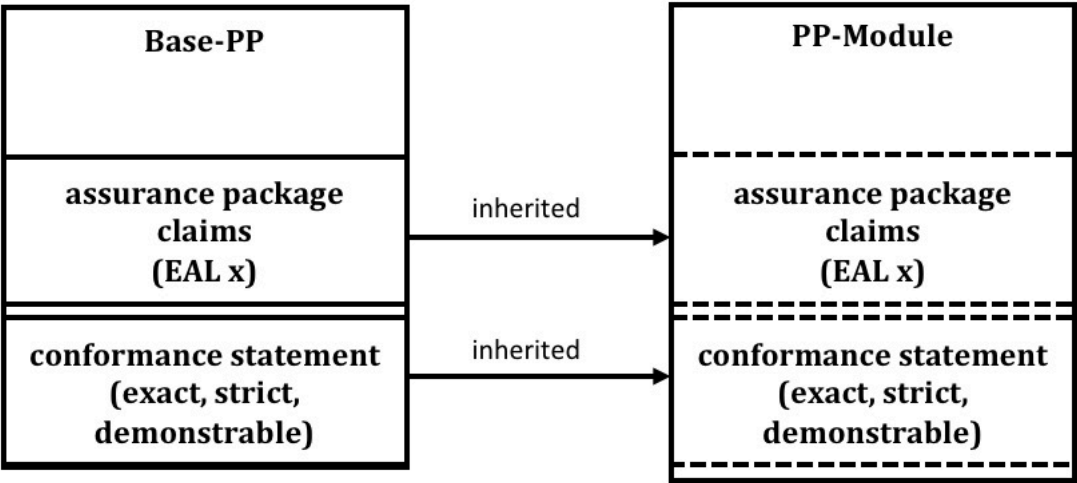
4074

4075

4076

4077

The conformance statement **must** be stated in a PP-Module. A PP-Module does not claim conformance to any PP, PP-Module, or PP-Configuration. However, a PP-Module inherits the conformance statement, exact, strict, or demonstrable, from its Base-PPs. The issue of two or more Base-PPs with different conformance statements **must** be resolved and is dealt with in the same way that an ST conformant to all those PPs deals with the issue.



4078

Figure B.4 — General case for inherited conformance claims and statement

4079

B.3.2.3.2.1 Exact conformance

4080

In the case of exact conformance, the conformance statement also includes

- 4081
- 4082
- 4083
- 4084
- an “allowed with” statement describing a list of other PPs and PP-Modules with which the PP-Module can be used;
 - the set of other PP-Modules that are allowed to be specified in a PP-Configuration that uses the PP-Module (in combination with the Base-PPs requiring exact conformance).

4085

4086

NOTE 1 A Base-PP with exact conformance is not allowed to be combined with Base-PPs with other types of conformance.

4087

4088

NOTE 2 This maintains the exact conformance concept that the PP-Module authors have control over which other requirements **can be** specified in combination with the requirements specified in their PP-Module.

4089

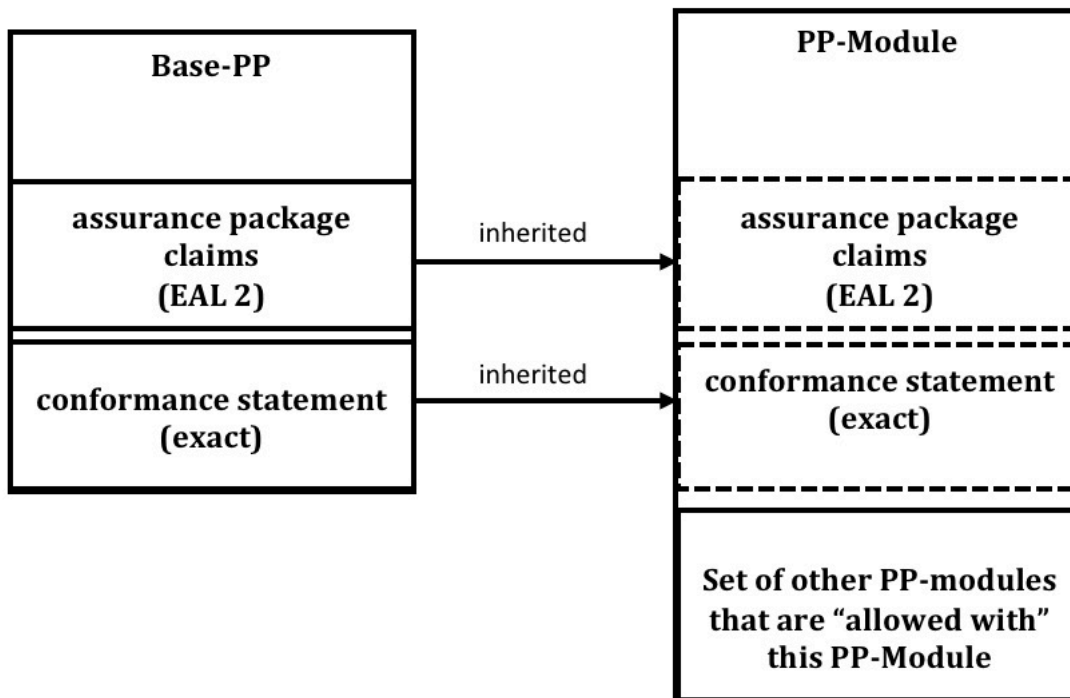


Figure B.5 — Exact conformance case for inherited conformance claims and statement

Editors' Note:

Do we really want to specify EAL2 in the above diagram? This specification is usually a matter for scheme or MRA policy rather than in the standard.

B.3.2.4 Security problem definition

This section defines the security problem addressed by the PP-Module. It can contain the SPD-elements assumptions, threats, and organizational security policies.

A PP-Module defines the security problem in relationship with the security problem of the Base-PPs and the definition of the TOE and its environment provided in the PP-Module's Introduction.

Each SPD-element **may could** either come from a Base-PP or be entirely new. Let E be an SPD-element of a PP-Module, one of the following cases holds:

- E belongs to an identified Base-PP; the PP-Module **may can** only contain a reference to the SPD-element in the Base-PP,
- E results from the refinement of an SPD-element of a Base-PP,
- E is a new SPD-element introduced by the PP-Module, related to additional features of the TOE or its environment.

NOTE 1 The interpreted / refined SPD-elements can be dealt with as new SPD-elements without any impact on the meaning of the SPD.

NOTE 2 In the same way that STs can, a PP-Module can introduce assumptions provided they cover aspects that are outside the scope of the Base-PPs.

B.3.2.5 Security Objectives

This section defines the Security Objectives for the TOE and for the TOE's operational environment.

A PP-Module defines new Security Objectives in context with the Security Objectives of the Base-PP(s).

Each Security Objective **may can** either come from a Base-PP or be entirely new. Let O be an objective of a PP-Module, one of the following cases holds:

— O belongs to an identified Base-PP; the PP-Module **may can** only contain a reference to the Security Objective in the Base-PP.

