



REPLACES:

ISO/IEC JTC 1/SC 27/WG 3
Information technology - Security techniques - Security evaluation, testing and specification
Convenorship: AENOR, Spain, Vice-convenorship: JISC, Japan

DOC TYPE: working draft

TITLE: Text for ISO/IEC 4th WD 22216 — Information technology — Security techniques — Evaluation Criteria for IT security — Introductory guidance on evaluation for IT security

SOURCE: Project editor

DATE: 2018-12-25

PROJECT: TR 22216

STATUS: In accordance with WG recommendation 11 and 12 (contained in SC 27 N18820) of 57th SC 27/WG 3 meeting held in Gjøvik, Norway, 30th September – 4th October 2018, this document is being circulated to experts and liaison organizations for study and comment closing by **2019-02-21**.

PLEASE submit your comments on the hereby attached document via the SC 27/WG 3 Consultations at:
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3>

PLEASE NOTE: For comments please use the SC 27 EXPERT COMMENTING TEMPLATE separately attached to this document.

ACTION: COMM

DUE DATE: 2019-02-21

DISTRIBUTION: M. Bañón, N. Kai, WG 3 Experts

MEDIUM: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3>

NO. OF PAGES: 1 + 108

1 **ISO/IEC JTC 1/SC 27/WG 3 N1633**

2 **Date: 2018-12-21**

3 **ISO/IEC TR 22216:####(EN)**

4 **ISO/IEC JTC 1/SC 27 IT Security techniques**

5 **Secretariat: DIN**

6 **IT Security techniques — Evaluation criteria for IT security — Introductory**
7 **guidance on evaluation for IT security**

8 **Techniques de sécurité IT — Critères d'évaluation pour la sécurité des**
9 **technologies de l'information — Guide d'introduction à l'évaluation de la**
10 **sécurité des technologies de l'information**

11

12 **WD stage**

13

14 **Warning for WDs and CDs**

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

17 Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of
18 which they are aware and to provide supporting documentation.

19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

© ISO 2018, Published in Switzerland

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

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

Editor's notes to Experts:

Editor's conventions for this draft.

Red text in a box are the Editor's comments

Blue text indicates that the text is probably useful only during the revision of ISO/IEC 15408 and ISO/IEC 18045 and should be removed before publication of this document.

Purple text for the multi-assurance level concept introduced in ISO/IEC 15408 CD1

These conventions will be removed in the final document.

39 **Contents**

40	1	Scope.....	1
41	2	Normative references	1
42	3	Terms and definitions.....	2
43	3.1	Terms	2
44	3.2	Abbreviations.....	2
45	4	Using this guidance	2
46	4.1	Using this guidance during the revision of ISO/IEC 15408 and ISO/IEC 18045	2
47	4.2	Using this guidance for transitional information	2
48	5	History of this revision of ISO/IEC 15408 and ISO/IEC 18045.....	2
49	5.1	Key documents.....	2
50	5.2	Categorization of study periods, and other inputs	3
51	5.3	General.....	3
52	6	Main changes to the standard.....	3
53	6.1	Approaches to security evaluation	3
54	6.1.1	The “specification-based” approach	5
55	6.1.2	The “attack-based” approach.....	6
56	6.2	Modularity	7
57	6.2.1	Composition mechanisms	8
58	6.2.2	Evaluation mechanisms for composition.....	9
59	6.2.3	Modularity within a TOE.....	9
60	6.2.4	Packages.....	9
61	6.2.5	Modular Protection Profiles.....	11
62	6.2.6	Multi-assurance Evaluations.....	11
63	6.3	Consistent Standard's Language	15
64	6.4	Differentiation of ISO/IEC 15408: Evaluation Methods	16
65	7	Mapping of evolutions with ISO/IEC 15408 and ISO/IEC 18045	17
66	7.1	Summary	17
67	7.2	Detailed evolutions	17
68	8	Migration from the third to the fourth edition of the ISO/IEC 15408 series.....	25
69	A.1	Vulnerability Assessment.....	26
70	A.2	Clarify & Streamline Evidence Requirements.....	27
71	A.3	Consistent Standard Metrics.....	27
72	A.4	Better use of development models and process.....	28
73	A.4.1	Incremental development	28
74	A.4.2	Other topics to be discussed.....	28
75	A.5	Reposition CEM.....	28
76	A.6	Review Tools and Techniques.....	28
77	A.7	New requirements.....	28
78	1	Introduction.....	32
79	1.1	Executive summary.....	32
80	1.2	Scope.....	32
81	1.3	Audience	32
82	1.4	Normative references	32
83	1.5	Terms and definitions.....	32
84	1.6	Notation	33

85	2	ISO/EC 15408-1 update.....	34
86	2.1	Multi-assurance evaluation.....	34
87	2.2	Security Targets	35
88	2.3	Protection Profiles, PP-Modules and PP-Configurations	36
89	2.3.1	Introduction.....	36
90	2.3.2	Protection Profiles.....	36
91	2.3.3	PP-Modules	36
92	2.3.4	PP-Configurations.....	37
93	2.3.5	Usage of PPs and PP-Configurations in Security Targets	40
94	2.4	Evaluation and evaluation results	42
95	2.5	Annex B – Specification of PPs	43
96	2.6	Annex C – Specification of PP-Modules.....	43
97	2.7	Annex D – Specification of STs.....	43
98	3	ISO/EC 15408-3: Class ACE	44
99	1.1	Introduction.....	44
100	1.2	PP-Module introduction (ACE_INT).....	45
101	1.2.1	Objectives.....	45
102	1.2.2	ACE_INT.1 PP-Module introduction.....	45
103	1.3	PP-Module conformance claims (ACE_CCL).....	47
104	1.3.1	Objectives.....	47
105	1.3.2	ACE_CCL.1 PP-Module conformance claims	47
106	1.4	PP-Module Security problem definition (ACE_SPD).....	49
107	1.4.1	Objectives.....	49
108	1.4.2	ACE_SPD.1 PP-Module Security problem definition.....	49
109	1.5	PP-Module Security objectives (ACE_OBJ).....	50
110	1.5.1	Objectives.....	50
111	1.5.2	Component levelling	50
112	1.5.3	ACE_OBJ.1 Direct Rationale PP-Module Security objectives	50
113	1.5.4	Application notes	50
114	1.5.5	ACE_OBJ.2 PP-Module Security objectives	51
115	1.5.6	Application notes	51
116	1.6	PP-Module extended components definition (ACE_ECD)	52
117	1.6.1	Objectives.....	52
118	1.6.2	ACE_ECD.1 PP-Module extended components definition.....	52
119	1.7	PP-Module security requirements (ACE_REQ).....	54
120	1.7.1	Objectives.....	54
121	1.7.2	Component levelling	54
122	1.7.3	ACE_REQ.1 PP-Module stated security requirements	54
123	1.7.4	ACE_REQ.2 PP-Module derived security requirements.....	56
124	1.8	PP-Module consistency (ACE_MCO).....	58
125	1.8.1	Objectives.....	58
126	1.8.2	ACE_MCO.1 PP-Module consistency.....	58
127	1.9	PP-Configuration consistency (ACE_CCO).....	60
128	1.9.1	Objectives.....	60
129	1.9.2	ACE_CCO.1 PP-Configuration consistency	60
130	3.1	Other assurance classes.....	64
131	1	Background	66
132	2	The concept approach introduction to ISO/IEC 15408-1	68
133	2.1	General action plan (GAP) to get the objective.....	68
134	2.2	What would be the impact of the GAP on the project timetable?	69
135	3	Identification of concepts.....	69
136	3.1	General.....	69
137	3.2	Concepts.....	71

138	3.2.1	Security Model.....	71
139	3.2.2	Assurance.....	72
140	3.2.3	Target of Evaluation, TOE.....	73
141	3.2.4	Evaluation techniques.....	73
142	3.2.5	Taxonomy	74
143	4	Assignment of Terms	75
144			

145 **Foreword**

146 ISO (the International Organization for Standardization) and IEC (the International Electrotechnical
147 Commission) form the specialized system for worldwide standardization. National bodies that are
148 members of ISO or IEC participate in the development of International Standards through technical
149 committees established by the respective organization to deal with particular fields of technical activity.
150 ISO and IEC technical committees collaborate in fields of mutual interest. Other international organiza-
151 tions, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In
152 the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC
153 JTC 1.

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

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

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

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

168 This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcom-
169 mittee SC 27, IT Security techniques.

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

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

173 This is the **first** edition of this document.

174 Introduction

175 This Technical Report will provide guidance and support to those responsible for implementing the
 176 Fourth edition of the ISO/IEC 15408 and ISO/IEC 18045 standards. This edition of the ISO/IEC 15408
 177 and ISO/IEC 18045 standards includes substantial changes from the third edition.

178 During the revision of ISO/IEC 15408 and ISO/IEC 18045, this document will cross reference and
 179 consolidate inputs from the related WG 3/CCDB study periods. It will provide the rationale for their
 180 inclusion or not in the second CD of the standard.

181 As the standards evolve, it is expected that comments and contributions will be made to the project.
 182 These comments and contributions will be disposed following the normal SC 27/WG 3 process.
 183 However, key points from the revision process will be tracked in this document.

184 During the revision of ISO/IEC 15408 and ISO/IEC 18045 the target audience will be the stakeholders
 185 involved in the revision of these standards. This will include the assigned Experts, National Bodies,
 186 liaison organizations, as well as the ISO, IEC, JTC1, and SC27 management.

187 After publication of the standard, the audience for this document will be those with an interest in the
 188 evolution of the ISO/IEC 15408 and ISO/IEC 18045 standards. These include:

- 189 — Security assurance consumers;
- 190 — IT product developers and those authoring Security Targets;
- 191 — Technical community subject matter experts (SMEs) developing Packages, Protection Profiles,
 192 evaluation methodologies, and other supportive documents;
- 193 — Evaluators;
- 194 — Evaluation schemes, and validators;
- 195 — Consultants supporting ISO/IEC 15408 and 18045 work, including developers of supportive
 196 tools;
- 197 — Others, including those involved with mutual recognition arrangements and academia.

198 It is expected that the audience for this transition guidance is familiar with the latest edition of the
 199 standard.

200

201 **Editors' note:**

202 This guide provides insight into the multi-assurance level concept in clause 6.2.6 and provides the latest version of
 203 the contribution in Annex B to facilitate the expert review.

204

205 IT Security techniques — Introductory guidance on evaluation for 206 IT security

207 1 Scope

208 The scope statement is, for now, the statement defined in the New Work Item Proposal (N16885) for this docu-
209 ment.

210 This document will:

- 211 — Follow and track the revision of ISO/IEC 15048 and ISO/IEC 18045;
- 212 — Map the evolutions between the initial version and the revised version;
- 213 — Cross reference and consolidate inputs from study periods and subsequent revision
214 contributions for ISO/IEC 15408/18045 and it will provide a rationale for their inclusion or not
215 in the revised standard;
- 216 — Introduce the break down between ISO/IEC 15408 and ISO/IEC 18045 and new parts of the
217 standard;
- 218 — Propose an evolution path and guidance on how to move from ISO/IEC 15408:2009 and ISO/IEC
219 18045:2008 to the revised new versions.

NOTE TR 22216 summarizes the Dispositions of Comments, instead of trying to map the individual comments. This will notably allow handling large sets of comments sorted by category, and to avoid duplicating the work done in the Dispositions of Comments.

220 2 Normative references

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

224 ISO/IEC 15408-1:2009, *Information technology — IT security techniques — Evaluation criteria for IT*
225 *security — Part 1: Introduction and general requirements*

226 ISO/IEC 15408-2:2008, *Information technology — IT Security techniques — Evaluation criteria for IT*
227 *security — Part 2: Security functional components*

228 ISO/IEC 15408- 3:2008, *Information technology — IT Security techniques — Evaluation criteria for IT*
229 *security — Part 3: Security assurance components*

230 ISO/IEC 18045: 2008, *Information technology — IT Security techniques — Methodology for IT security*
231 *evaluation*

232 ISO/IEC 15408-1:20XX, *Information technology — IT security techniques — Evaluation criteria for IT*
233 *security — Part 1: Introduction and general requirements*

234 ISO/IEC 15408-2: 20XX, *Information technology — IT Security techniques — Evaluation criteria for IT*
235 *security — Part 2: Security functional components*

236 ISO/IEC 15408- 3: 20XX *Information technology — IT Security techniques — Evaluation criteria for IT*
237 *security — Part 3: Security assurance components*

238 ISO/IEC 15408- 4: 20XX, *Information technology — IT Security techniques — Evaluation criteria for IT*
239 *security — Part 4: Framework for the specification of evaluation methods and activities*

240 ISO/IEC 15408- 5: 20XX, *Information technology — IT Security techniques — Evaluation criteria for IT*
241 *security — Part 5: Pre-defined packages of security requirements*

242 ISO/IEC 18045: 20XX, *Information technology — IT Security techniques — Methodology for IT security*
243 *evaluation*

244 **3 Terms and definitions**

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

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

248 — ISO Online browsing platform: available at <http://www.iso.org/obp>

249 — IEC Electropedia: available at <http://www.electropedia.org/>

250 **3.1 Terms**

251 **Terms and definitions specific to this document will be updated as required in the next draft stage.**

252 **3.2 Abbreviations**

253 **Abbreviations specific to this document will be updated as required in the next draft stage.**

254 **4 Using this guidance**

255 **4.1 Using this guidance during the revision of ISO/IEC 15408 and ISO/IEC 18045**

256 This guidance is intended to support those involved in the revision of the ISO/IEC 15408 series and
257 ISO/IEC 18045. As these revisions progress, this document will reflect the changes and may be used to
258 assist readers in their review of the evolutions.

259 During the revision of the standard, this guide will describe the changes made, ensuring that they are
260 traceable to the Study Period inputs as well. For this purpose, this guidance provides, in appendix, a
261 mapping of the experts' contributions to the Study Period. Experts should check that their contributions
262 are reflected appropriately in the current draft of the standard and provide comments accordingly.

263 Comments received on the current draft will be disposed following the usual JTC1 disposition process.

264 **4.2 Using this guidance for transitional information**

265 **This part will be completed during the next stage of the standard. At the moment, the document is mainly used for**
266 **summarising changes as the standard edition progresses and for tracking changes with regard to Study Period**
267 **inputs.**

268 **5 History of this revision of ISO/IEC 15408 and ISO/IEC 18045**

269 **5.1 Key documents**

270 During 2015 and 2016 an ISO/IEC JTC 1/SC 27/WG 3 Study Period was held in liaison with the Common
271 Criteria Development Board (CCDB) that received a great many contributions. The terms of reference
272 and call for contributions were provided in SC27/WG 3 N1258.

273 Two calls for contributions were initiated (see WG 3 N1258 and WG 3 N1317), and a summary of the
274 contributions can be found in WG 3 N1295 and WG 3 N1362.

275 After analysis of the contributions by the Study Period rapporteurs, WG 3 initiated a revision of both
276 ISO/IEC 15408 and ISO/IEC 18045. In addition, two additional parts of 15408 were proposed in New

277 Work Item Proposals (NWIPs). These were balloted within ISO and approval for this change was gained.
278 (SC27 N17025, N17026, N17027, N17028, N17029, and N17023).