— O is a result of the refinement of a security objective of a Base-PP,

— O is a new objective introduced by the PP-Module.

NOTE The refined objectives can be dealt with as new objectives without any impact on the meaning of the whole set of objectives.

A PP-Module **can** introduce new objectives for the TOE operational environment only when they address aspects that are outside the scope of the Base-PPs.

In the case where a PP-Module refines the TOE type, some Security Objectives for the environment of the Base-PPs ~~could~~**can** become Security Objectives for the TOE in the PP-Module.

This section also defines the rationale between the SPD and the Security Objectives of the PP-Module, which consists of a mapping that traces the SPD of the PP-Module to their Security Objectives as well as a justification demonstrating that the tracing is effective, as specified in section B.7. Moreover, the mapping has to show not only that all the SPD-elements are covered but also that there is no useless security objective.

It **may-can** happen that some Security Objectives of the PP-Module cover also SPD-elements of the Base-PPs that do not belong to the SPD of the PP-Module itself. This information is not required but can be provided in application notes.

B.3.2.6 Extended functional components definition

This section is identical to the standard PP and ST extended components section specified in section A.8, applied to functional components only.

B.3.2.7 Security functional requirements

This section defines the security functional requirements for the TOE in relationship with the set of TOE Security Objectives in the PP-Module and with the security functional requirements of the Base-PPs.

Each security functional requirement **may can** either come from a Base-PP or be entirely new. Let R be a security functional requirement of a PP-Module, one of the following cases holds:

— R belongs to an identified Base-PP; the PP-Module **may can** only contain a reference to the requirement in the Base-PP,

— R results from the refinement of an SFR of a Base-PPs,

— R is a new requirement introduced by the PP-Module.

NOTE The refined requirements can be dealt with as new ones without any impact on the meaning of the whole set of requirements.

This section also defines the rationale between the SFRs and the TOE Security Objectives of the PP-Module, which consists of a mapping that traces the TOE objectives of the PP-Module to one or more SFRs and a justification demonstrating that the tracing is effective, as specified in section B.9. Moreover, the mapping **must** fulfil the conditions specified in section B.14.10 and has to show not only that all the objectives for the TOE are covered but also that there is no useless security functional requirement.

It **may-can** happen that some SFRs of the PP-Module cover also TOE Security Objectives of the Base-PPs that do not belong to the PP-Module itself. This information is not required but can be provided in application notes.

B.3.3 Direct Rationale PP-Modules

PP-Modules **may can** be written with the intention that they be used with a Direct Rational PP(s) as their Base-PP(s). In this case Security Objectives for the TOE are not included in the PP-Module and Security Objectives for the TOE's operational environment **may can** be included.

The contents of a Direct Rationale PP-Module are shown in figure B.6.

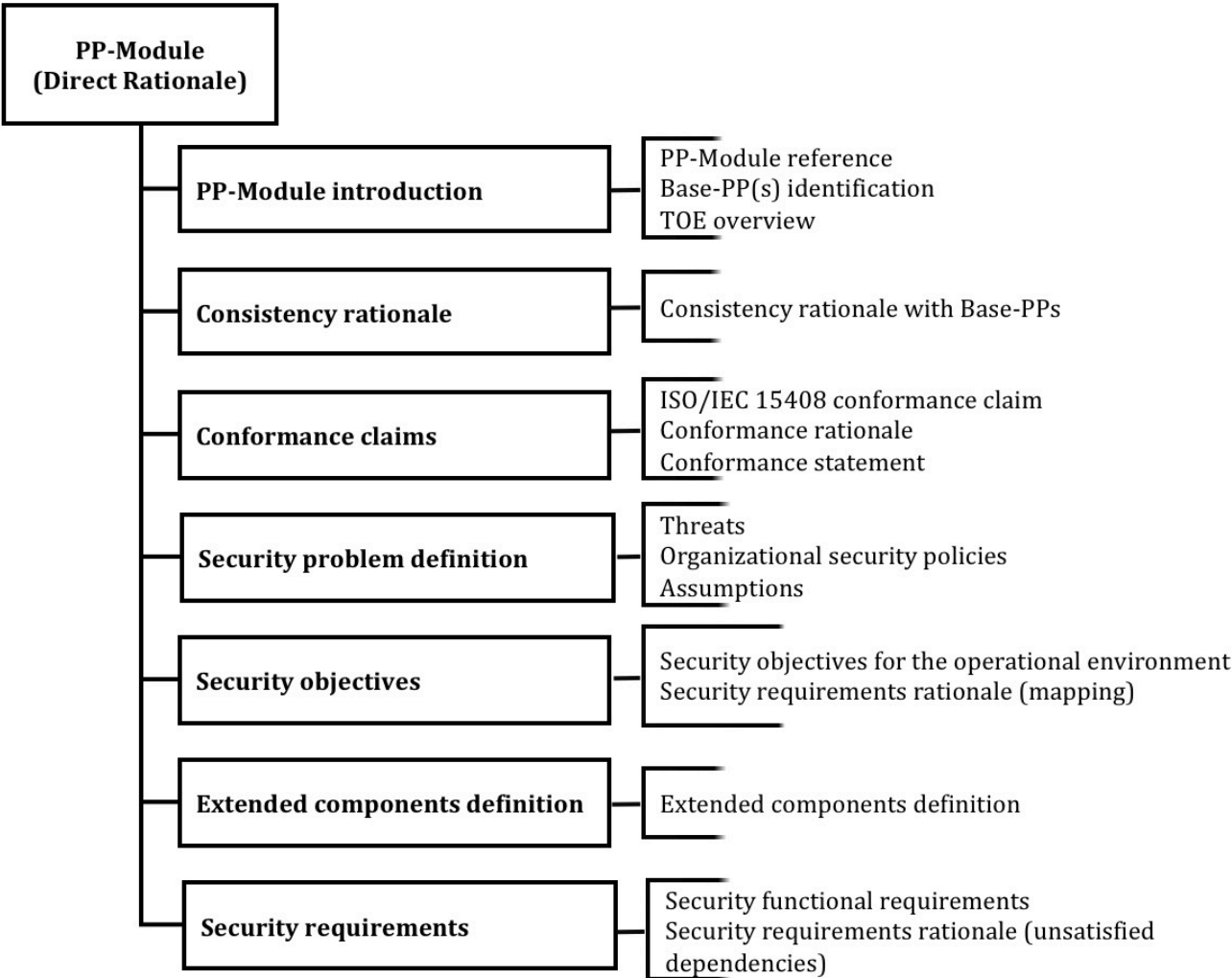


Figure B.6 — Direct Rationale PP-Module

B.3.4 Guidance for inclusion of SPD-elements from Base-PP

In order to limit the amount of information contained in the PP-Module, the PP-Module editors **may** apply the following rules.

Let E, O and R belong to the SPD, the Security Objectives, and the security functional requirements of a Protection Profile Q, respectively, with E mapped to O and O mapped to R.

Let P be a PP-Module and let Q be one of the Base-PPs of P. P has to satisfy the following condition:

E, O, R, and the mappings between them **may can** belong to P only if at least one of these SPD-elements is linked to a new SPD-element in P, that is

- Either there is a new SPD-element E' in the SPD of P such that E' is mapped to O, or
- There is a new objective O' in P such that E is mapped to O' or O' is mapped to R, or
- There is a new requirement R' in P such that O is mapped to R'.

That is, a PP-Module would not contain portions of Base-PPs unless they are required to fulfil new needs. Here, refined SPD-elements are considered new.

B.4 Specification of PP-Configurations

B.4.1 Mandatory content of a PP-Configuration

The content of a PP-Configuration is summarized below in Figure B.6 and explained in detail in Annexes B.4.1.1 through B.4.1.4. A PP-Configuration contains:

- a PP-Configuration reference that uniquely identifies the PP-Configuration,
- a Components statement that identifies the PPs, Base-PPs and the PP-Modules composing the PP-Configuration,
- a Conformance statement, that specifies whether the conformance of STs to this PP-Configuration has to be exact, strict, or demonstrable,
- A SAR statement, specifying the SAR package, or a list of the security assurance components selected that are applicable to the PP-Configuration.

NOTE An SAR package can be an EAL drawn from ISO/IEC 15408-5.

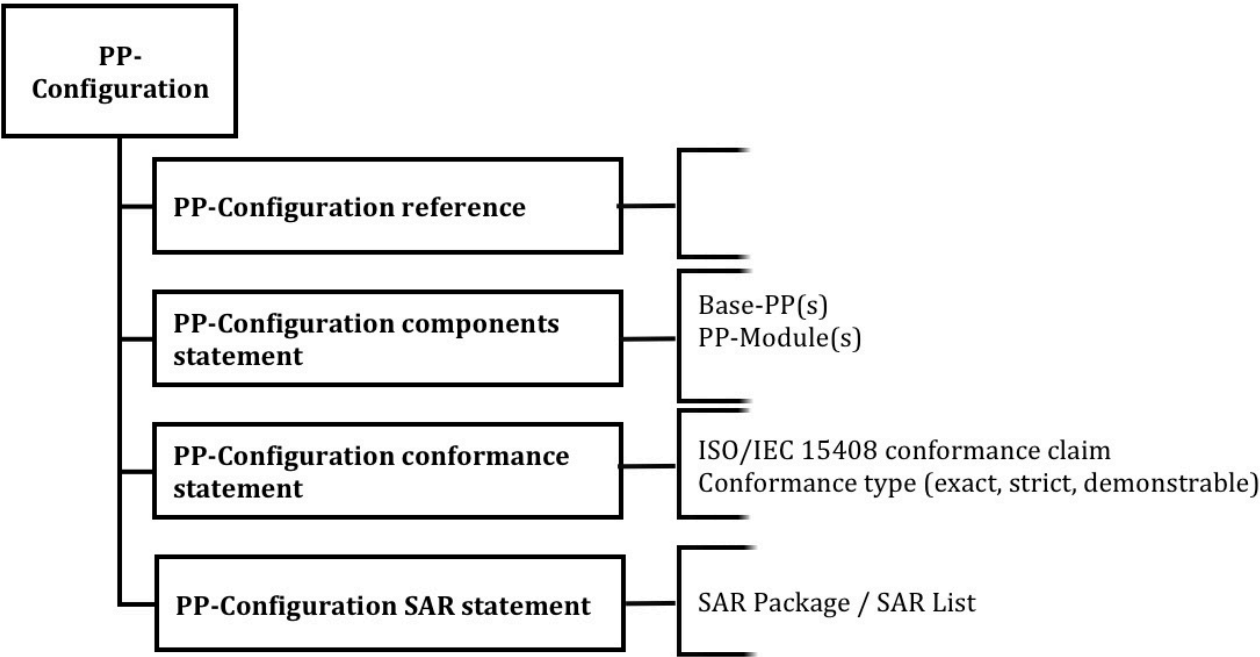


Figure B.7 — Content of a PP-Configuration

B.4.1.1 PP-Configuration reference

The PP-Configuration reference provides a clear and unambiguous identification, usually made of a title, version number, author, and the publication date.

The PP-Configuration reference will be used to index the document in catalogues.

B.4.1.2 PP-Configuration components statement

The PP-Configuration components statement identifies the PPs, Base-PPs and the PP-Modules that compose the PP-Configuration.

The PP-Configuration components statement must include at least all PPs and Base-PPs referenced in the PP-Modules. If the PP-Module specifies alternative sets of Base-PPs, only one of these sets must be referred to in the PP-Configuration.

B.4.1.3 PP-Configuration conformance claims and conformance statement

B.4.1.3.1 General

The conformance claims section of a PP-Configuration describes how the PP-Configuration conforms with ISO/IEC 15408-2 and ISO/IEC 15408-3.

The PP-Configuration conformance statement specifies whether the conformance to this PP-Configuration by an ST is one of exact, strict, or demonstrable.

B.4.1.3.2 Exact conformance

If one Base-PP in the PP-Configuration has an exact conformance statement, then all Base-PPs, and therefore all the PP-Module(s) in the PP-Configuration must also have exact conformance statements.

4206 Further, all Base-PPs and PP-Modules in the PP-Configuration **must** allow all other Base-PPs and PP-
 4207 Modules to be combined in their respective conformance statements. This is illustrated in Figure B.8