279 A call for editors was made, and editors were assigned in April 2017 and were instructed to present the
280 first Working Drafts for distribution to, and consideration by the interested Experts and WG 3 liaisons.
281 WD1 and WD2 have been produced by WG 3.

282 In April 2018, WG 3 decided to move to Committee Draft stage (CD1). The present document integrates
283 the WD2 disposition of comments and changes made to the standard in CD1 documents.

284 In October 2018, WG 3 decided to move to second Committee Draft (CD2). The present document
285 integrates the CD1 disposition of comments and changes made to the standard in CD2 documents. CD1
286 and CD2 have been produced by WG 3.

287 **5.2 Categorization of study periods, and other inputs**

288 This section describes the categorization that the editing team used to review the inputs:

- 289 a) Approaches to security evaluation
- 290 b) Modularity
- 291 c) Consistent Standard's Language
- 292 d) Vulnerability Assessment
- 293 e) Clarify & Streamline Evidence Requirements
- 294 f) Consistent Standard Metrics
- 295 g) Better use of Development models & Process
- 296 h) Differentiation of ISO/IEC 15408

297 The main changes to the standard correspond to categories a), b), c) and h), which are described in
298 clause 6 of the present document. Categories d) to g) are referred to in the Annex.

299 **5.3 General**

300 The following are general considerations for the revision of the standard:

- 301 — Consideration of Common Criteria users, especially existing MRAs, and their stakeholders,
NOTE CCRA and SOG-IS MRA are the only existing recognition arrangements.
- 302 — Continued alignment with the supporting documents developed in the context of the existing
303 MRAs;
- 304 — Consideration of commonly used approaches for the criteria;
- 305 — Provision of transition guidance and explanations of modifications to the standards.

306 **6 Main changes to the standard**

307 **6.1 Approaches to security evaluation**

308 This new version of the standard now supports two different approaches to evaluation, as shown in
309 **Figure 1** hereafter:

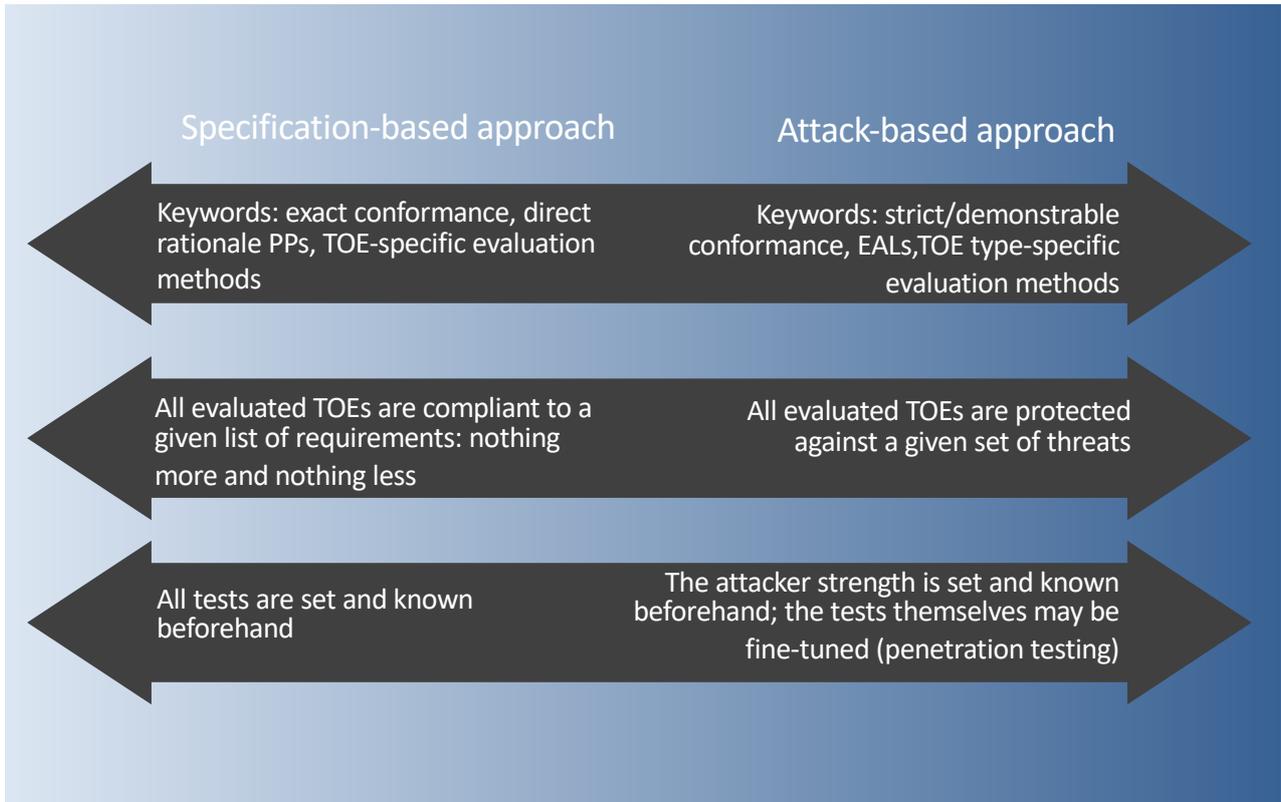


Figure 1 — Specification-based and attack-based approaches

The main differences between them are as follows:

- A new approach, which is called hereafter the “specification-based approach”, consists in defining, at the PP level, the requirements, and the corresponding evaluation activities. This approach:
 - uses exact conformance to Protection Profiles;
 - does not use EALs;
 - may use Direct Rationale Protection Profiles and Security Targets.

This approach is best used when the main expected benefit is to confirm that a TOE meets a set of tests that is known in advance, even if this means that newly relevant attack scenarios are not tested. It also aims to suppress the need of evaluator judgement and to avoid the need to define a tailored test plan during the evaluation: the evaluator works exclusively based on a white list of tests instead of performing TOE-specific penetration testing.

- The standard still supports the evaluation approach used in its previous versions, which is called hereafter the “attack-based approach” (also called “investigative” approach). Notably, this approach:
 - still mostly uses demonstrable or strict conformance;
 - still uses the EAL scale, the AVA_VAN components and the notions of refinement and extended component to define TOE-specific evaluation methodologies;

330 – still uses standard Protection Profiles and Security Targets.

331 This approach is best used in contexts where state-of-the-art and agility with regard to new
 332 attacks is demanded by certificate users/consumers and constitutes a requirement for both
 333 evaluators and developers, even if this means that the developer cannot anticipate all and each
 334 of the tests that will be considered/ performed by the evaluator. This approach also favours
 335 penetration testing, due to the use of AVA_VAN components. Penetration testing implies the use
 336 of a flaw hypothesis methodology: the evaluator identifies potential flaws based on what is
 337 observed during conformity testing and documentation analysis, academic research, and more
 338 largely, any source “deemed appropriate”. Eventually, the evaluator defines a test plan to
 339 ascertain the presence/exploitability of these potential flaws.

340 **6.1.1 The “specification-based” approach**

341 This approach corresponds to the initiative taken within the CCRA and resulting in international
 342 Technical Communities (iTCs) and collaborative Protection Profiles (cPPs).

343 The “specification-based” approach implies the specification of detailed product-type-specific SFRs, as
 344 well as Evaluation Activities derived from ISO/IEC 15408-3. The details added to SFRs and SARs are
 345 meaningful in particular contexts, for a particular TOE type, or in a given industry sector.

346 This approach is intended to define minutely, at the PP level, the requirements to be met and the
 347 corresponding evaluation activities. This approach relies on a requirement-setting body to define the
 348 detailed Evaluation Activities and clear pass/fail criteria ahead of actual evaluations, which allows to
 349 achieve a high degree of consistency in the application of the assurance requirements.

350 **6.1.1.1 Conformance**

351 The “specification-based” approach uses exact conformance Protection Profiles, which ensures that the
 352 conformant ST does not change or even add anything to the Protection Profile requirements. This
 353 concept is intended to support procurement processes, since it ensures that products will not claim
 354 additional features that are not relevant to the interests of the PP owner. The approach also aims at
 355 making it easier for potential customers to compare products and ensuring that the assurance
 356 consumers can see the details of the Evaluation Activities that have been successfully carried out. The
 357 approach ultimately aims at helping consumers to relate more easily the meaning of the certification to
 358 the requirements of their deployment environment.

359 It should be noted that “optional features” in exact conformance PPs are addressed by optional security
 360 functional requirements (SFRs).

361 A given type of TOE may provide a selection-based alternative for some of its SFRs. However, such
 362 selections may require the inclusion of different dependencies. For example, keys used in an IPsec
 363 tunnel may either be distributed or created by the equipment itself, after a negotiation. In the first case,
 364 a single cryptographic SFR is needed. In the second case, a PP editor might want to define requirements
 365 on the whole negotiation protocol. In both cases, the ST writer using the PP must be able to select only
 366 one of those two sets of SFRs. In this case, these sets may be described as optional requirements.

367 **6.1.1.2 Evaluation methodology**

368 The “specification-based” approach does not use EALs. Instead of relying on an assurance scale, the PP
 369 editor derives tailored evaluation activities. Used in common with exact conformance, this allows the PP
 370 editor to keep control of evaluators’ activities at the level of each test or verification for each
 371 requirement. These evaluation activities are derived from ISO 18045 activities and must be defined
 372 using the new ISO/IEC 15408-4. This approach claims the following properties:

373 — Reproducibility, repeatability, and availability of tests are ensured by the fact that they are
 374 completely defined in the PP or its supporting documents, the specification of which requires a
 375 substantial involvement of domain experts;

- 376 — A given product type can be evaluated following this approach *only if* a PP is already defined;
- 377 — Evolutions in the state-of-the-art can be taken into account by updating the PP or the supporting
- 378 documents describing the requirements and the evaluation methodology.

379 6.1.1.3 Edition of Protection Profiles and Security Targets

380 The “specification-based” approach may use standard or Direct Rationale Protection Profiles and

381 Security Targets. Direct Rationale PPs and STs do not use security objectives for the TOE; they include

382 instead a direct mapping from threats to SFRs underpinned by a rationale on the mapping

383 appropriateness.

384 Direct Rationale PPs and STs were previously called “low assurance” PPs and STs because they were

385 only allowed for EAL1 evaluations. These simplified PPs and STs are appropriate for the “specification-

386 based” approach, which does not use EALs.

387 The general philosophy of PPs in the “specification-based” approach implies:

- 388 • Less emphasis on the analysis of the security problem, which has a limited impact on the evalua-
- 389 tions since there is no need to perform TOE-specific vulnerability analysis;
- 390 • Maximizing the use of selection-based SFRs, and minimizing the use of open-ended assign-
- 391 ments;
- 392 EXAMPLE Identification of required versions of protocols and cryptographic algorithms in SFRs.
- 393 • Making extensive use of extended SFRs to specify the expected characteristics of the TOE;
- 394 • Making extensive use of application notes to describe the intended technology-specific adapta-
- 395 tion of SFRs;

396 Defining Evaluation Activities using ISO/IEC 15408-4, i.e. derived from the SARs in ISO/IEC 15408-3

397 and the evaluator actions in ISO/IEC 18045 to specifically address the details of the known TOE context

398 and the individual SFRs.

399 6.1.2 The “attack-based” approach

400 As in previous versions, the standard supports the evaluation methodology defined in ISO/IEC 18405.

401 This approach is based on evaluations carried out in situations where the implemented security

402 functionality may vary, e.g. according to technology choices or IP constraints, provided they enforce the

403 protection of the assets as expected. Such evaluations may be carried out without reference to a

404 Protection Profile or may be based on Protection Profiles that do not define the details of their intended

405 TOE type or deployment context. This maximizes the number of different realizations of the

406 requirements that may be accepted as conformant. The pre-defined packages of security assurance

407 requirements and generic evaluator actions, given in ISO/IEC 18045, are interpreted for each TOE type

408 and specialized to the characteristics of each actual TOE to confirm the assurance level. This assurance

409 is derived from a sound/well-defined hierarchy of assurance requirements and evaluation work units by

410 using TOE-related evidence, which allows the evaluator to specialize the generic evaluation work units

411 and thereby to define the most suitable set of tests for this specific product.

412 This approach is commonly deployed where there is an advantage in having flexibility in the application

413 of the assurance requirements.

414 6.1.2.1 Conformance

415 The “attack-based” approach uses demonstrable or strict conformance, which results in the possibility

416 to add SFRs and SARs to an individual ST (such additions may be organized in a package). However, the

417 approach does not forbid the use of the exact conformance concept whenever appropriate.

418 6.1.2.2 Evaluation methodology

419 The “attack-based” approach uses the EALs, which are characterized by increasing amounts of
 420 developer and evaluator activity aimed at describing internal details of the TOE and interpreting generic
 421 assurance requirements within the context of a particular TOE type and product. This notably includes
 422 AVA_VAN components. This approach claims the following properties:

- 423 • Reproducibility, repeatability, and availability of tests are ensured partly by ISO/IEC 18405
 424 (which provides common notions such as the attack potential), and by the evaluation schemes
 425 that use the standard (which are in charge of ensuring that evaluators have similar approaches,
 426 and that developers are appropriately informed); for mature technologies, dedicated evaluation
 427 methods can also be defined;
- 428 • All product types can be evaluated, as long as the evaluator is deemed competent for the assur-
 429 ance level and/or type of technology considered. As a consequence, the state-of-the-art of at-
 430 tacks has to be taken into account by the evaluator, for the AVA_VAN used, regardless of the
 431 functional features described in the underlying PP(s);
- 432 • Tests are not defined in advance, so that evaluators are allowed to introduce independent and
 433 reasoned analysis in the process, which leads to:
 - 434 – fine-tuning tests depending on the TOE itself (for example, language-specific tests: Python
 435 and C do not lead to the same type of vulnerabilities);
 - 436 – fine-tuning tests depending on evaluation findings: the evaluator is typically simulating an
 437 attacker in a limited timeframe; in this context, based on their knowledge of the TOE,
 438 evaluators define a suitable set of tests;
 - 439 – fine-tuning tests depending on the evolution of the state-of-the-art (for example, if new
 440 attacks have been discovered in the field or in the academic literature).

441 6.1.2.3 Edition of Protection Profiles and Security Targets

442 The “attack-based” approach uses standard or Direct Rationale Protection Profiles and Security Targets.
 443 In particular, this aims at allowing the use of PPs that are specified independent of detailed assumptions
 444 about the TOE context (or use of STs without conformance to PPs, such as for TOEs that are developer-
 445 specific or that need to allow for new solution types in areas of disruptive technologies or technology
 446 evolution). This:

- 447 • Allows customization and adaptation of SPDs, objectives, and SFRs at the ST stage; this differen-
 448 tiation may be of benefit to innovation by allowing vendors to complete their own require-
 449 ments, as opposed to unified Protection Profiles;
 - 450 EXAMPLE Open-ended assignments in PPs’ SFRs allow to make the most suitable instantiations
 451 within the STs.
- 452 • Implies a limited use of extended SFRs, but does not prevent it;
- 453 • Favors approaches where evaluators define test plans based on ISO/IEC 18045 activities; when-
 454 ever a technical domain is mature enough, ISO/IEC 15408-4 or standard refinement and ex-
 455 tended components techniques can also be used to derive dedicated evaluation methods.