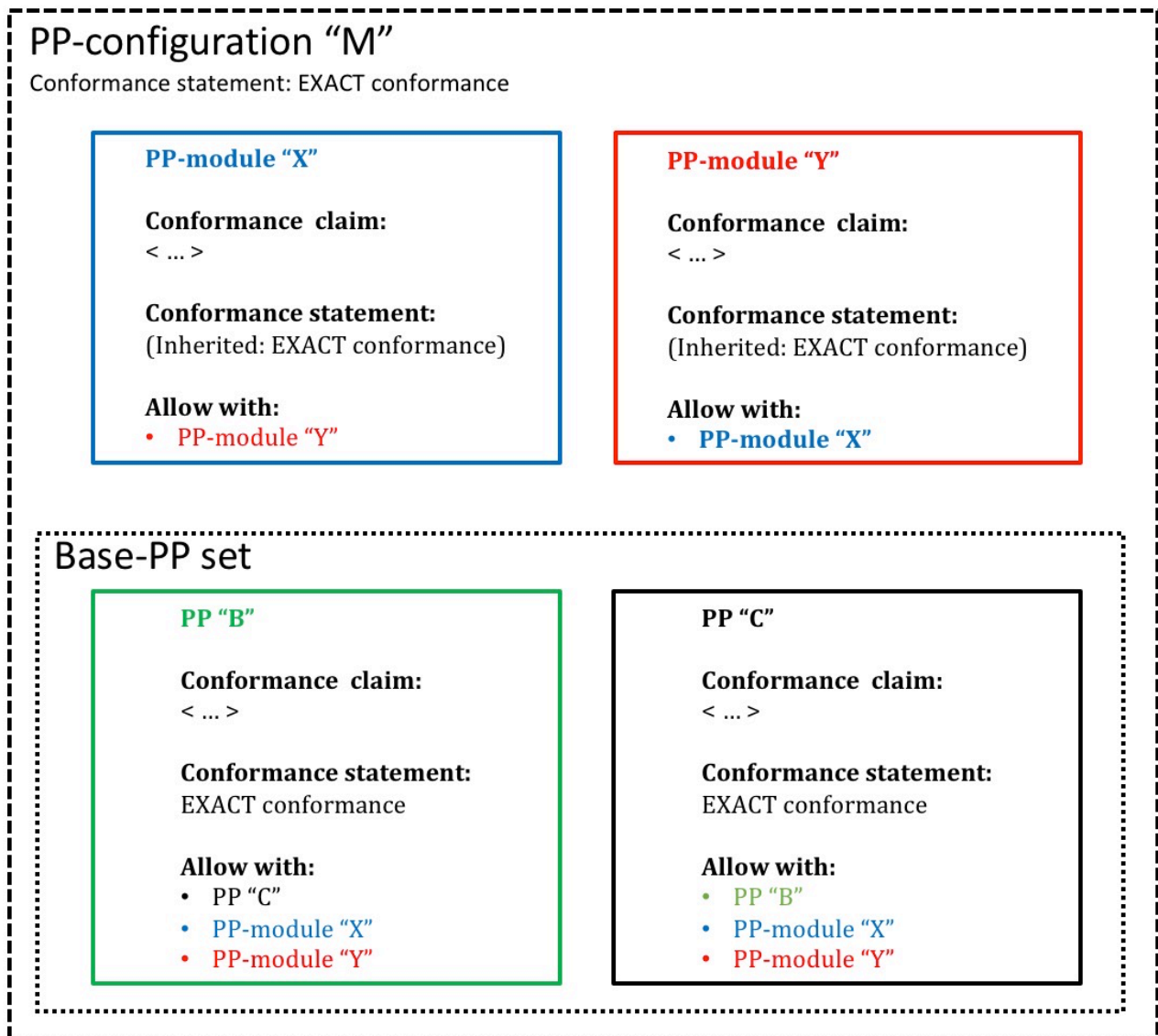


Figure B.8 — PP-Configuration and exact conformance

EXAMPLE

A PP-Configuration requires exact conformance in its conformance statement because exact conformance is required in both Base-PPs, and is therefore inherited by the PP-Modules. PP-Modules X and Y both have an identical Base-PP set: PP B and PP-C both of which require exact conformance. The following statements (shown in the diagram) **must** be true for this to be an evaluable PP-Configuration with a conformance statement of "exact conformance":

- The PP-Modules inherit the conformance statement from their Base-PPs, so their conformance statement is exact conformance.
- The PP-Configuration **must** require exact conformance since the PP-Modules require exact conformance.
- PP B **must** specify in its conformance statement that it is allowed to be used with PP C, PP-Module X, and PP-Module Y.
- PP C **must** specify in its conformance statement that it is allowed to be used with PP B, PP-Module X, and PP-Module Y.
- PP-Module X **must** specify in its conformance statement that it is allowed to be used with PP-Module Y.

- f) PP-Module Y **must** specify in its conformance statement that it is allowed to be used with PP-Module X.

Any ST that claims conformance to the PP-Configuration **shall must** conform to the conformance type required in the conformance statement of the PP-Configuration.

B.4.1.4 PP-Configuration SAR statement

The SAR statement specifies the set of SARs applicable to any product evaluation with a ST that claims conformance to this PP-Configuration.

EXAMPLE

An example of a set of SARs is an EAL predefined in ISO/IEC 15408-5

B.4.2 Using a PP-Configuration

PP-Configurations address the specific needs of groups of users, consumers, organizations, etc.

An instantiated PP-Configuration can be used in the same way as a standard Protection Profile, as explained in section B.4.4.

Editors' Note:

The word "instantiated" was added. Since otherwise the above statement is incorrect since a PP-Configuration is a collection of meta-data in regard to an allowed set of PPs and PP-Modules. So, a PP-Configuration cannot be used like a PP!

B.4.3 Evaluation of a PP-Configuration

PP-Configurations **may can** be evaluated.

The assurance components for PP-Configuration evaluation, defined in ISO/IEC 15408-3:20XX Clause 8: Class ACE are the following: ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_ECD.1, ACE_OBJ.1, ACE_REQ.1, ACE_MCO.1 and ACE_CCO.1.

Editors' Note:

1. This reference to particular content of the standard means that we have to give a dated reference.

2. Other parts of Annex "B" did not discuss evaluation as a topic.

Editors suggest either to remove this subclause or add similar subclause to the other parts of the annexes to discuss evaluation.

B.4.4 Interpretation of PP-Configuration as a PP

B.4.4.1 General

Once evaluated, the instantiation of a PP-Configuration **can** be refined and used in the same way as a PP. This sub-clause, B.4.4, explains how to combine the content of the PP-Module(s), Base-PP(s) and PPs of a PP-Configuration so as to interpret it as a single PP.

The consistency analysis performed during a PP-Configuration's evaluation ensures that the combination is valid.

B.4.4.2 TOE type

The TOE type of the PP is constituted from the TOE type of the PPs and or Base-PP(s) with any additions introduced by the TOE types of the PP-Module(s).

The evaluation of an instantiated PP-Configuration ensures that it forms a consistent TOE type.

B.4.4.3 Conformance claims and conformance statement

B.4.4.3.1 General

The conformance claims of the PP instantiated from a PP-Configuration **must** contain:

- The edition of the ISO/IEC 15408 series, and if ISO/IEC 15408-2 and ISO/IEC 15408-3 have been extended or not;
- If the PP includes evaluation methods and activities, then a conformance claim to ISO/IEC 15408-4 is made;

Editors' Note:

See WD2 US/NIAP26 ^

Editors request comments from other NBs in regard to IF evaluation methods and activities may be included in a PP.

- The conformance to any other PP(s) or PP-Modules whose conformance is claimed in PP(s) of the PP-Configuration.
- The conformance to SAR packages/lists, including any pre-defined EALs, from the PPs of the PP-Configuration.
- The conformance to functional packages from the Base-PPs and any PP-Modules.

NOTE 1 The issue of two or more PPs with different conformance statements has to be dealt with in the same way that an ST conformant to all those PPs would.

NOTE 2 The issue of two or more PPs with different SAR packages such as EALs has to be dealt with just as in an ST conformant to all those PPs would, i.e. the PP **must** claim the minimum set of SARs (such as an EAL) of all the included PPs).

NOTE 3 The issue of two or more PPs with different functional packages has to be dealt in the same way that an ST conformant to all those PPs would.

B.4.4.3.2 Exact Conformance

If the PP-Module inherits a conformance claim from a set of Base-PPs of exact conformance, then the PP-Module **may** lists in its conformance statement a set of other PP-Modules that are allowed to be specified in a PP- Configuration, in combination with the Base-PPs, with that PP-Module.

A PP with an exact conformance statement is not allowed to be combined with PPs with other types of conformance.

NOTE This maintains the exact conformance concept that the PP-Module authors have control over which other requirements **can be** specified in combination with the requirements specified in their PP-Module.

B.4.4.4 Security problem definition

The SPD of the PP **should** contains the union of the SPD-elements from the PPs, Base-PP(s) and PP-Module(s) of the PP-Configuration.

B.4.4.5 Security Objectives

The Security Objectives of the PP **should** contains the union of the Security Objectives from the PPs, Base-PP(s) and PP-Module(s) of the PP-Configuration.

NOTE For PP-Configurations following a Direct Rationale approach, then the Security Objectives would not contain any Security Objectives for the TOE.

B.4.4.6 Extended functional components definition

The extended functional components of the PP **should** contain all of the extended functional components / SFRs from the PPs, Base-PP(s) and PP-Module(s) of the PP-Configuration.

B.4.4.7 Security functional requirements

The set of security functional components and/or SFRs of the PP contains:

- all the security functional components and/or SFRs from the PP-Module(s) of the PP-Configuration.

- 4291 — all the security functional components and/or SFRs from the PPs and Base-PP(s) except those
4292 which are refined in the PP-Module(s). This ~~may~~ can include selection-based SFRs from the
4293 Base-PP(s).
- 4294 — all the security functional components and/or SFRs from functional packages claimed in the PP-
4295 Configuration.
- 4296 The consistency analysis performed during a PP-Configuration's evaluation ~~should~~ ensures that this set
4297 of SFRs is valid.

Annex C (informative)

Specification of Packages

Editors' Note:

The 2018 Directives have clarified the normative/informative status of Annexes

Note that informative annexes may contain **optional** requirements, however the main clauses would then describe in which case the option could be taken.

This Annex is informative. The various requirements and permissions appearing in this annex,

Either need to be moved in the corresponding normative clauses of 15408-1, -2 or -3;

or the verbal form needs to be changed.

The verbal forms used by ISO are very specific.

— Requirement: shall or shall not

— Recommendation: should or should not

— Permission: may or may not

— Possibility and capability: can or cannot

— External constraint: "must"

Additionally, we should consider verifying that any requirements, recommendations and permissions are actually present as SARs or CEM activities.

More information on verbal forms and the annex statuses are found in the latest directives at:

<http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype>

C.1 Goal and structure of this Annex

The goal of this annex is to give the requirements for packages. This annex does not define evaluation criteria since packages are not separately evaluated.

Editors' Note:

For PPs and STs the requirements for structure etc are embodied in the ASE and APE criteria given in part 3.

Editors acknowledge that WD2 US/NIAP64 which asked that similar criteria be developed for evaluating packages was accepted:

C.2 Structure of packages and package families

C.2.1 General

Figure C.1 shows the structure of a package family. Each part is discussed in the following subclauses.

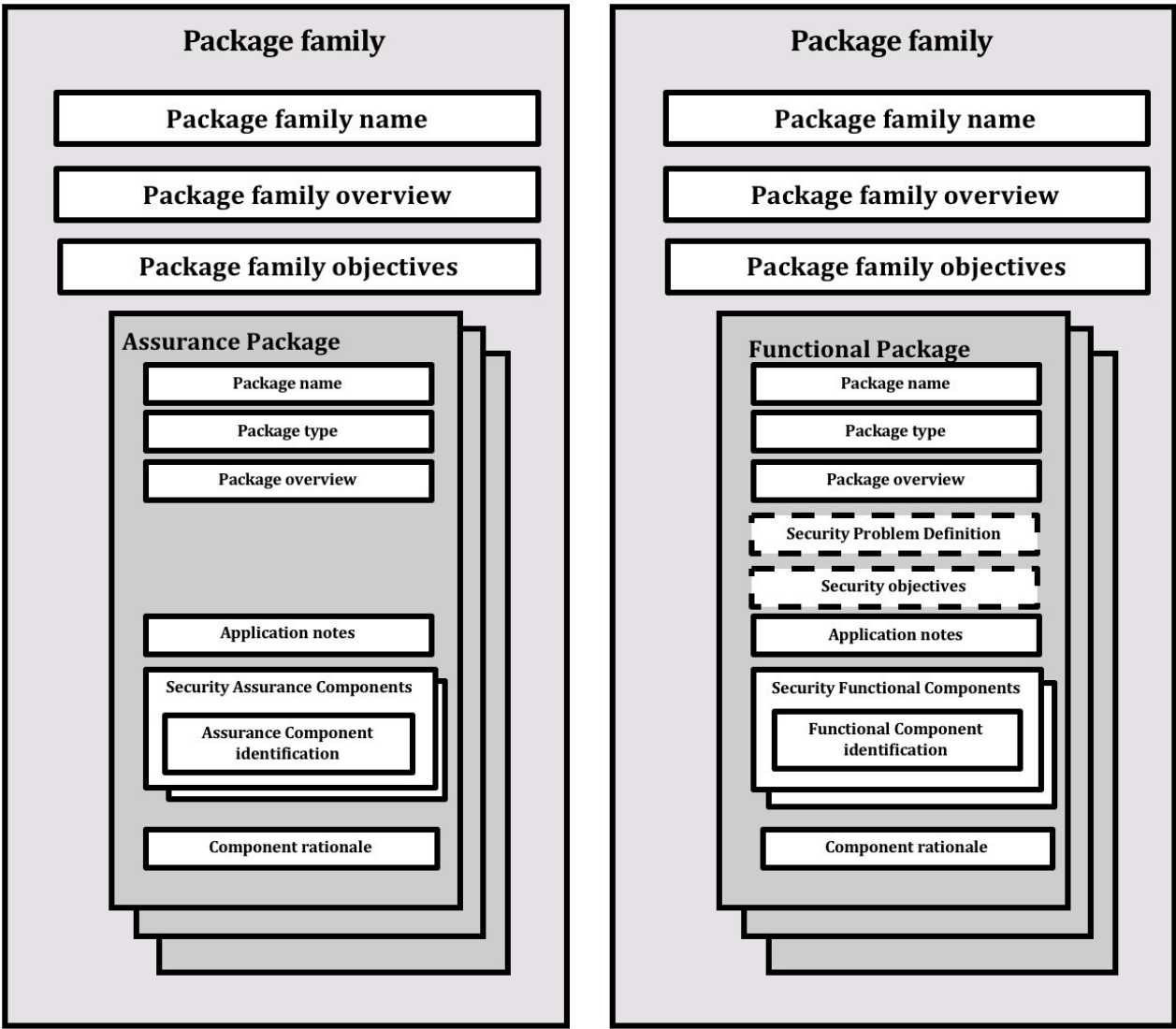


Figure C.1 — The structure of a package family with assurance or functional packages

C.2.2 Package family name

Packages with related objectives ~~may~~ can optionally be presented as a family of packages. In this case, the package family name is mandatory and the package family sponsor ~~should~~ endeavors to allocate a unique name.