456 6.2 Modularity

457 This category introduces the various mechanisms providing modularity options to stakeholders and
 458 explains the benefits and limits of each existing mechanism in the standard. In particular, it explains and
 459 introduces the following aspects:

- 460 a) Modularity of the evaluation process: Splitting a product between **different TOEs**, resulting in
 461 several Security Targets, and evaluating the complete product via a composition mechanism.
 462 This includes typically two main mechanisms:

- 463 • Composition of evaluated products using the ACO assurance class;
- 464 • Composite product evaluation using _COMP assurance components;
- 465 b) Modularity of requirements within a **single TOE**, the following mechanisms may help taking
- 466 into account the notion of modularity:
- 467 • Functional and assurance packages (notably EALs);
- 468 • Modular Protection Profiles, which provide additional means to define optional features
- 469 and extended TOEs through PP-Modules and standard PPs combined in PP-Configura-
- 470 tions;
- 471 • Multi-assurance evaluation paradigm, which allows addressing heterogeneous products
- 472 or systems;
- 473 • Requirement bundling¹, i.e. the structuring of functional and assurance requirements in
- 474 dedicated subsections dependent on their purpose.

475 This revision of the standard introduces new mechanisms for modularity.

476 **EXAMPLES:**

477 - Architectural Patterns for the definition of security domains;

478 - More generally, how the standards can be used when evaluating complex products, as opposed to hierarchical

479 composition situations, e.g. smartcards.

480 This transition guide should, whenever possible, clarify how these mechanisms can be used, in actual products,

481 and whether they can be used in complex mass-market products such as cars, mobile systems, cloud-based sys-

482 tems, etc.

483 Expert contributions are welcome to provide descriptions of real world examples.

484 **6.2.1 Composition mechanisms**

485 The first step that can be used to manage complexity is to break down a product into different parts that

486 can be evaluated separately. This is typically performed by composition mechanisms.

487 The standard suggests several possible ways to break down a product into several parts, namely:

- 488 — Layered,
- 489 — Network, or bi-directional,
- 490 — Embedded,
- 491 — Top-to-bottom.

492 They are described in detail in Clause 13 of ISO/IEC 15408-1. The next sections provide some guidance

493 on how and when to use each one of these models.

494 At the moment, composition is practically supported only for the layered model, which is the most used.

495 **6.2.1.1 Layered**

496 In the layered model the product is composed of a base component and a dependent component. The

497 base component is independent of the dependent component. On the contrary, the dependent compo-

498 nent relies on the base component.

499 **6.2.1.2 Network, or bi-directional**

500 The network model is more relevant to integrators that build systems upon several evaluated products,

501 which rely on each other in a bi-directional way.

1 Besides the constructs included in ISO/IEC 15408-1, ST/PP authors may bundle requirements in dedi-
cated subsections in order to improve readability of a PP or ST.

502 6.2.1.3 Embedded

503 In this type of composition, a component is used as part of a larger component or product. The typical
504 example would consist of an application (major component) including a cryptographic library (embed-
505 ded, or minor, component).

506 This model is of interest for developers building common subsystems, or libraries, intended to be used
507 in several of their products in the future. It may also be relevant for providers of building blocks to
508 other developers.

509 6.2.1.4 Top-to-bottom

510 The top-to-bottom approach is an extension of both the *embedded* and the *layered* model. It basically
511 describes a layered supply chain in which the final evaluation is performed by the base layer actor. For
512 example, a developer evaluates a full mobile OS, so that it can be used on different hardware platforms
513 and lets the hardware vendors perform the final evaluation.

514 6.2.2 Evaluation mechanisms for composition

515 This version of the standard supports two approaches to perform composition according to the *layered*
516 model:

- 517 — The evaluation methodology defined in ISO/IEC 18405 for the ACO assurance class;
- 518 — The composite evaluation methodology defined in [16] and introduced in ISO/IEC 18405 for
519 the `_COMP` assurance components.

520 No mechanism is promoted for other composition models in the standard, but such mechanisms may be
521 provided by communities such as evaluation schemes or MRAs.

522 ACO allows to evaluate a product composed of two evaluated products by reusing the results of the two
523 evaluation and by evaluating the interaction between them.

524 COMP allows to evaluate a composite product made of an evaluated base component and a dependent
525 component by reusing the evaluation of the base component(s). The composite approach is suitable in
526 the context of a complete product evaluation when the product's components are developed by multi-
527 ple, different entities.

528 The composite product evaluation is typically used in the secure element domain, where a product can
529 consist of several layers and the evaluation can be incremental:

- 530 — An Integrated Circuit (IC) and its dedicated embedded software, which is evaluated first;
- 531 — An execution environment, or platform, running on top of the IC and allowing the use of high-
532 level programming languages for the applicative layer, which is evaluated using `_COMP` ;
- 533 — Some applications running on the platform, which is evaluated using `_COMP`.

534 6.2.3 Modularity within a TOE

535 Packages and modular PPs are described in ISO/IEC 15408-1 . This section provides some context on
536 their differences and respective benefits.

537 6.2.4 Packages

538 Packages are sets of security components or requirements. They are intended for communities. For this
539 reason, packages have specific characteristics:

- 540 • They are intended to be reusable (this is why they are named);
- 541 • They are typically written or validated by a community. For example, the EAL packages are
542 adopted in the standard itself;
- 543 • As a consequence, they are not only intended to improve understanding, but are meant to in-
544 clude requirements that are “useful and effective in combination” (as explained in ISO/IEC
545 15408-1).

546 A package applies to the TOE type/TOE defined in the PP/ST where it is defined or used.

547 Packages may be either:

- 548 • Assurance packages, containing only assurance components or requirements, or
- 549 • Functional packages, containing only functional components or requirements.

550 Both types of packages adhere to a structure that includes:

- 551 • The package identification, comprising the package's name, its version information, its latest
552 update date, the sponsor, and a reference to the used edition of the ISO/IEC 15408 series;
- 553 • The package type, i.e. assurance or functional package;
- 554 • A package overview describing the intent of the package;
- 555 • Optional application notes containing information of particular interest to the package users;
- 556 • The package's components (either SARs or SFRs), as well as a rationale for their selection.

557 Additionally, a functional package may include a Security Problem Definition (SPD) and Security
558 Objectives (for the TOE and the operational environment) derived from that SPD. Furthermore,
559 functional packages may optionally declare a set of SFRs that are required in order for the package to be
560 used or included by another requirements specification. If declared, this set of SFRs may be seen as a
561 mandatory dependency at the package level.

562 It is not mandatory for packages to include all dependent components. However, all dependencies must
563 be met in a Protection Profile or a Security Target using the package. Otherwise, for any dependency
564 that is not met, a rationale must be provided.

565 Functional packages may also include optional evaluation methods and activities. These may be
566 included in the package associated with the relevant security requirements. Alternatively, the evaluation
567 methods and activities may be provided in a separate document.

568 EXAMPLE 1

- 569 • Alternative packages driven by a selection that is operated in an SFR.

570 EXAMPLE 2

- 571 • Using packages as a consistent set of assurance requirements: EALs are an example of
572 assurance packages, which are widely used;
- 573 • Using packages as a consistent set of functional requirements: A given community may want to
574 define a functional package to cover specific security objectives, such as secure channels using a
575 given proprietary protocol, for example. This protocol can be broken down into several SFRs,
576 e.g. authentication, information flow control policy, and corresponding cryptographic
577 capacities. Such a package could then be reused within the community by "copying and pasting"
578 it in different STs or PPs, without having to re-analyze which SFRs are needed;
- 579 • Inclusion of an SPD in a package: depending on the richness of the functionalities offered by the
580 package, the editor might consider including a specific SPD in the package itself. In the previous
581 example, a PP for an IPSec tunnel will include a "key distribution" package and a "negotiation
582 and key generation" package. Each package comes with its specific threats, that are not relevant
583 to the other:
 - 584 ○ In the "key distribution" package, assumptions will be needed to cover interception
585 threats during the distribution,
 - 586 ○ In the "negotiation and key generation" package, threats of key leakage or deduction
587 have to be considered.

588 New assurance packages have been introduced in ISO/IEC 15408-5:

- 589 • COMP is meant to facilitate the evaluation of composite products;
- 590 • PPA (Protection Profile Assurance) provides assurance packages for Direct Rationale PPs and
591 standard PPs evaluation;
- 592 • STA (Security Target Assurance) provides assurance packages for ST evaluation.

593 6.2.5 Modular Protection Profiles

594 When compared to functional packages, modular Protection Profiles provide an additional level of
595 control for PP editors:

- 596 • Packages may be used to expose possible functional variations of a TOE type/TOE but do not
597 modify the TOE type/TOE defined in the PP/ST.
- 598 • PP-Modules are mostly intended to describe TOEs built out of modules, including modules that
599 are sourced from different developers and/or are evaluated separately. PP-Modules rely on one
600 or more base PPs and may introduce changes to their TOE types. PP-Modules may use other PP-
601 Modules as a base.
- 602 • PP-Modules may identify a set of selection-based SFRs provided that such SFRs do not introduce
603 changes to the TOE and the TOE boundaries. Otherwise, it may be more suitable to define sev-
604 eral PP-Modules.
- 605 • Moreover, a PP-Module claiming demonstrable or strict conformance may carry a specific set of
606 assurance components for the module (see multi-assurance evaluation in clause 6.2.6).

607 Modular PPs, by definition, deal with the fact that different configurations can arise when integrating
608 modules in a TOE. The evaluation of PP-Modules is enforced through the evaluation of the
609 configurations they belong to, thus ensuring their consistency. The ACE assurance class, which
610 complements APE, covers the evaluation of PP-Configurations and their PP-Modules. The evaluation of
611 PPs, PP-Modules and PP-Configurations can be reused as usual.

612 PP-Modules can be used for representing:

- 613 • alternative architecture choices (for example, a smart meter exposing wired and/or wireless
614 interfaces for the same functionality);
- 615 • optional features or modules (for example, a payment terminal providing a magnetic stripe
616 reader and/or a smartcard reader and/or contactless payment via a smartphone...).

617 **EXAMPLE** An editor may want to define a PP for an application that is found in different ecosystems, for exam-
618 ple, smartcards and mobile devices. Modular PPs allow addressing the specific threats of each underlying plat-
619 form. Mandatory PP-Modules may typically be used with alternative sets of base PPs, each corresponding to a
620 given platform.

621 6.2.6 Multi-assurance Evaluations

622 In addition to PP-Modules and PP-Configurations, the standard defines a flexible framework for the
623 multi-assurance evaluation of IT products using predefined EALs from ISO/IEC 15408-5 or assurance
624 components from ISO/IEC 15408-3, which allows claiming a global set of assurance requirements/as-
625 surance package for the entire TOE, and possibly multiple different sets of assurance requirements/as-
626 surance packages for different parts of the TOE.

627 The previous section already outlined the benefits of modular PPs. In addition, multi-assurance evalua-
628 tion allows addressing heterogeneous products and evaluating modular TOEs that require different as-
629 surance for different parts of their functionality. The main benefit hereby is that the complete TOE is
630 assessed within one evaluation. Hence, the soundness of the security claims can be ensured.

631 The following sections illustrate three practical examples for multi-assurance evaluations.

632 Annex B contains the entire contribution on multi-assurance evaluation, which includes the definition
 633 of the concept (for 15408-1), the extension of ACE assurance class (for 15408-3) and the interpretation
 634 of the standard assurance classes in the context of a multi-evaluation.

635 **6.2.6.1 Example 1: High-assurance selected functions**

636 This example consists of a TOE where some parts of the security functionality require higher assurance
 637 than the rest of the security functionality within the TOE.

638 We assume the existence of a bigger TOE that is evaluated at a lower assurance level overall, with one
 639 or more sub-TOEs that require a higher assurance level.

640 With the multi-assurance approach, a PP/ST author identifies the bigger TOE and the sub-TOEs includ-
 641 ing their boundaries and assigns a combination of both SFRs and SARs to each (sub-)TOE. In this man-
 642 ner the PP/ST identifies clearly what functionality is implemented, where it is implemented, and which
 643 is the assurance expected for each functionality (each TOE part).

644 **EXAMPLE**

645 For example, a modern smartphone with a secure hardware-backed key store could be such a TOE. The
 646 risk owner has determined that the assurance for the whole smartphone needs to be at EAL2 level as
 647 there is sufficient mitigation (ownership of the phone by the user, good monitoring of attacks, quick re-
 648 sponse times, effective patching) to allow authorization of transactions to be performed by the phone.
 649 However, the risk owner has also determined that the hardware-backed key store needs a higher assur-
 650 ance (e.g. EAL4 with AVA_VAN.5) so that long term keys are not compromised.

651 The bigger TOE might then have SFRs encoding user authentication and authorization of a transaction
 652 verified at EAL2 level, and a sub-TOE with SFRs for the key store at EAL4+ level. The sub-TOE's SFRs
 653 would encode the access control to the long-term keys as not allowing anyone to export them out of the
 654 sub-TOE and requiring authorization from the user via the bigger TOE to perform the cryptographic sig-
 655 nature operation. This example is illustrated in Figure 2 hereafter.