Packages of SARs and packages of SFRs ~~shall not~~ cannot be mixed in the same package family.

C.2.3 Package family overview

Packages presented as a family of packages ~~shall~~ must contain a section giving an overview of the family, describing the family at a high-level.

C.2.4 Package family objectives

The objectives section of the package family presents the intent of the family.

C.2.5 Package identification

The identification ~~shall~~ must include:

- a) the package name. The name ~~should~~ provides a unique descriptive information about the intent of the package;
- b) package version information;

- c) last updated date;
- d) sponsor;
- e) reference to the edition of the ISO/IEC 15408 series that is used.

The package ~~may~~ can also be given a short name.

EXAMPLE Evaluation Assurance Level 1 is also known as "EAL 1"

NOTE For those packages defined in ISO/IEC 15408-5, items b) – e) are implicit in the edition information of ISO/IEC 15408-5.

C.2.6 Package type

A package ~~shall~~ must be identified as one of the following types:

- a) Functional package; or
- b) Assurance package.

C.2.7 Package overview

Packages ~~shall~~ must contain a section giving a high-level overview and the intent of the package.

C.2.8 Security problem definition

Assurance packages ~~shall not~~ must not contain this section.

Functional packages ~~may~~ can include this section.

This section ~~shall~~ must include any threats, organizational security policies and assumptions which describe the security problem addressed by the functional package,

In the case of a functional package used for direct rationale PPs/STs TOE Security Objectives ~~must not~~ be included.

C.2.9 Security objectives

The Security Objectives section of a functional package ~~shall~~ must present any additional TOE Security Objectives or Security Objectives for the operational environment derived from the SPD.

C.2.10 Application notes

The inclusion of application notes is optional. The application notes, if present, contains information of particular interest to users of the package. The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention ~~may~~ can be required.

For functional packages, any additional audit and management requirements relating to the SFRs included in the package ~~must~~ be specified in the Application notes section

NOTE Users of packages include PP and ST authors, integrators, and evaluators.

C.2.11 Components (either SFRs or SARs)

The SFRs, potentially including selection-based SFRs, or the SARs included in the package are given. This section also provides the rationale for the selection of the requirements.

Editors' Note:

Further comments are requested in order to determine the best way to address optional requirements.

A package family ~~shall~~ must contain either assurance packages or functional packages. Different package types ~~shall not~~ must not be mixed in the same package family.

Annex D (informative)

Guidance for Operations

D.1 Introduction

As described in this document, Protection Profiles and Security Targets contain pre-defined security requirements, as well as providing PP and ST authors the ability to extend the component lists in some circumstances.

D.2 Examples of operations

The four types of operations are given in 7.2. Examples of the various operations are described below:

D.2.1 The iteration operation

As described in 7.2.1, the iteration operation **may can** be performed on every component. The PP/ST author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component is different from all other iterations of that component, which is realized by completing assignments and selections in a different way, or by applying refinements to it in a different way. Different iterations **should be** are uniquely identified to allow clear rationales and tracings to and from these requirements.

EXAMPLE A typical example of iteration is:

FCS_COP.1 Cryptographic operation being iterated twice in order to require the implementation of two different cryptographic algorithms. An example of each iteration being uniquely identified is:

Cryptographic operation (RSA and DSA signatures) (FCS_COP.1(1))

Cryptographic operation (TLS/SSL: symmetric operations) (FCS_COP.1(2))

D.2.2 The assignment operation

As described in 7.2.2, an assignment operation occurs where a given component contains an element with a parameter that **may can** be set by the PP/ST author. The parameter **may can** be an unrestricted variable, or a rule that narrows the variable to a specific range of values.

EXAMPLE

An example of an element with an assignment is:

FIA_AFL.1.2 "When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions]."

D.2.3 The selection operation

As described in 7.2.3 the selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

EXAMPLE An example of an element with a selection is:

FPT_TST.1.1 "The TSF **shall** run a suite of self-tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test **should** occur]] to demonstrate the correct operation of..."

7.2.3 also describes the notion of a selection-based SFR. The following is an example of such an SFR; FTP_ITC.1.1 is the SFR with the selection and FCS_IPSEC.1 is the selection-based SFR.

EXAMPLE

FTP_ITC.1.1 The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between...

Application Note:

In the selection for FTP_ITC.1.1, the ST author selects the mechanism or mechanisms supported by the TOE, and then ensures that the selection-based requirements in Appendix B of this PP that correspond to the selected mechanism or mechanisms are included in the ST.

Appendix B (of the example PP)

The following SFRs are included in the ST if the ST author selects “IPsec” in FTP_ITC.1.1:

FCS_IPSEC.1 [...]

D.2.4 The refinement operation

As described in 7.2.4, the refinement operation **can** be performed on every requirement. The PP/ST author performs a refinement by altering that requirement.

EXAMPLE An example of a valid refinement is:

FIA_UAU.2.1 “The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.” being refined to “The TSF shall require each user to be successfully authenticated by username/password before allowing any other TSF-mediated actions on behalf of that user.”

The first rule for a refinement is that a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP/ST (i.e. a refined requirement **must** be “stricter” than the original requirement)

The only exception to this rule is that a PP/ST author is allowed to refine a SFR to apply to some but not all subjects, objects, operations, security attributes and/or external entities.

EXAMPLE An example of a such an exception is:

FIA_UAU.2.1 “The TSF **shall** require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.” being refined to “The TSF **shall** require each user **originating from the internet** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.”

The second rule for a refinement given is that the refinement **shall must** be related to the original component. For example, refining an audit component with an extra element on prevention of electromagnetic radiation is not allowed.

A special case of refinement is an editorial refinement, where a small change is made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar, or to make it more understandable to the reader. This change is not allowed to modify the meaning of the requirement in any way.

EXAMPLE An example of an editorial refinements is:

the SFR FPT_FLS.1

“The TSF **shall** continue to preserve a secure state when the following failures occur: **breakdown of one CPU**” could be refined to FPT_FLS.1

“The TSF **shall** continue to preserve a secure state when the following failure occurs: **breakdown of one CPU**” or even FPT_FLS.1

“The TSF **shall** continue to preserve a secure state when **one CPU breaks down**”.

D.3 Organization of components

ISO/IEC 15408-2 and ISO/IEC 15408-3 have organized the components in into hierarchical structures:

— Classes, consisting of

- Families, consisting of
- Components, consisting of
- Elements.

This organization into a hierarchy of class - family - component - element is provided to assist consumers, developers, and evaluators in locating specific components.

The ISO/IEC 15408 series present functional and assurance components in the same general hierarchical style and use the same organization and terminology for each.

D.3.1 Class

EXAMPLE An example of a class is the FIA: Identification and authentication class that is focused at identification of users, authentication of users and binding of users and subjects.

D.3.2 Family

EXAMPLE An example of a family is the User authentication (FIA_UAU) family which is part of the FIA: Identification and authentication class. This family concentrates on the authentication of users.

D.3.3 Component

EXAMPLE An example of a component is FIA_UAU.3 Unforgeable authentication which concentrates on unforgeable authentication.

D.3.4 Element

EXAMPLE An example of an element is FIA_UAU.3.2 which concentrates on the prevention of use of copied authentication data.

D.4 Extended components

D.4.1 How to define extended components

Whenever a PP/ST author defines an extended component, this has to be done in a similar manner to the existing ISO/IEC 15408 series components: clear, unambiguous and evaluable (it is possible to systematically demonstrate whether a requirement based on that component holds for a TOE). Extended components **must** use similar labelling, manner of expression, and level of detail as the existing ISO/IEC 15408 series components.

The PP/ST author also has to make sure that all applicable dependencies of an extended component are included in the definition of that extended component. Examples of possible dependencies are:

- a) if an extended component refers to auditing, dependencies to components of the FAU: Security audit class **may might** have to be included;
- b) if an extended component modifies or accesses data, dependencies to components of the Access control policy (FDP_ACC) family **may might** have to be included;
- c) if an extended component uses a particular design description a dependency to the appropriate ADV: Development family **may might** have to be included.

EXAMPLE An example of the ADV development family is the Functional Specification.

In the case of an extended functional component, the PP/ST author also has to include any applicable audit and associated operations information in the definition of that component, similar to existing ISO/IEC 15408-2 components. In the case of an extended assurance component, the PP/ST author also

4462 has to provide suitable evaluation method for the component, similar to the method provided in
4463 ISO/IEC 18045.

4464 Extended components ~~may~~ can be placed in existing families, in which case the PP/ST writer has to
4465 show how these families change. If they do not fit into an existing family, they ~~shall~~ must be placed in a
4466 new family. New families have to be defined similarly to those given in ISO/IEC 15408-2 or ISO/IEC
4467 15408-3.

4468 New families ~~may~~ can be placed in existing classes in which case the PP/ST writer has to show how
4469 these classes change. If they do not fit into an existing class, they ~~shall~~ must be placed in a new class.
4470 New classes have to be defined similarly to those defined in ISO/IEC 15408-2 or ISO/IEC 15408-3.

Annex E (informative) PP Conformance

E.1 General

A PP is intended to be used as a “template” for an ST. That is: the PP describes a set of user needs, while an ST that conforms to that PP describes a TOE that satisfies those needs.

NOTE 1: It is also possible for a PP to be used as a template for another PP that specifies either strict or demonstrable conformance type. That is, PPs specifying either strict or demonstrable conformance can claim conformance to other PPs. This case is completely similar to that of an ST vs. a PP. For clarity, this annex describes only the PP/ST case, but it holds also for the PP/PP case.

The ISO/IEC 15408 series does not allow any form of partial conformance, so if PP conformance is claimed, the PP/ST **must** conform to the referenced PP(s) or PP-Configuration.

NOTE 2: In the case of selection-based SFRs, the inclusion or exclusion of these types of SFRs as outlined in ISO/IEC 15408-2 is still considered to be conformant with the PP.

The ISO/IEC 15408 series defines three types of conformance: “demonstrable”, “strict” and “exact” where the type of conformance allowed is determined by the PP. That is, the PP states, in accordance with B.2.3, what the allowed types of conformance for the derivative ST/PPs are.

As indicated in 9.2.1, if a PP specifies exact conformance, then an ST/PP can only claim conformance to that PP, either by itself or when it is included in a PP-Configuration that also requires exact conformance.

The distinction between demonstrable, strict, and exact conformance when such conformance statements are contained in multiple PPs to which a PP/ST is claiming conformance is applicable to each PP to which an PP/ST **can** claim conformance on an individual basis. This **can** mean that the PP/ST conforms strictly to some other PPs and demonstrably to other PPs. A PP/ST is only allowed to conform to a PP in a demonstrable manner if the PP explicitly allows this. However, a PP/ST **can** always conform either exactly or strictly to a PP that requires either demonstrable or strict conformance.

NOTE 3: A PP/ST is only allowed to conform to a PP in a demonstrable manner if the PP explicitly allows this. This means that PP/STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP. In principle that means that the PP/ST can contain statements that vary from the PP, provided that overall the ST levies the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

E.2 Demonstrable conformance

Demonstrable conformance is orientated to the PP sponsor who requires evidence that the ST is a suitable solution to the generic security problem described in the PP.

Where there is a clear subset- superset type relation between PP and ST in the case of strict conformance, the relation is less clear-cut in the case of demonstrable conformance. STs claiming conformance to the PP **must** offer a solution to the generic security problem described in the PP.

However, claiming conformance is allowed only in the case that the ST imposes the same, or more, restrictions on the TOE and the same, or less, restrictions on the operational environment of the TOE.

E.3 Strict conformance

Strict conformance is oriented to the PP sponsor who requires evidence that the requirements in the PP are met, that the ST is an instantiation of the PP, though the ST could be broader than the PP. In essence, the ST specifies that the TOE does at least the same as in the PP, while the operational environment does at most the same as in the PP.

EXAMPLE

A typical example of the use of strict conformance is in selection-based purchasing where an IT product's security requirements are expected to match those specified in the PP.

An ST instantiating strict conformance to a PP **can** still introduce additional restrictions to those given in the PP.

E.4 Exact conformance

Exact conformance is oriented to the PP sponsor who requires evidence that the requirements in the PP are met, and that the ST is an instantiation of exactly those requirements (SFRs) without including additional functionality. In essence, the ST specifies that the TOE does what is required in the PP without making additional claims.

If “exact” conformance is selected, the PP author also has the option of specifying the following information:

- a) Other PPs to which an ST can claim conformance in combination with the subject PP and still maintain exact conformance;
- b) Packages to which an ST can claim conformance in combination with the subject PP and still maintain exact conformance;
- c) PP-Modules that can specify the subject PP as a Base-PP for use with that PP-Module in a PP-Configuration and still maintain exact conformance;

The ISO/IEC 15408 series allows STs to claim conformance to multiple PPs.

NOTE PPs **can** also claim conformance to multiple PPs, but if a PP requires exact conformance then another PP **cannot** claim conformance to the subject PP, so the multiple-PP case is not applicable.

In the case where a PP requires exact conformance, this has the potential to circumvent the intent behind exact conformance, which gives the PP author more control over the functionality and assurance provided for conformant STs than either strict or demonstrable conformance does.

EXAMPLE 1 If an ST **can** claim conformance to PP A (which requires exact conformance) and to PP B (which requires demonstrable conformance) at the same time, this would pull in SFRs which PP A's author did not explicitly approve to be used in combination with PP A's functionality when an ST claims conformance to PP A.

To address this issue, the conformance statement in the PP, described in B.2.3, may also include a statement specifying which PPs an ST author may simultaneously claim conformance to with the subject PP: the “Allow with” statement. All identified PPs **must** require exact conformance in their conformance statement and **must** also list the subject PPs, and all other PPs being claimed, in their conformance statement.