656

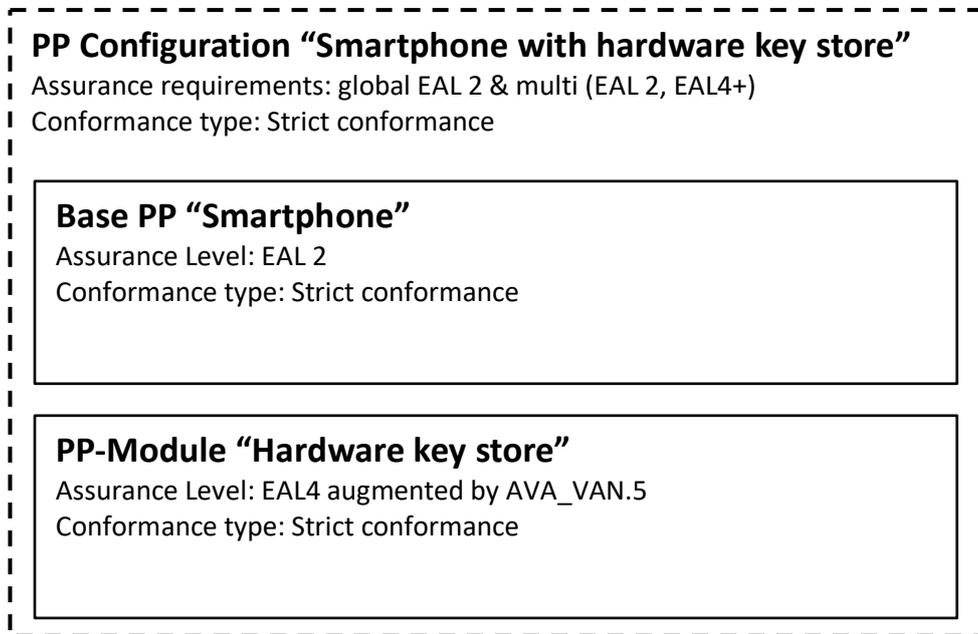


Figure 2 Smartphone with hardware key store

657 **6.2.6.2 Example 2: Low assurance selected functions**

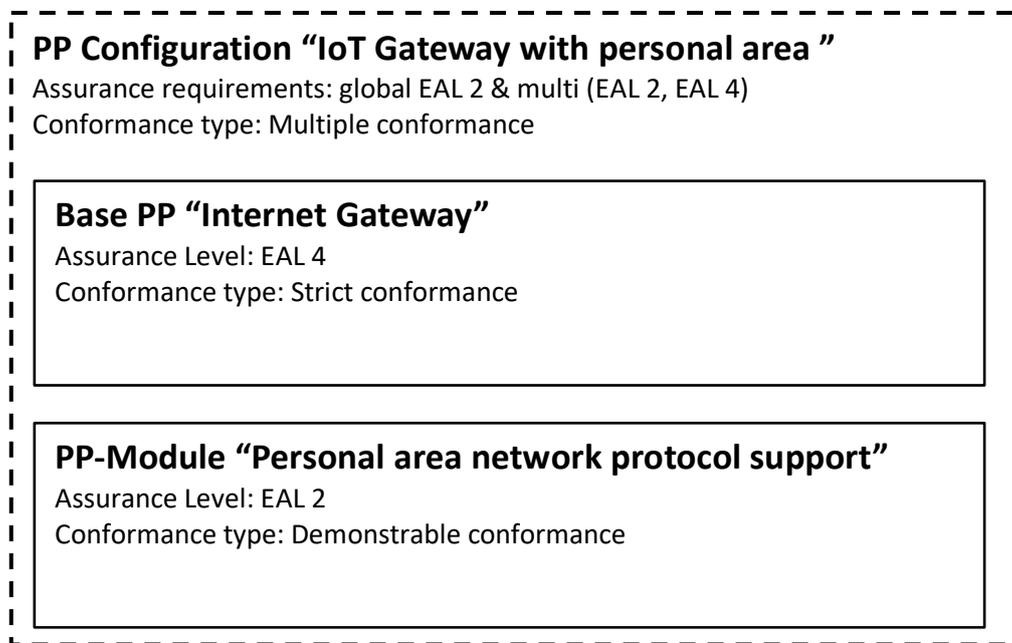
658 **EXAMPLE**

659 This example consists of a TOE where some parts of the security functionality do not require the same
660 high evaluation assurance as other more exposed parts of the TOE.

661 We assume the existence of a TOE that is evaluated on a higher assurance level for most parts, with one
662 or more sub-TOEs that allow a lower assurance level.

663 With the multi-assurance approach, a PP/ST author identifies the bigger TOE and the sub-TOEs includ-
664 ing their boundaries and assigns a combination of both SFRs and SARs to each (sub-)TOE. In this man-
665 ner, the PP/ST clearly shows what functionality is implemented, where it is implemented, and at which
666 is the assurance expected for each functionality.

667 For example, an IoT gateway device could be such a TOE. The risk owner has determined that the assur-
668 ance on the cloud connection services of the IoT gateway device needs to be at EAL4 level as the device
669 is exposed to the internet. However, on the local area and personal area network the risk owner deter-
670 mined that assurance at EAL2 level is sufficient for checking the implementation of IoT protocols and
671 potential lightweight cryptographic cipher suites. This example is illustrated in Figure 3 hereafter.



685 **Figure 3 — IoT gateway with personal area**

686

687 The IoT gateway device might have SFRs encoding the secure channel and transport layer security to-
688 wards an internet cloud connection at EAL4 level, and the sub-TOE with SFRs for authentication and a
689 secure channel towards the personal area network at EAL2 level.

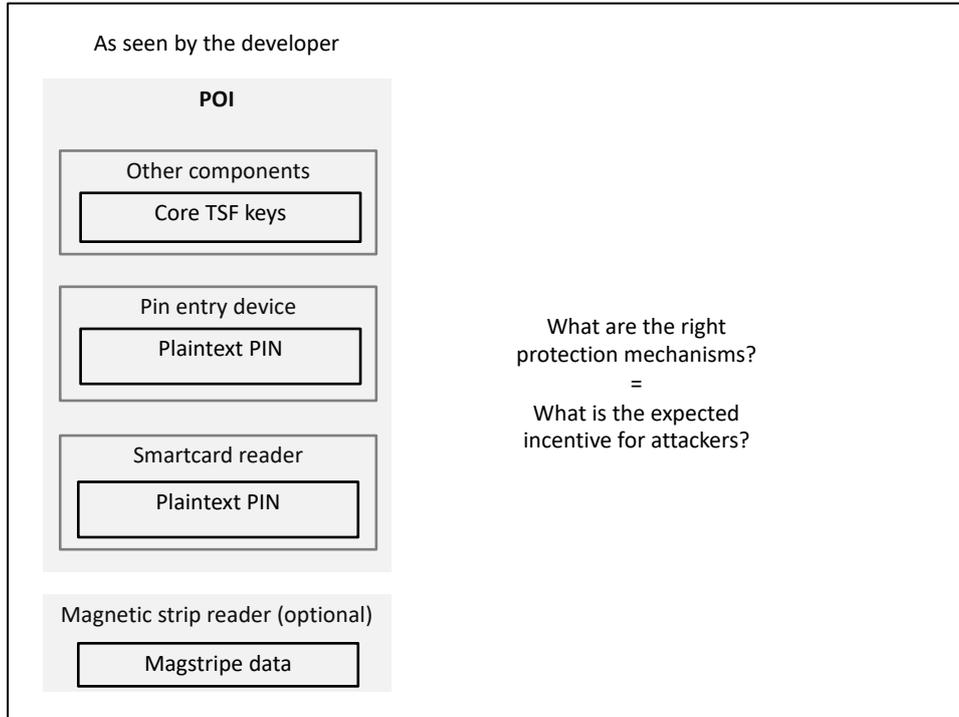
690 Another important notion to consider is that the risk owner will only need EAL2 sub-TOEs on the per-
691 sonal area network because there is an EAL4 gateway acting as a protection against outside threats. So,
692 the rationale is expected to show that:

- 693
- 694 • outside threats are not applicable to the sub-TOEs present on the personal area network (the
695 consistency rationale shall demonstrate that the statements of the security objectives of the PP-
696 Module and its base PPs and PP-Modules are consistent), because
 - 697 • the outside threats are exclusively handled by the gateway (typically via an information flow
698 control SFR, which ensures that connections to these sub-TOEs are not possible from outside
the personal area network).

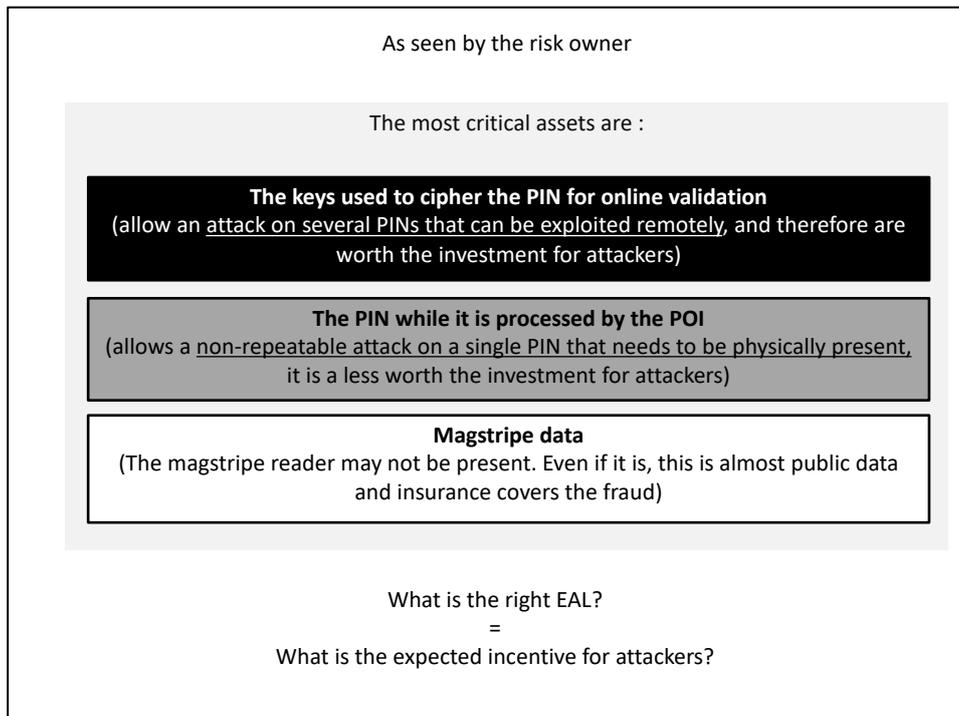
699 **6.2.6.3 Example 3: Point of Interaction use case**

700 The Point of Interaction (POI) is a paradigmatic example of a product composed of parts that respond to
 701 different security problems and assurance needs². The POI PP defines several multi-assurance PP-Con-
 702 figurations, which could be expressed using the Modular PP concepts.

703 The following diagrams illustrate the motivation behind some of the POI PP-Configurations. The con-
 704 cepts have been simplified to allow non-POI specialist understand the concepts behind this organiza-
 705 tion of the TSF in parts, each of them associated with a specific AVA_VAN component.

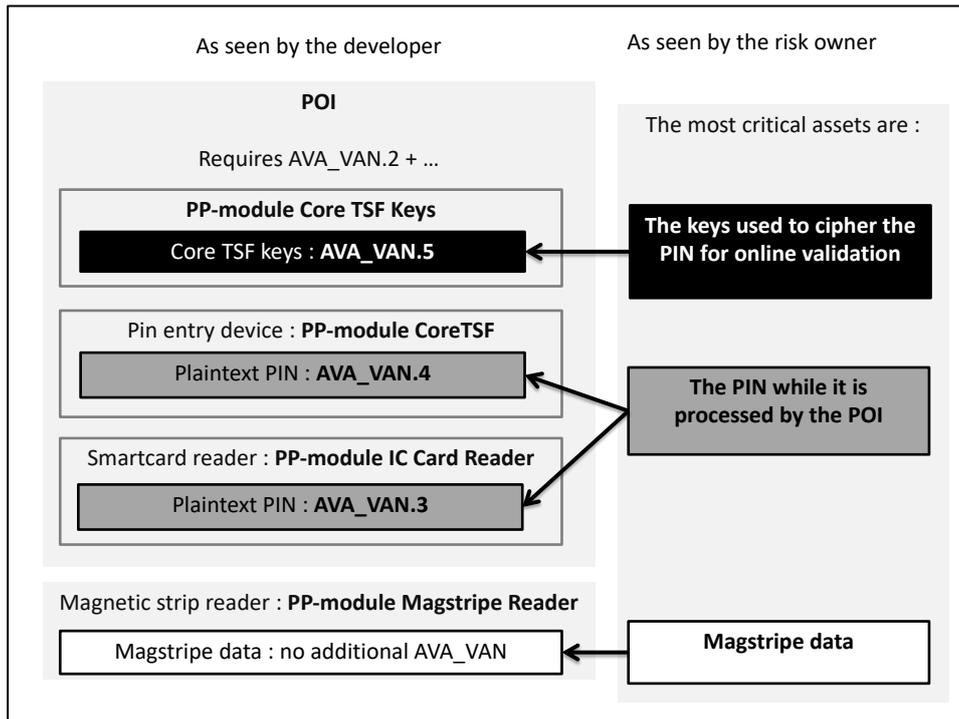


706



707

² The POI PP has led to the definition of the Modular PP concept (PP-Modules and PP-Configurations) integrated in CC v3.1 R5 and is the source for the definition of the multi-assurance evaluation approach.



708

		Assurance requirements : AVA_VAN.2 + AVA_VAN.x where x follows the sensitivity of assets				
		AVA_VAN.5	AVA_VAN.4	AVA_VAN.3	no additional AVA_VAN	
		Core TSF keys	Core TSF (PED)	IC Card Reader	Magstripe Reader	...
Base PP at EAL2 + different PP-Modules for different multi-assurance PP-Configurations	POI-CHIP-ONLY	yes	yes	yes	not present	...
	POI-COMPREHENSIVE	yes	yes	yes	yes	...

709

710 **6.3 Consistent Standard's Language**

711 As highlighted by the Study Period, different communities use the ISO/IEC 15408 and ISO/IEC 18045
712 standards, with varying needs and contexts. Two of these are introduced for consideration in section
713 5.1.

714 In order to improve the standard language for all communities,

- 715 - Terms and definitions have been updated;
- 716 - SFRs that are used *de facto* in Protection Profiles have been introduced in the standard, while
717 other SFRs are currently being refactored to better reflect the state-of-the-art (see Table 3);

718 The notion of SFR-supporting subsystems and modules is now considered optional. In practice, many developers
 719 have legacy ADV_TDS documentation that is still relevant, and there is no reason to force them to refactor the
 720 whole documentation to remove the SFR supporting elements. For this reason, the *SFR-supporting* notion has
 721 been kept in the standard, so that existing ADV_TDS documentation is still compliant to the standard. However,
 722 developers are advised to use only the *SFR-enforcing* and *SFR non-interfering* notions from now on (see ISO/IEC
 723 15408-3 for more details).

724 Some update proposals concerning SARs have been discussed and finally not integrated into the revision. Never-
 725 theless, expert contributions are welcome to improve the standard language or make it more consistent.

726 In its final state, this document needs to help users of the standard to understand:

- 727 a) how they can adapt the standard to their needs by defining supporting documents;
- 728 b) how they can adapt the standard to their needs by refinements or application notes;
- 729 c) how they can adapt the standard to their needs by defining extended requirements in an ST or
 730 PP;
- 731 d) which adaptations of the standard could not be made by these means, and were made by modi-
 732 fying the standard.

733 6.4 Differentiation of ISO/IEC 15408: Evaluation Methods

734 6.4.1.1 Introduction

735 As highlighted by the Study Period, there is a concern about how the standard can address more tech-
 736 nology areas.

737 The main change introduced to take this issue into account is the notion of evaluation methods in
 738 ISO/IEC 15408-4. It is often reminded that ISO/IEC 15408 is technology-agnostic, and evaluations fol-
 739 lowing ISO/IEC 15408 require some degree of technology-specific adaptations, in order to match the
 740 specifics of the evaluated TOE technology. This new version of ISO/IEC 15408 standardizes how to de-
 741 rive evaluation methods from ISO/IEC 18045.

742 Evaluation methods using ISO/IEC 15408-4 are meant to be used in communities where stakeholders
 743 are able to formally validate them.

744 6.4.1.2 Evaluation methods for exact conformance

745 The notion of exact conformance aims at completely defining requirements and tests before an evalua-
 746 tion begins. These requirements and tests are approved within a community (this community may be a
 747 set of suppliers for a given customer, a national certification scheme, an MRA ...) and are typically sup-
 748 plied in the form factor of a PP and some supporting documents. Note that a PP can directly contain
 749 evaluation methods and activities associated to its SFRs. Examples of this can be found in currently used
 750 collaborative Protection Profiles and their corresponding supporting documents (see documents [8] to
 751 [15]).

752 In this context, ISO/IEC 15408-4 is to be used to define the exact set of tests derived from ISO/IEC
 753 18045 work units. The objective of such a derivation process is:

- 754 • To adapt ISO/IEC 18045 to a given technology, but also
- 755 • Whenever possible, to ensure that the evaluator's verdict is completely free of any interpreta-
 756 tion.

757 For this reason, evaluation methods are meant to be based on detailed, and easily reproducible, test
 758 steps. The results of these steps are expected to be clear, so that no ambiguity is left to be managed at
 759 the evaluator's level.

760 6.4.1.3 Evaluation methods outside exact conformance contexts

761 Currently, evaluation methods defined using SAR and 18045 refinements are performed through sup-
 762 porting documents. In particular, efforts have been made in some technical communities such as the
 763 smartcard community to refine the ISO/IEC 15408 and ISO/IEC 18045.

764 EXAMPLE

765 Examples of such refinements are the JIL supporting documents [1], [2], [6], and [7].

766 Similar efforts have been made for the evaluation of payment terminals and Hardware Devices with Security Boxes (see documents [3] to [5]).

768 This new version of the standard does not render these documents obsolete or non-compliant to
769 ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 15408-4 is another way of specifying TOE-specific evaluation
770 methods.

771 **7 Mapping of evolutions with ISO/IEC 15408 and ISO/IEC 18045**

772 **7.1 Summary**

773 ISO/IEC 15408 has been modified to include two additional parts, ISO/IEC 15408-4 and ISO/IEC 15408-
774 5.

775 ISO/IEC 15408-1 has been modified to incorporate the latest changes from the CCDB version CC 3.1 R5
776 and the trial addendum on exact conformance.

777 In addition, ISO/IEC 15408-1 has been re-structured and it now incorporates explanatory text for
778 Modularity (Composition, Packages, Modular Protection Profiles, Multi-assurance), Consistent
779 Standard's Language, etc.

780 ISO/IEC 15408-2 has been modified to standardize some SFRs that have been defined in the past as
781 extended SFRs in published PPs.

782 ISO/IEC 15408-3 has been modified to include changes related to CC 3.1 R5, to the composite evaluation
783 approach, to the multi-assurance concept and to the evaluation of packages. Text relating to EAL and
784 CAP security assurance packages has been moved to ISO/IEC 15408-5.

785 ISO/IEC 15408-4 is a new part that defines a framework for deriving evaluation methods and activities
786 from the standard evaluation methodology given in ISO/IEC 18045. For example, when a particular
787 technology-type requires a specific evaluation methodology.

788 ISO/IEC 15408-5 is a new part; it contains the text in regard to EALs and CAPs that was previously given
789 in ISO/IEC 15408-3. New packages consisting of SARs for Direct Rationale assessments versus standard
790 PPs/STs have been added.

791 ISO/IEC 18045 has been modified to integrate the composite evaluation requirements _COMP, changes
792 related to multi-assurance evaluations and to package evaluation.

793 **7.2 Detailed evolutions**

794 [The following tables provide an overview of the changes leading to the current CD 2. Tables 2, 3, 4, 5, 6,](#)
795 [and 7 provide an overview of the changes made up to CD 1. Tables 2-2, 3-2, 4-2, 5-2, 6-2, and 7-2](#)
796 [summarize the changes made between the CD 1 and CD 2 documents.](#)

797 Table 1 — Changes to the ISO/IEC 15408 structure

Topic	Edition 3	Edition 4 (CD 2 stage)
Structure of ISO/IEC 15408	Three parts of the standard were defined: a) ISO/IEC 15408-1:2009, <i>Information technology — IT security techniques — Evaluation criteria for IT</i>	Five parts of the standard are defined: a) ISO/IEC 15408-1:20XX, <i>IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general requirements.</i>

	<p><i>security — Part 1: Introduction and general requirements.</i></p> <p>b) ISO/IEC 15408-2:2008, <i>Information technology — IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.</i></p> <p>c) ISO/IEC 15408- 3:2008, <i>Information technology — IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.</i></p>	<p>b) ISO/IEC 15408-2:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.</i></p> <p>c) ISO/IEC 15408- 3:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.</i></p> <p>d) ISO/IEC 15408- 4:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities.</i></p> <p>e) ISO/IEC 15408- 5:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements.</i></p>
New ISO/IEC directives		All parts have been updated to conform with the latest JTC 1 directives.
Location of pre-defined package definitions	EAL and CAP security assurance packages were located in ISO/IEC 15408-3.	EAL and CAP security assurance packages are now located in ISO/IEC 15408-5.

798

799

Table 2 — Proposed Changes in ISO/IEC 15408-1

Topic	Edition 4 (CD 1 stage)
Structure of ISO/IEC 15408-1	This part of ISO/IEC 15408 has been restructured to allow the grouping of related topics appropriately.
Terminology	<p>a) Changes to terminology as a result of the JTC 1 directives.</p> <p>b) Proposals for technical changes in terminology and new terms as a result of other changes in the standards.</p> <p>c) Consolidation of terms given in ISO/IEC 18045 into ISO/IEC 15408-1, since the new ISO/IEC 15408-4 will use these terms.</p> <p>The terms and definitions have been organized in alphabetical order in the first CD. Later drafts will introduce a hierarchy of concepts for the terms and definitions.</p> <p>Definitions have been added for:</p> <ul style="list-style-type: none"> - Assurance Level (AL) - Global Assurance level - Sub-TSF <p>Alternate definitions have been proposed for: EAL, evaluation authority, evaluation scheme, evaluation technical report, external entity user, operation, security requirement, security functional requirement, SAR, trusted IT product, user data.</p>

	New definitions for terms related to compositions have been suggested.
Protection Profiles and Packages	<p>a) New text has been proposed to define the structure of security packages and package families.</p> <p>b) Text discussing functional packages has been added. Functional packages may include an SPD and security objectives derived from the SPD.</p>
CC V 3.1 R5	Changes introduced in CC 3.1 R5 have been included. These are related to PP-Modules and PP-Configurations.
Exact Conformance	Changes proposed in the CC 3.1 R5 Addenda have been included. These are related to Exact Conformance and include the Selection-based SFRs and Optional SFR constructs.
Direct Rationale	Text has been proposed that describes the notion of a Direct Rationale approach. This approach can be used with PPs, PP-Modules, STs and/or functional packages, allowing for a PP-Configuration that adopts a Direct Rationale approach to be specified. This construct allows for an alternative method of the specification of the SFRs. The SPD is still defined, but an approach to specifying the SFRs by mapping directly from the SPD is allowed and the Security Objectives Rationale is omitted. Security objectives for the TOE are not included, although security objectives for the operational environment may be specified.
Low assurance PPs/STs	Low assurance PPs/STs. Specified in the third edition of ISO/IEC 15408 have been removed from this edition of the ISO/IEC 15408 series.
Modularity	<p>Text has been proposed that describes the types of modularity supported by ISO/IEC 15408.</p> <p>“Allowed with” construct added to PPs and PP-Modules, which thus have to declare explicitly with which other PPs/PP-Modules they may be used.</p> <p>STs cannot directly claim conformance to PP-Modules.</p> <p><i>Text that describes the multi-assurance evaluation paradigm has been proposed.</i></p> <p>Text describing PP-Module Conformance claims and statements, as well as text describing PP-Configuration conformance statements has been updated.</p>
PP-Configurations	<p>The concept of PP-Configurations has been added. This allows for the reasoned valid combination of PPs and PP-Modules using either the “specification-based” or “attack-based” approach described above.</p> <p>Combining a PP-Module with a PP introduced the concept of a “Base PP” which is a PP developed with the notion that it will be combined with a PP-Module or PP-Modules.</p>
Composition of assurance	Text has been proposed that describes the topic of the composition of security assurance, and how evaluation results might be re-used.
New Annex E	An informative annex has been proposed that describes various legitimate use-cases for the application of the ISO/IEC 15408 model.

800

801

Table 2-2 — Proposed Changes in ISO/IEC 15408-1

Topic	Edition 4 (CD 2 stage)
-------	------------------------

Structure of ISO/IEC 15408-1	This part of ISO/IEC 15408 has been restructured to allow the grouping of related topics appropriately.
Terminology	<p>a) Changes to terminology as a result of the JTC 1 directives.</p> <p>b) Proposals for technical changes in terminology and new terms as a result of other changes in the standards.</p> <p>c) Consolidation of terms given in ISO/IEC 18045 into ISO/IEC 15408-1, since the new ISO/IEC 15408-4 will use these terms.</p> <p>The terms and definitions have been organized in alphabetical order as was the case in the first CD. Later drafts will introduce a hierarchy of concepts for the terms and definitions.</p> <p>Definitions have been added for:</p> <ul style="list-style-type: none"> - Security functional requirement (SFR) - Security assurance requirement (SAR) - Global set of assurance requirements/assurance package (replaces Global Assurance Level from CD1) - Multi-assurance evaluation <p>Alternate definitions have been proposed for: evaluation authority, trusted IT product.</p> <p>The terminology related to composition has been revised.</p> <p>New definitions for terms related to compositions have been suggested.</p>
Packages	<p>Text discussing the mandatory contents of packages has been added to the sub-clause 8.2 Package types.</p> <p>Text discussing optional requirements has been added.</p> <p>A new sub-clause has been added to discuss the inclusion of optional evaluation methods and activities in packages.</p>
Protection Profiles	Text has been added for allowing Protection Profiles that require exact conformance to specify (and allow for use) optional requirements.
Modularity	<p>STs cannot directly claim conformance to PP-Modules, only to PP-Configurations.</p> <p>Text describing PP-Module Conformance claims and statements, as well as text describing PP-Configuration conformance statements has been updated.</p>
Multi-assurance	<p>Text that describes the multi-assurance evaluation paradigm has been updated.</p> <p>Relation between multi-assurance evaluation and composition has been clarified.</p>
PP-Configurations	Text has been added for allowing PP-Modules that require exact conformance to specify (and allow for use) optional requirements.
Composition of assurance	<p>The clause related to composition has been restructured.</p> <p>Text describing the objective for the composite product evaluation technique has been updated.</p>

	The roles related to composite evaluation have been defined.
New Annex numbering and structure	<p>The annexes were re-numbered in order to mirror the order of the main clauses in the normative part. Annex B from CD 1 which presented information and guidance for PPs as well as PP-Configurations has been split into two different annexes.</p> <p>Currently, the document includes the following informative annexes:</p> <ul style="list-style-type: none"> Annex A) Specification of Packages Annex B) Specification of Protection Profiles Annex C) Specification of PP-Modules and PP-Configurations Annex D) Specification of Security Targets and Direct Rationale STs Annex E) Guidance for Operations Annex F) PP Conformance

802

803

Table 3 — Proposed Changes in ISO/IEC 15408-2

Topic	Edition 4 (CD 1 stage)
Proposed new families	<p>Families used in existing protection profiles have been added to the standard:</p> <ul style="list-style-type: none"> — FCS_RBG (Random bit generation) — FCS_RNG (Generation of random numbers) — FIA_API (Authentication proof of identity) — FMT_LIM (Limited capabilities and availability) — FPR_UNL (Unlinkability) — FPT_EMS (TOE emanation) — FPT_INI (TSF initialization) — FTA_TAB (TOE access banners) — FTP_PRO (Secure channel) <p>Some SFRs are still placeholders and a call for experts' contributions has been included in the document.</p>
Existing families with new components and/or re-leveling	<p>FCS_CKM: Cryptographic key management: refactoring is considered for cryptographic SFRs, but input from CCDB Crypto WG is requested. Placeholders have been added to this effect in the document.</p> <p>FDP_SDC has been modified to better incorporate notions such as full disk encryption</p> <p>FIA_UAU: User authentication</p> <p>FPT_STM: Time stamps</p>
Deleted families (from WD 2)	<p>FIA_PMG: Password management</p> <p>FCO_TCC: Trusted channel proposed for removal in favor of FPT_PRO</p> <p>FPT_ADM: Ad-hoc domain management</p>

804

805 **Table 3-2 — Proposed Changes in ISO/IEC 15408-2**

Topic	Edition 4 (CD 2 stage)
Existing families with modifications (compared to CD 1)	<ul style="list-style-type: none"> - FDP_IRC (Information Retention Control) has been restructured and rewritten to increase precision. - FPR_UNL (Unlinkability): FPR_UNL.2 and FPR_UNL.3 have been deleted - FPT_EMS (TOE Emanation): FPT_EMS.1.1 has been deleted - FPT_INI (TSF initialization): FPT_INI.1 has been rewritten.
Deleted families (from CD 1)	<ul style="list-style-type: none"> - FCO_TCC (Trusted channel) removed in favour of FPT_PRO (Secure channel) - FPR_TRD (Distribution of trust) removed for maintenance and usability reasons

806

807 **Table 4 — Proposed Changes in ISO/IEC 15408-3**

Topic	Edition 4 (CD 1 stage)
General	Text related to assurance packages (i.e. EALs and CAPs) has been moved to ISO/IEC 15408-5.
CC V 3.1 R5	Changes introduced in CC 3.1 R5 have been included. These are related to the ACE class
Clause 8 Class APE: Protection Profile evaluation	Class APE is to be extended to cover the concept of “selection-based SFR”.
Clause 9 Class ASE: Security Target evaluation	Class ASE is to be extended to cover the concept of “selection-based SFR”.
Clause 12 Class ALC: Life- cycle support	Changes have been introduced in ALC_TAT and ALC_CMC, in order to better take into account issues related to semi-automated evidence generation.

808

809 **Table 4-2 — Proposed Changes in ISO/IEC 15408-3**

Topic	Edition 4 (CD 2 stage)
Clause 7 Class APE: Protection Profile evaluation	APE_CCL has been modified to allow a check to acknowledge the possible identification of explicit evaluation methods and activities in the PP’s Conformance Statement.

	APE_REQ has been updated to include considerations of environment objectives alongside SFRs when mapping to OSPs. APE_REQ.2 has been updated so as to not include requirements that are specific to Direct Rationale PPs.
Clause 8 Class ACE: Protection Profile configuration evaluation	An equivalent of ACE_CCO.1.6C as stated in ISO/IEC 18045 CD1 has been included.
Clause 9 Class ASE: Security Target evaluation	ASE_REQ.2 has been updated so as to not include requirements that are specific to Direct Rationale PPs.
Clause 12 Class ALC: Life- cycle support	ALC_PTD (Practices for trustable development) has been renamed to ALC_TDA (TOE Development Artifacts). Descriptions of purpose for ALC_TDA and ALC_COMP have been added.