An example is given to clarify this concept (an ST claiming conformance to multiple PPs).

EXAMPLE

For the ST example, suppose PP B’s authors wanted to allow STs to claim conformance to it, and also to allow conformance claims to it in combination with PP C. This situation is pictured in Figure E.1

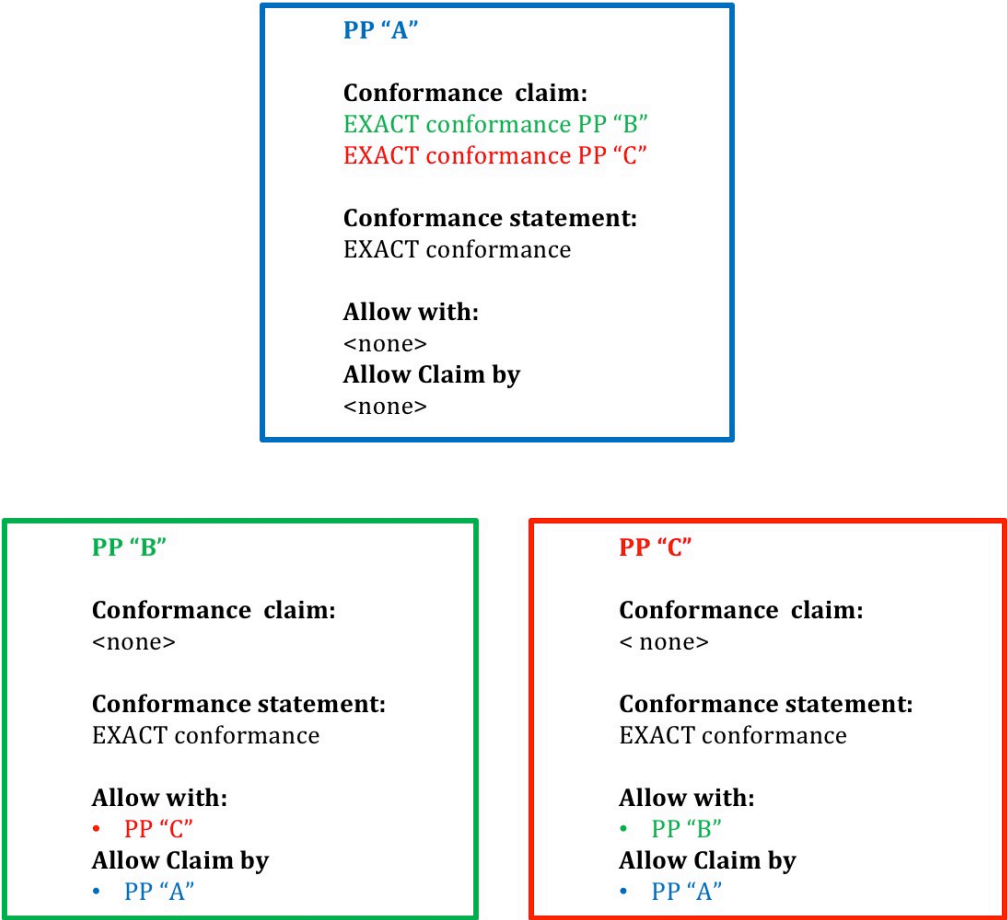


Figure E.1 — Exact conformance of an ST to multiple PPs

- Then the following would have to be true:
- a) Both PP B and PP C would have to specific exact conformance in their conformance statement.
 - b) PP B would list PP C as allowed with PP B in its conformance statement.
 - c) PP C would list PP B as allowed with PP C in its conformance statement.

If any of these statements did not hold, then the ST could not claim exact conformance to PPs B and C.

This concept also extends to PP-Modules and the PP-Configurations. A PP-Module can identify a set of Base-PPs; if one of the identified Base-PPs has a conformance statement of exact conformance, then all of the Base-PPs specified by the PP-Module must also have conformance statements specifying exact conformance. Further, in order to ensure that the PP-Modules are allowed for use with the Base-PP, each Base-PP specifies in its conformance statement the PP-Modules that are allowed to specify it as a Base-PP for use in a PP-Configuration.

NOTE The reverse is not true; a PP-Module does not need to specify any of its Base-PPs in the Allow with statement because it has implicitly done so by defining the PP as a Base-PP.

Furthermore, a PP-Module also specifies which other PP-Modules or Protection Profiles in the PP-Configuration that are not included as one of the PP-Module’s Base-PPs can be used in combination with it in a PP-Configuration.

In exact conformance a PP can only claim conformance to one PP-Configuration. However, an ST can claim conformance to more than one PP-Configuration.

Bibliography

This bibliography contains references to further material and standards that the reader of The ISO/IEC 15408 series **may** find useful. For undated references the reader is recommended to refer to the latest edition of the referenced document.

ISO/IEC standards and guidance

[1] ISO/IEC 8367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

[2] ISO/IEC 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*

[3] ISO/IEC 15446, *Information technology — Security techniques — Guidance for the production of Protection Profiles and Security Targets*

[4] ISO/IEC TR 18018:2010, *Information technology — Systems and software engineering — Guide for configuration management tool capabilities*

[5] ISO/IEC TR 18031:2011, *Information technology — Security techniques — Random bit generation*

[6] ISO/IEC 19608, *Information technology — Security techniques — Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*

[7] ISO/IEC 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems, and applications*

[8] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[9] ISO/IEC 19791, *Information technology — Security techniques — Security assessment of operational systems*

[10] ISO/IEC 19896-1, *IT Security techniques — Competence requirements for information security testers and evaluators: Part 1: Introduction, concepts, and general requirements*

[11] ISO/IEC 19896-3 *IT Security techniques — Competence requirements for information security testers and evaluators: Part 3: Knowledge, skills, and effectiveness requirements for ISO/IEC 15408 evaluators*

[12] ISO/IEC 20004, *Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*

[13] DRAFT ISO/IEC TR 22216, *Information technology — Security techniques — Introductory guidance on evaluation for IT security*

Editors' Note:

Note that while in draft, this companion document to 15408/18045 revision 4 aims to provide a useful overview of changes to the ISO revision audience and is updated in step with the ISO/IEC 15408/18045 revision

The editors expect that ISO/IEC 22216 will be published concurrently with this standard

[14] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[15] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[16] ISO/IEC 27034, *Information technology — Security techniques — Application security*

Other standards and guidance

[16] CCDB. *Composite product evaluation for Smart Cards and similar devices*, April 2012, V1.2 Available at <http://www.commoncriteriaportal.org/files/supdocs/CCDB-2012-04-001.pdf>

Catalogues of PPs and evaluated products

- 4601 [17] Common Criteria portal: Certified Products, available at
4602 <http://www.commoncriteriaportal.org/products/>
- 4603 [18] Common Criteria portal: Protection Profiles, available at
4604 <http://www.commoncriteriaportal.org/pps/>
- 4605 [19] Common Criteria portal: Collaborative Protection Profiles, available at
4606 <http://www.commoncriteriaportal.org/pps/?cpp=1>