810

811 **Table 5 – New ISO/IEC 15408-4**

Topic	Edition 4 (CD 1 stage)
General	This is a new part of ISO/IEC 15408. This document describes a framework that shall be used for specifying evaluation methodologies using these more specific evaluation activities that may be included in PPs, STs and any documents supporting them.
Clause 6 Structure of an Evaluation Method	6.1 Overview 6.2 Specification of an Evaluation Method 6.2.1 Overview 6.2.2 Identification of evaluation methods 6.2.3 Scope of the evaluation method 6.2.4 Dependencies 6.2.5 Required input from the developer or other entities 6.2.6 Set of evaluation activities 6.2.7 Required tool types 6.2.8 Required evaluator competences 6.2.9 Rationale for the evaluation method 6.2.10 Additional verb definitions 6.2.11 Requirements for reporting
Clause 7	7.1 Overview

Structure of Evaluation Activities	<p>7.2 Specification of an evaluation activity</p> <p>7.2.1 Unique Identification of the evaluation activity</p> <p>7.2.2 Objective of the evaluation activity</p> <p>7.2.3 Relation of the evaluation activity to SFRs, SARs, and other evaluation activities</p> <p>7.2.4 Rationale for the evaluation activity</p> <p>7.2.5 Tool types required to perform the activity</p> <p>7.2.6 Required evaluator competences</p> <p>7.2.7 Required input from the developer or other entities</p> <p>7.2.8 Assessment strategy</p> <p>7.2.9 Pass/fail criteria</p> <p>7.2.10 Requirements for reporting</p>
------------------------------------	---

812

813 **Table 5-2 - New ISO/IEC 15408-4**

Topic	Edition 4 (CD 2 stage)
Clause 6 Structure of an Evaluation Method	A diagram depicting the content and structure of an evaluation method has been provided.

814

815 **Table 6 — New ISO/IEC 15408-5**

Topic	Edition 4 (CD 1 stage)
Summary	<p>The text in regard to assurance packages (EAL and CAP) from ISO/IEC 15408-3 has been incorporated into ISO/IEC 15408-5.</p> <p>New assurance packages have been proposed to facilitate the evaluation of composition and Direct Rationale PPs and STs.</p> <ul style="list-style-type: none"> — COMP (Composite Product) — PPA (Protection Profile Assurance) — STA (Security Target Assurance)

816

817 **Table 6-2 — New ISO/IEC 15408-5**

Topic	Edition 4 (CD 2 stage)
Summary of changes	The ALC_TDA assurance component has not been included in the EAL tables.

818

819 **Table 7 — Proposed Changes in ISO/IEC 18045**

Topic	Edition 4 (CD 1 stage)
Structure of ISO/IEC 18045	This part of ISO/IEC 15408 has been restructured to allow the grouping of like topics appropriately
Terminology	Consolidation of terms given in ISO/IEC 18045 into ISO/IEC 15408-1, since the new ISO/IEC 15408-4 will use these terms

820

821 **Table 7-2 — Proposed Changes in ISO/IEC 18045**

Topic	Edition 4 (CD 2 stage)
Summary	<p>Work units corresponding to ASE_COMP, ALC_COMP, ADV_COMP, ATE_COMP, and AVA_COMP defined in Appendix 1.1 of <i>JIL Composite product evaluation for Smart Cards and similar devices</i> have been inserted.</p> <p>Work units for the new APE components describing how evaluation methods and activities are to be presented and evaluated have been inserted.</p> <p>Optional requirements have been introduced and optional/mandatory packages have been eliminated.</p>

822

823 **8 Migration from the third to the fourth edition of the ISO/IEC 15408 series**824 **To be completed**

825

NOTE The third edition of the ISO/IEC 15408 series is technically identical to the Common Criteria Version 3.1 revision 4.

826

827 **Annex A**
828 **(informative)**
829 **Study Periods Overview**

830 This annex presents the experts contributions to the Study Period and an overview per categories for
831 which expert contributions have not been provided or accepted by WG3 experts..

832 This Annex merges previous Annexes B and C.

833 **A.1 Vulnerability Assessment**

834 As previously stated, the study period determined that communities with different needs are to use the
835 Common Criteria standard:

- 836 — Currently, ISO/IEC 15408 allows low assurance evaluations (up to EAL2), and also allows add-
837 ing SARs on top of any EAL, which makes CC valuable among communities that have no need
838 for focused vulnerability analysis;
- 839 — At the same time, ISO/IEC 15408 allows grading EALs evaluations up to EAL7, which is of ben-
840 efit to communities that have a need for high assurance, and need a scale based upon increas-
841 ing levels of vulnerability and conformity assessment.

842 As a consequence, the new edition of the standards needs to keep this structure and continue to support
843 a scale of increasingly demanding vulnerability assessments as the backbone of Evaluation Assurance
844 Levels.

845 **Experts opinions on vulnerability assessment**

846 The Study Periods showed that a consensus on definitions in regard to vulnerability assessments is needed. Work-
847 ing draft 1 of ISO/IEC 15408-1 proposed some improvements, but Experts are invited to contribute.

848 This document should also clarify the differences between the assurance given by vulnerability assessment and
849 the assurance given by quality control methods such as compliance testing. In particular, this document should
850 clarify how the standards should be used to provide factual, consistent, and comparable robustness assessment
851 through vulnerability analysis. Here, the document should focus on the methods of analysis, and the notion of at-
852 tack potential, in a way that relates to risk assessment methods used by sponsors and developers. This document
853 may also provide guidance for communities, so that they can define meaningful methods for vulnerability assess-
854 ment on specific products or technologies.

855 This work has begun in section 5.1. Additionally, a new study period on competence requirements for evaluation
856 labs (N1514) may support a part of these needs. Results from the Study Period will have to be integrated in this
857 section.

858 More generally, additional expert contributions are welcome.

859

860 **Experts opinions on CEM completion for EAL5 and higher**

861 Comments emitted during the 2nd Study Period highlighted the need for harmonization of ADV_SPM.1 evaluation.
862 At the moment, ISO/IEC 18045 does not cover all the SARs required for EAL5 and higher: users of Common Crite-
863 ria rely the supporting document *AIS 34* to complete the ISO/IEC 18045 regarding EAL5+ or EAL6 evaluations.

864 Instead of addressing only the initial remark of the study period (harmonizing ADV_SPM.1), editors suggest that
865 ISO/IEC 18045 should be reworked so as to cover as many SARs of ISO/IEC 18045 Part 3 as possible. A first step
866 in this direction would be the inclusion of the *AIS 34* content in the ISO/IEC 18045.

867

868 **Experts opinions on improvements for vulnerability assessment**

869 The Study Period proposed that additional guidelines and examples might further improve the standard. For ex-
870 ample, the standard could address:

871 - static, dynamic, or memory analysis techniques that may be used during vulnerability assessment on top of usual
872 penetration testing techniques and manual source code analysis;

873 - Semi-automated dynamic techniques, such as fuzzing, may also be used.

874 The revised standards may provide examples and guidance for communities willing to define supporting docu-
875 ments, in order to help them integrate such techniques in vulnerability assessment activities. Alternatively, ex-
876 perts could consider a supporting technical report to cover this matter.

877 As a sidenote, a contribution on fuzzing for developers has already been suggested in WD1, but was ultimately
878 rejected because it did not give enough perspective on the complete set of relevant development activities that can
879 be used alongside fuzzing, and did not clarify how this would be taken into account from an evaluation methodol-
880 ogy point of view.

881 A.2 Clarify & Streamline Evidence Requirements

882 New assurance families (ADV_ARK, ADV_TDK, ADV_TRA, ATE_MTK) have been discussed in order to
883 provide an alternative to document-based assurance for development activities. Nevertheless, such
884 families are out of scope of the current update of the standard.

885 Additionally, the standard introduces some changes related to semi-automated evidence generation in
886 ALC classes (see Table 4).

887 **Experts opinions** The study period identified the following issues:

888 — This document may also provide guidelines to clarify how other kinds of evidences may be used during the
889 evaluation. As an example, static, dynamic, or memory analysis techniques may be used on top of documentation
890 evidences. Changes introduced at the moment in ALC_CMC and ALC_TAT are still modest.

891 — Developers would like to reuse test evidences compliant to other standards, for example by using supporting
892 documents.

893 — More generally, explanations on how the new standard will allow the reuse of compliance to other standards.

894 A new study period has been launched (N1513) in order to evaluate potential overlap and re-use from other
895 standards. The results from the Study period may be integrated to allow the reuse of test evidences compliant to
896 other standards.

897 More generally, expert contributions are welcome on this topic.

898 A.3 Consistent Standard Metrics

899 As highlighted by the study period, the standard needs to consider how to allow a better comparison of
900 evaluated products.

901 On the one hand, the transition guide needs to introduce the changes made to introduce more
902 measurability in the standard.

903 On the other hand, the transition guide also needs to clarify when more objectivity would be
904 detrimental to genericity, agility with regard to state-of-the-art evolutions, and independence from the
905 verticals and/or technologies. In this case, the transition guide may provide guidelines or
906 recommendations to the communities in charge of defining evaluation methods. (detailed in the
907 document itself)

908 In both cases, we suggest that the notion of *attack potential* provides a large part of the solution when
909 comparing evaluated products. As a consequence, the cluster on vulnerability assessment should be
910 addressed first.

911 **Experts opinions on metrics**

912 At the moment, changes in the standard do not yet address the issue of measurability.

913 **A.4 Better use of development models and process**

914 **A.4.1 Incremental development**

915 The standard benefits from the new modularity mechanisms and allows an easier management of agile
916 development methods. More generally, changes are intended to allow evaluators to perform evaluation
917 tasks as soon as possible during the development lifecycle.

918 In particular, ASE_AMA, ADV_MTC and ATE_MTT are an example where packages or modules may be
919 used to describe a TOE that will be developed by increments, and where the evaluator is allowed to
920 work on the different, non-final versions of the TOE. Nevertheless, such families are out of scope of the
921 current update of the standard.

922 **A.4.2 Other topics to be discussed**

923 The consensus of the study period seems to be that additional discussions are needed to define a
924 measurable characteristic for the development model. However, there is a clear need from specific
925 communities, and the new standard should, in a way or another, try to address:

- 926 — compatibility with agile development methods, in particular the need for short sprints (a few
927 weeks) and the use of automated test methods;
- 928 — compatibility with patch management and optimization of assurance continuity methods;
- 929 — compatibility with “secure development” best practices, such as automated source code analy-
930 sis.

931 This document may, as a first step, provide context by summarizing existing work (supporting
932 documents) and new contributions on these topics. The French NOTE-06 is an example of how the new
933 standard could integrate these concerns in evaluation activities.

934 These contributions might be used as guidelines or examples for SAR definition (ISO/IEC 15408-3).

935 **Experts opinions**

936 At the moment, among the issues raised during the study period, only the patch management issue has been ad-
937 dressed, and resulted in a study period. Results of the study period will have to be discussed here.

938 Expert contributions are welcome on the other topics of this section.

939 **A.5 Reposition CEM**

940 To be completed

941 Contributions to the project are encouraged

942 **A.6 Review Tools and Techniques**

943 Improvements have been introduced with regard to ALC_TAT (see Table 4).

944 To be completed

945 Contributions to the project are encouraged

946 **A.7 New requirements**

947 New SFRs and new SARs are listed in Tables 3 and 4.

948
949
950

Annex B
(informative)
Multi-assurance evaluation

951 This Annex contains the integral contribution on the multi-assurance evaluation concept as
952 defined in ISO/IEC 15408-1 CD2 and ISO/IEC 15408-3 CD2.

Foreword

953

954 This is a contribution to the Common Criteria and the associated Common Evaluation Meth-
 955 odology for Information Technology Security Evaluation through ISO SC27 WG3 which is
 956 leading the update of the standard.

957 Document History:

958 V0.1, June 2018: Initial version (draft).

959 V0.2, June 2018: Integrates contributor's feedback

960 V0.3, June 2018: Completed proposal of multi-assurance approach for delivery to ISO
 961 SC27 WG3. Updates provided for main body of ISO-EC 15408-1 and ex-
 962 ample class (ACE) for ISO-EC 15408-3. Full updates (such as ISO-EC
 963 15408-1 annexes and ISO-EC 15408-3 ASE and APE Classes) to be pro-
 964 vided following agreement (in principle) of approach by ISO SC27 WG3.

965 V0.4, August 2018: Internal version with annotations

966 V0.5, September 2018: Integrates ISO experts' comments

967 V0.6, September 2018: For discussion with ISO co-editors

968 V0.7, September 2018: Integrates co-editors' feedback

969 V0.8, September 2018: Updated contribution for distribution to SC27 WG3

970 V0.9, December 2018: Updated contribution for delivery to ISO experts

971

972 Table of Contents

973 1 Introduction 32

974 1.1 Executive summary 32

975 1.2 Scope 32

976 1.3 Audience 32

977 1.4 Normative references 32

978 1.5 Terms and definitions 32

979 1.6 Notation 33

980 2 ISO/EC 15408-1 update 34

981 2.1 Multi-assurance evaluation 34

982 2.2 Security Targets 35

983 2.4 Evaluation and evaluation results 42

984 2.5 Annex B – Specification of PPs 43

985 2.6 Annex C – Specification of PP-Modules 43

986 2.7 Annex D – Specification of STs 43

987 3 ISO/EC 15408-3: Class ACE 44

988 1.1 Introduction 44

989 1.2 PP-Module introduction (ACE_INT) 45

990 1.3 PP-Module conformance claims (ACE_CCL) 47

991 1.4 PP-Module Security problem definition (ACE_SPD) 49

992 1.5 PP-Module Security objectives (ACE_OBJ) 50

993 1.6 PP-Module extended components definition (ACE_ECD) 52

994	1.7 PP-Module security requirements (ACE_REQ)	54
995	1.8 PP-Module consistency (ACE_MCO)	58
996	1.9 PP-Configuration consistency (ACE_CCO)	60
997	3.1 Other assurance classes	64

998	1	Introduction	
999	1.1	Executive summary	
1000	1	This document contains the proposal for introducing the multi-assurance evaluation paradigm into Common Criteria (CC), leveraging the concepts of PP-modules and PP-Configurations.	
1001			
1002			
1003	1.2	Scope	
1004	2	This document contains all the normative elements required to define and evaluate multi-assurance modular protection profiles and security targets, and to perform multi-assurance TOE evaluations.	
1005			
1006			
1007	3	These elements supplement CC Part 1, CC Part 3 and CEM and should eventually be integrated to the standard.	
1008			
1009	1.3	Audience	
1010	4	This document is intended for ISO SC27 WG3 experts in the framework of the update of ISO/IEC 15408 and ISO/IEC 18045 currently in progress.	
1011			
1012	1.4	Normative references	
1013	5	The following references apply to this document.	
1014		[CC-1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 1: Introduction and general model. CCMB-2017-04-001.
1015			
1016			
1017		[CC-2]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components. CCMB-2017-04-002.
1018			
1019			
1020		[CC-3]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 3: Security assurance components. CCMB-2017-04-003.
1021			
1022			
1023		[CEM]	Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 5, April 2017. Evaluation methodology. CCMB-2017-04-004.
1024			
1025			
1026		[CC-1-CD2]	ISO/IEC 15408-1 CD2, December 2018
1027		[CC-3-CD2]	ISO/IEC 15408-3 CD2, December 2018
1028	1.5	Terms and definitions	
1029		<i>[[CC-1-CD2] §3.1 „Terms and definitions in alphabetical order“)</i>	
1030	6	global assurance package – assurance package, i.e. set of well-formed assurance requirements drawn from ISO/IEC 15408-3 or defined as a set of extended assurance components, that applies to the entire TOE in a multi-assurance evaluation.	
1031			
1032			

- 1033 7 **multi-assurance evaluation** – evaluation where the TOE is organised in parts, each
1034 part being associated with its own assurance package.
- 1035 8 **sub-TSF** (or TSF part) – notion applied in multi-assurance evaluation to denote a
1036 portion of the TSF that provides a well-defined subset of security functionality,
1037 which corresponds to a set of SFRs that is closed by dependencies, objectives, and
1038 SPD elements.
- 1039 9 Note 1: a sub-TSF has all the characteristics of a TSF.
- 1040 10 Note 2: a sub-TSF is associated with its own set of SARs/assurance package in a
1041 multi-assurance PP-Configuration.
1042
- 1043 **1.6 Notation**
- 1044 11 The first occurrence of new or modified normative elements introduced for the def-
1045 inition of the multi-assurance evaluation approach is written in **bold** police.
1046

1047 **2 ISO/EC 15408-1 update**

1048 12 This section presents the updated of multi-assurance clauses as defined in [CC-3-
1049 CD2].

1050 **2.1 Multi-assurance evaluation**

1051 *([CC-1-CD2] §6.3.1 „General “)*

1052

1053 13 ISO/IEC 15408 series defines a flexible framework for the evaluation of IT Prod-
1054 ucts.

1055 14 As this evaluation may need to meet varying assurance needs, the standard provides
1056 different tools, from predefined assurance levels (ISO/IEC 15408-5) to well-formed
1057 assurance components and packages (ISO/IEC 15408-3) and a companion evalua-
1058 tion methodology (ISO/IEC 18045), as well as a mechanism to define extended
1059 assurance components (ISO/IEC 15408-1).

1060 15 *([CC-1-CD2] §6.3.4 „Multi-assurance evaluation“)*

1061 16 The standard evaluation approach consists in applying a single set of standard as-
1062 surance requirements to the entire TOE. However, the standard also provides a
1063 method (ISO/IEC 15408-4) to specialize the standard assurance components and
1064 evaluation activities and a multi-assurance evaluation framework to apply different
1065 assurance requirements to different parts of the TSF, while enforcing a global set
1066 of SARs/assurance package for the entire TOE.

1067 17 The multi-assurance evaluation paradigm:

- 1068 ○ addresses heterogeneous IT products where different security needs require
1069 different assurance within a single evaluation
- 1070 ○ ensures that the multiple assurance requirements are sound with regard to
1071 the security needs for the product.

1072 18 Technically, a multi-assurance evaluation is driven by a Security Target that com-
1073 plies with one (and only one) multi-assurance PP-Configuration. The multi-assur-
1074 ance PP-Configuration ensures that applying different assurance requirements to
1075 different parts of the TOE is consistent with their security needs. In this evaluation
1076 approach, each sub-TSF enforces some security functionality, e.g. an authentication
1077 protocol, a firewall policy, the boot process, encryption/decryption operations, and
1078 in some cases, the part can be associated with a subset of TOE components, for
1079 instance a TPM, a cryptographic library or a card reader.

1080 19 Examples where the multi-assurance paradigm is relevant are the following:

- 1081 ○ A device where some security functionality requires higher assurance than
1082 the rest, for instance, a key storage and processing unit, a secure boot
1083 module, etc.

- 1084 ○ A device where some parts of the security functionality do not require the
1085 same high evaluation assurance as other more exposed parts of the device,
1086 for instance an internet gateway with support for personal area network
1087 protocols.
- 1088 ○ A family of devices where some security functionality is shared across all
1089 the devices with the same assurance, and some security functionality is
1090 implemented in different ways for different use cases, for instance in a
1091 tamper-resistant module or in a software module or through COTS,
1092 requiring different assurance. The multi-assurance paradigm allows to
1093 combine the shared functionality and the use-case dependent functionality
1094 in as many multi-assurance PP-configurations as needed.
- 1095 ○ Multi-assurance is eventually relevant for products claiming conformance
1096 to different Protection Profiles with different assurance packages: by
1097 defining and evaluating a PP-Configuration, the multi-assurance paradigm
1098 allows better control over possible inconsistencies between these PPs. The
1099 evaluation of electronic passports implementing both Basic Access Control
1100 and Extended Access Control constitutes a typical example, as these access
1101 control mechanisms are subject to different security problems and assurance
1102 requirements.

1103 Editor's Note:

1104 The motivation for the multi-assurance evaluation is driven by the risks over the
1105 assets in the given threat model (see examples above).

1106 The concept does not break or weaken existing CC concepts. It is a true addition to
1107 allow the certification of products that hold assets with different sensitivity (as in
1108 POI PP).

1109 The developer will document each TSF part as usual since TSF parts are closed by
1110 dependencies, objectives and SPD. The vulnerability analysis of each TSF part
1111 complies with the current definition of AVA_VAN which considers the whole TOE
1112 as the attack surface.

1113 **2.2 Security Targets**

1114 *(completes sub-clause [CC-1-CD2]§ 6.3.2.1 „General“)*

1115

- 1116 20 A Security Target may be defined as a standalone document for the specific TOE
1117 or may comply with one or more preexistent Protection Profiles or PP-Configura-
1118 tions and thereby reuse and specialize their generic definitions to meet the specific
1119 TOE. In the second case, the ST shall meet the conformance conditions set forth in
1120 the PPs/PP-Configurations.

1121

1122 *([CC-1-CD2]§ 11.3 “Multi-assurance security targets”)*

1123 21 A multi-assurance Security Target must organise the TSF in parts and claim a specific set of SARs/assurance package for each of the parts and a global set of
 1124 SARs/assurance package for the entire TOE: this is achieved exclusively through
 1125 the conformance to a multi-assurance PP-Configuration which defines the parts and
 1126 the sets of SARs/assurance packages.
 1127

1128 22 A multi-assurance Security Target may extend the PP-Configuration with additional SFRs (and related SPD and security objectives as necessary) so that each new
 1129 element completes at a minimum one standard PP or PP-Module of the PP-Config-
 1130 uration provided the required conformity rules are satisfied. That is, the new SFRs
 1131 are aimed at extending the sub-TSFs defined by the components of the PP-Config-
 1132 uration. As a consequence, the extended sub-TSFs are subject to the set of SARs/as-
 1133 surance packages as defined in the original PPs/PP-Modules.
 1134

1135 23 A multi-assurance Security Target may claim the sets of SARs/assurance packages
 1136 defined in the PP-Configuration, or may provide a rationale to claim “augmented”
 1137 sets of SARs/assurance packages, similar to Security Targets in the general model.

1138 24 Note: In order to conform with two or more PPs that define different sets of
 1139 SARs/assurance packages, a multi-assurance PP-Configuration composed of the
 1140 PPs must be defined and claimed by the Security Target.

1141 **2.3 Protection Profiles, PP-Modules and PP-Configurations**

1142 **2.3.1 Introduction**

1143 *(completes [CC-1-CD2]§10.3.1)*

1144

1145 25 A PP-Configuration is a way to build a PP out of a set of PPs and PP-Modules.

1146 **2.3.2 Protection Profiles**

1147 *(completes [CC-1-CD2]§9.3.2 Assurance requirements)*

1148

1149 26 A standard PP of demonstrable or strict conformance which complies with ISO/IEC
 1150 15408-3 (possibly extended) must define the set of SARs/assurance package that
 1151 applies to the entire TOE:

1152 ○ If the set of SARs/assurance package is an (augmented) predefined EAL
 1153 (EAL1 to EAL7) or an (augmented) assurance package defined in an
 1154 applicable external reference, then the same name should be used.

1155 27 A PP may define a distinctive name for the sets of SARs/assurance packages that
 1156 are applicable.

1157 **2.3.3 PP-Modules**

1158 *(completes [CC-1-CD2]§10.2.2.2 PP-Module Conformance claims and conformance statements)*

- 1159 28 A PP-Module must declare its **conformance type**, which must be one of demon-
1160 strable, strict, or exact:
- 1161 ○ For demonstrable and strict conformance, there is no restriction on the
1162 conformance type of the PP-Module's base PPs/PP-Modules. The
1163 combination of demonstrable and strict conformance must be validated in
1164 the PP-Configuration evaluation.
 - 1165 ○ The combination of exact conformance with other types of conformance is
1166 not allowed.
 - 1167 ○ For exact conformance, the base PPs/PP-Modules must all declare exact
1168 conformance type.
- 1169 29 Note: such explicit declaration of demonstrable or strict conformance allows spon-
1170 sors to make the most appropriate statement in each PP-Module.
- 1171
- 1172 *([CC-1-CD2]§10.2.2.2 PP-Module assurance requirements)*
- 1173
- 1174 30 A PP-Module of demonstrable or strict conformance must define the set of
1175 SARs/assurance package that applies to the TSF that is introduced in the PP-Mod-
1176 ule:
- 1177 ○ If the set of SARs/assurance package is an (augmented) predefined EAL
1178 (EAL1 to EAL7) or an (augmented) assurance package defined in an
1179 applicable external reference, then the same name should be used.
- 1180 31 A PP-Module may define a distinctive name for the sets of SARs/assurance pack-
1181 ages that are applicable.
- 1182 32 A PP-Module of demonstrable or strict conformance must provide an assurance
1183 **rationale** that justifies
- 1184 ○ the consistency of the set of SARs/assurance package with regard to the
1185 threat model as defined in the SPD of the PP-Module,
 - 1186 ○ the consistency of the set of SARs/assurance package with all the sets of
1187 SARs/assurance package(s) defined in the base PPs/PP-Modules.
- 1188 33 Note: The PP-Module assurance rationale contributes to ensuring that the set of
1189 SARs/assurance package defined in the PP-Module does not undermine the security
1190 that is expected for the assets that are shared between the PP-Module and its base
1191 PPs/PP-Modules (if shared assets exist).
- 1192 34 Example: The assurance rationale may explain, for instance, the relationship with
1193 predefined EALs.

1194 **2.3.4 PP-Configurations**

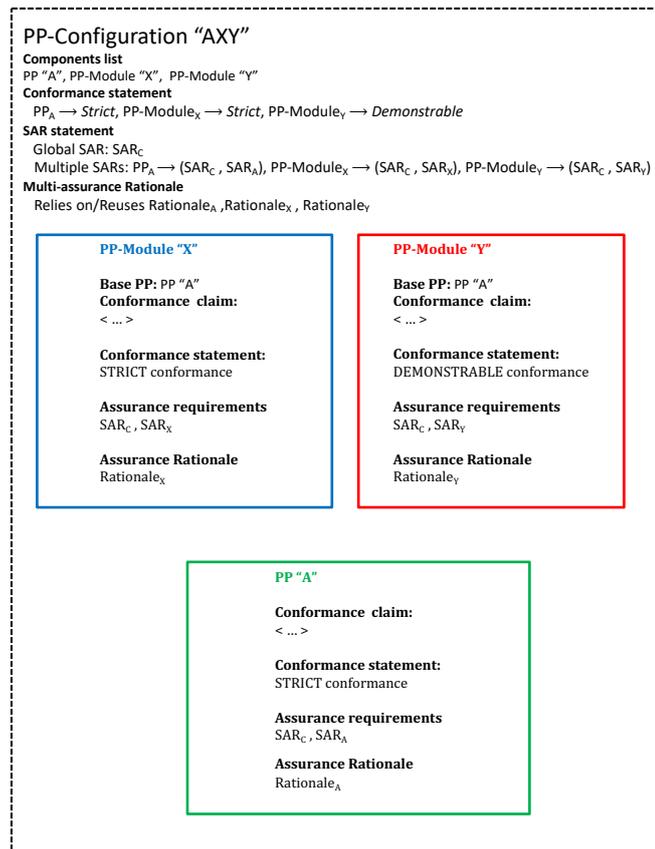
1195 *(completes [CC-1-CD2] §10.3.2.1)*

1196

- 1197 35 A PP-Configuration must define the **components list** that uniquely identifies all the
1198 PPs and PP-Modules that compose the PP-Configuration. A PP-Configuration must
1199 contain two or more components including at least one PP.
- 1200 36 A PP-Configuration must define the TOE and its organisation in terms of the sub-
1201 TSFs defined in its PPs and PP-Modules. A PP-Configuration contains exactly the
1202 SPD, security objectives and SFRs defined in its PPs/PP-Modules; the specification
1203 of any additional element must be done through the PPs/PP-Modules.
- 1204 37 Note 1: In the single-assurance evaluation approach, the sub-TSF organization is
1205 an option (i.e. it is acceptable to define one sub-TSF), which may facilitate the un-
1206 derstanding of the TSF and possibility definition of the evaluation strategy. How-
1207 ever, it does not impact the developer or evaluator activities (in the standard case
1208 where the PP-Configuration complies with ISO 15408-3 all the assurance require-
1209 ments apply to the entire TOE and TSF).
- 1210 38 Note 2: In the multi-assurance evaluation approach, the sub-TSF organization is
1211 mandatory. It allows ensuring that the different sets of SARs/assurance packages
1212 linked to those sub-TSFs are consistent and to apply the assurance requirements as
1213 required by each PP/PP-Module.
- 1214 39 Note 3: For the simplest multi-assurance PP-Configuration, that is, for a PP-Con-
1215 figuration containing one PP and one PP-Module with different sets of SARs/as-
1216 surance packages, the TSF organization is as follows: the global TSF is the union
1217 of the SFRs defined in the PP and in the PP-Module, and there are two sub-TSFs,
1218 which consist of the PP's TSF and the PP-Module's TSF.
- 1219 40 *(completes [CC-1-CD2] §10.3.2.3)*
- 1220 41 A PP-Configuration must declare the list of conformance types, which is inherited
1221 from the conformance types of its components (demonstrable, strict, or exact):
- 1222 ○ A PP-Configuration where all its components share one conformance type
1223 must declare the same conformance type, i.e. demonstrable, strict, or exact
1224 conformance.
 - 1225 ○ Otherwise, the PP-Configuration must provide the list of demonstrable and
1226 strict conformance types inherited from each of its components. The
1227 compatibility of demonstrable and strict conformance must be validated in
1228 the ST evaluation.
 - 1229 ○ The combination of exact conformance with other types of conformance is
1230 not allowed.
- 1231 42 *([CC-1-CD2] §10.3.2.4)*
- 1232 43 A PP-Configuration consisting of demonstrable and/or strict conformance compo-
1233 nents must define the applicable SARs/assurance packages:

- 1234 ○ The global set of SARs/assurance package that applies to the entire TOE.
 1235 This can be an (augmented) predefined EAL (EAL1 to EAL7), an
 1236 (augmented) assurance package defined in an applicable external reference
 1237 or a set of SARs/assurance package that is defined within the PP-
 1238 Configuration itself.
- 1239 ○ For each TSF part, the applicable set of SARs/assurance package. This can
 1240 be the same set of SARs/assurance package inherited from the PP or PP-
 1241 Module defining the TSF part, or a larger set (augmentation) which requires
 1242 the provision of a rationale.
- 1243 44 A PP-Configuration may define a distinctive name for the sets of SARs/assurance
 1244 packages that are globally and partially applicable.
- 1245 45 A PP-Configuration consisting of demonstrable and/or strict conformance compo-
 1246 nents must provide an assurance rationale for
- 1247 ○ the consistency of the global set of SARs/assurance package with regard to
 1248 the threat models as defined in the SPDs of the component PPs and PP-
 1249 Modules, and
- 1250 ○ the consistency of the global set of SARs/assurance package and all the sets
 1251 of SARs/assurance packages for the TOE parts with each other.
- 1252 46 Note 1: The multi-assurance approach allows applying multiple predefined EALs
 1253 to products with assets of different sensitivity. However, for the same reasons as
 1254 for PPs in the general model, PP-Configurations can claim sets of SARs/assurance
 1255 packages that are different from predefined EALs and/or that contain extended
 1256 SARs.
- 1257 47 Note 2: In most cases, the global set of SARs/assurance package can be built as the
 1258 common denominator of the sets of SARs/assurance packages that apply to the TSF
 1259 parts. However, as it is the case with Security Targets in the general model, the PP-
 1260 Configuration can declare additional or higher SARs than the common denomina-
 1261 tor. The evaluation of the PP-Configuration will ensure the consistency of the claim,
 1262 similar to the general approach for compliance with two or more PPs defining dif-
 1263 ferent sets of SARs/assurance packages, and similar to the approach for multi-as-
 1264 surance Security Targets which can extend the sets of SARs/assurance packages
 1265 defined in the associated PP-Configuration.
- 1266 48 Note 3: The PP-Configuration cannot claim less assurance requirements as the
 1267 global set of SARs/assurance package than those contained in the common denom-
 1268 inator of SARs/assurance packages that apply to all the TSF parts.
- 1269 49 By definition, the common denominator holds for all the TSF parts in the context
 1270 of the TOE, on all the TOE parts also holds on the global TOE.
- 1271 50 Note 4: The PP-Configuration assurance rationale contributes to ensuring that the
 1272 multiple sets of SARs/assurance packages do not undermine the security expected
 1273 for the assets that are shared between the PPs and PP-Modules that compose the
 1274 PP-Configuration. The PP-Configuration assurance rationale should rely on and/or
 1275 reuse the PP-Modules's assurance rationales.

1276 51 Figure 2-1 shows an example of multi-assurance PP-Configuration with one stand-
 1277 standard PP A and two PP-Modules X and Y. The common denominator of the sets of
 1278 SARs defined in A, X and Y is SAR_C, which has been chosen as global set of SARs
 1279 for the entire TOE (the rules allow to augment this set). The multiple sets of SARs
 1280 applicable to the sub-TSFs defined in A, X and Y are unchanged as well.



1281 52

Figure 2-1: Example of multi-assurance PP-Configuration

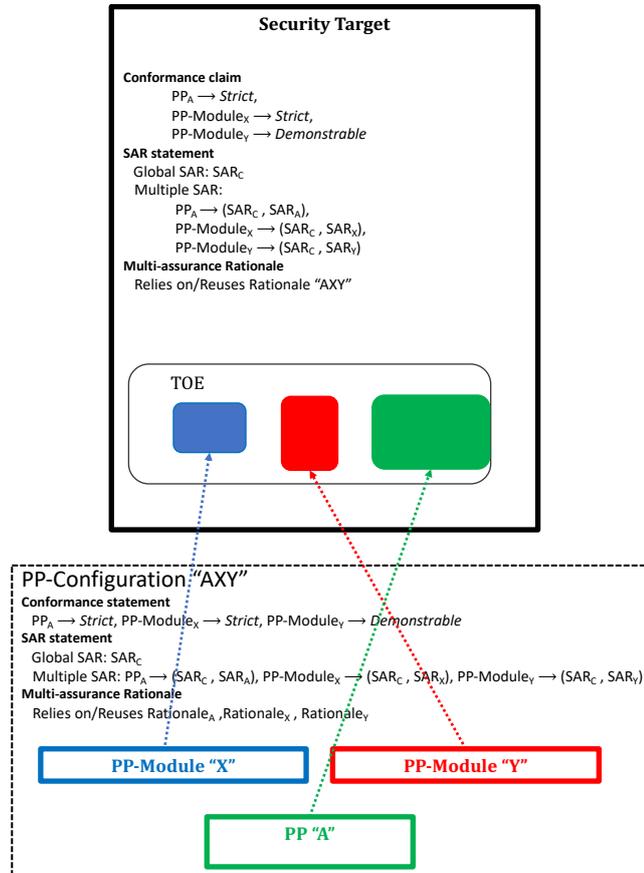
1282 **2.3.5 Usage of PPs and PP-Configurations in Security Targets**

1283 53 *(completes [CC-1-CD2] §11.4.1)*

1284 54 A Security Target may claim conformance with one or more PPs and PP-Configu-
 1285 rations, thereby complying with their conformance types. The consistency of the
 1286 combination of demonstrable and strict conformance must be validated in the ST
 1287 evaluation.
 1288

- 1289 55 The combination of exact conformance with other conformance types is not allowed, i.e. an ST cannot claim conformance to an exact PP/PP-Configuration and
1290 to a demonstrable or strict PP/PP-Configuration.
1291
- 1292 56 A Security Target that claims conformance with ISO/IEC 15408-3 (possibly extended)
1293 must define:
- 1294 • the **global set of SARs/assurance package** that applies to the entire TOE.
1295 This can be an (augmented) predefined EAL (EAL1 to EAL7), an
1296 (augmented) assurance package defined in an applicable external reference,
1297 or a set of SARs/assurance package defined within the ST itself.
- 1298 57 A Security Target that claims conformance with exactly one multi-assurance PP-
1299 Configuration may become a **multi-assurance Security Target** by additionally defining:
1300
- 1301 • for each TSF part, the applicable set of SARs/assurance package. This can
1302 be the same set of SARs/assurance package inherited from the PP-
1303 Configuration, or a larger set (augmentation) which requires the provision
1304 of a rationale.
- 1305 58 A multi-assurance Security Target may define a distinctive name for the sets of
1306 SARs/assurance packages that are globally and partially applicable. This name
1307 should be consistent with the name given in the PP-Configuration (if a name is
1308 given).
- 1309 59 A multi-assurance Security Target that extends the sets of SARs/assurance packages
1310 of the associated PP-Configuration must provide an assurance rationale that
1311 justifies the consistency of the extension.
- 1312 60 A multi-assurance Security Target has to conform according to each and all of the
1313 individual conformance types that are identified in the multi-assurance PP-Configuration.
1314
- 1315 61 Note 1: A Security Target that claims conformance with more than one PP/PP-
1316 Configuration can only define a global set of SARs/assurance package that applies
1317 to the entire TOE. In such case, the standard ASE rules for ensuring the consistency
1318 of the assurance requirements of the ST with regard to PPs/PP-Configurations apply.
1319
- 1320 62 Note 2: A Security Target that claims conformance with one PP-Configuration
1321 which defines only one set of SARs/assurance package for the entire TOE and its
1322 parts cannot become a multi-assurance Security Target. The reason is that the multi-
1323 assurance consistency rules are defined at PP-Configuration level. In order to
1324 achieve this, a multi-assurance PP-Configuration derived from the standard PP-
1325 Configuration must be defined and evaluated.
- 1326 63 Figure 2-2 shows an example of multi-assurance Security Target that claims conformance
1327 to PP-Configuration “AXY” with one standard PP A and two PP-Modules X and Y. The sub-TSF
1328 structure consists of the three TSF defined in A, X and Y. The global set of SARs (SAR_C) and the multiple sets of SARs applicable to the
1329 sub-TSFs have been taken from the PP-Configuration without augmentation.
1330

1331 64



1332 65

1333 **Figure 2-2: Example of multi-assurance Security Target**

1334 **2.4 Evaluation and evaluation results**

1335 *([CC-1 CD2]§12.8 Multi-assurance evaluation)*

1336 66 For a multi-assurance PP-Configuration, the ACE requirements ensure that the
 1337 combination of different sets of SARs/assurance packages does not undermine the
 1338 expected security of the underlying assets, as defined in the SPDs of the component
 1339 PPs and PP-Modules.

1340 67 For a multi-assurance ST, the ASE requirements ensure that the ST is conformant
 1341 to a multi-assurance PP-Configuration which satisfies ACE assurance require-
 1342 ments. This means that the organisation of the TSF in parts and the sets of SARs/as-
 1343 surance packages are consistent with the PP-Configuration.

1344 68 The multi-assurance evaluation of a TOE which complies with a multi-assurance
 1345 ST consists in evaluating the entire TOE against the global set of SARs/assurance
 1346 package and evaluating each of the TSF parts against the corresponding sets of
 1347 SARs/assurance packages.

1348 69 The order of the evaluation activities is left to the evaluator. The most suitable order
 1349 depends on factors such as the actual structure of the global TSF in terms of the
 1350 sub-TSFs and the difference between the global set of SARs/assurance package and
 1351 the multiple sets of SARs/assurance packages that apply to the sub-TSF.

1352 70 The limitation of multi-assurance evaluation to products (and Security Targets) that
 1353 comply with one multi-assurance PP-Configuration and the definition of the multi-
 1354 assurance consistency rules in ACE limits the impact on the other assurance classes.
 1355 The interpretation of the SARs applicable to a TSF part in a multi-assurance eval-
 1356 uation relies on the sub-TSF decomposition and is uniform for all assurance classes:
 1357 "TOE" stands for "global TOE" and "TSF" stands for "sub-TSF".

1358 2.5 Annex B – Specification of PPs

1359 Editor's Note:

1360 This annex is to be completed and updated in order to cover the multi-assurance paradigm once the
 1361 corresponding multi-assurance text is stable.

1362 2.6 Annex C – Specification of PP-Modules

1363 Editor's Note:

1364 This annex is to be completed and updated in order to cover the multi-assurance paradigm once the
 1365 corresponding multi-assurance text is stable.

1366 2.7 Annex D – Specification of STs

1367 Editor's Note:

1368 This annex is to be completed and updated in order to cover the multi-assurance paradigm once the
 1369 corresponding multi-assurance text is stable.

1370

1371 **3 ISO/EC 15408-3: Class ACE**

1372 71 This section presents the update of Class ACE to address the multi-assurance eval-
1373 uation framework as defined in [CC-3-CD2].

1374 72 Some indications for the CEM are attached to the statement of the components.

1375

1376 **73 (Clause 8) Class ACE: Protection Profile Configuration evaluation**1377 **1.1 Introduction**

1378 Evaluating a PP-Configuration is required to demonstrate that the PP-Configuration is
1379 sound and consistent. These properties are necessary for the PP-Configuration to be suita-
1380 ble for use as the basis for writing an ST.

1381 The class ACE is defined for the evaluation of a PP-Configuration composed of PPs and PP-
1382 Modules³. The evaluation of PPs is addressed in Class APE. The present class ACE defines
1383 the requirements for

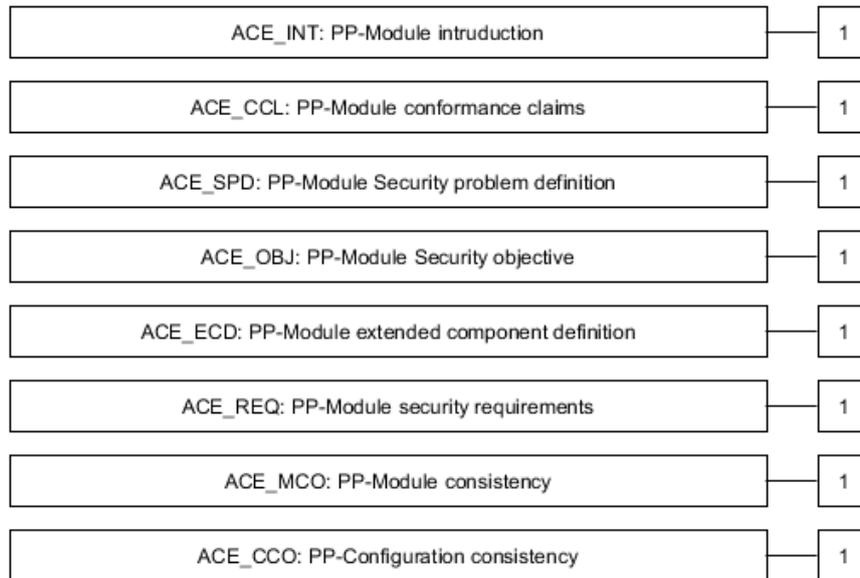
1384 • Evaluating the PP-Modules under the assumption that their base PPs/PP-Modules is
1385 internally consistent.

1386 • Evaluating the consistency of the combination of all the PPs and PP-Modules that be-
1387 long to the PP-Configuration.

1388 The evaluator shall decide the order in which the unevaluated components of a PP-Configu-
1389 ration (PPs and PP-Modules) are evaluated.

1390 This Clause should be used in conjunction with Annexes B and D in ISO/IEC 1540-1, as these
1391 Annexes clarify the concepts and provide examples.

³ Two PP-Modules may define each other in their basis, which means that a PP-Configura-
tion that contains one of them also contains the other.



1392

1393

Figure 3: ACE: Protection Profile Configuration evaluation class decomposition

1394 **1.2 PP-Module introduction (ACE_INT)**

1395 **1.2.1 Objectives**

1396 The objective of this family is to describe the TOE in a narrative way.

1397 The evaluation of the PP-Module introduction is required to demonstrate that the PP-Mod-
1398 ule is correctly identified, and that the PP-Module reference and TOE overview are con-
1399 sistent with each other.

1400

1401 **1.2.2 ACE_INT.1 PP-Module introduction**

1402 Dependencies: No dependencies.

1403

1404 **1.2.2.1 Developer action elements**

1405 **1.2.2.1.1 ACE_INT.1.1D**

1406 **The developer shall provide a PP-Module introduction.**

1407

1408 **1.2.2.2 Content and presentation elements**

1409 **1.2.2.2.1 ACE_INT.1.1C**

1410 **The PP-Module introduction shall contain a PP-Module reference and a TOE over-**
1411 **view.**

1412

1413 **1.2.2.2.2 ACE_INT.1.2C**

1414 **The PP-Module reference shall uniquely identify the PP-Module.**

1415

1416 **1.2.2.2.3 ACE_INT.1.3C**

1417 **The TOE overview shall summarise the usage and major security features of the TOE.**

1418

1419 **1.2.2.2.4 ACE_INT.1.4C**

1420 **1.2.2.2.5 The TOE overview shall identify the TOE type.**

1421 **1.2.2.2.6 ACE_INT.1.5C**

1422 **The TOE overview shall identify any non-TOE hardware/software/firmware available**
1423 **to the TOE.**

1424

1425 **1.2.2.2.7 ACE_INT.1.6C**

1426 **The PP-Module introduction shall uniquely identify the base PPs and PP-Modules it**
1427 **depends on.**

1428

1429 **1.2.2.2.8 ACE_INT.1.7C**

1430 **The PP-Module introduction shall describe the dependency structure of the base PPs**
1431 **and PP-Modules.**

1432

1433 **1.2.2.2.9 ACE_INT.1.8C**

1434 **The TOE overview shall describe the differences of the TOE with regard to the TOEs**
1435 **defined in the base PPs and PP-Modules.**

1436

1437 **1.2.2.3 Evaluator action elements**

1438 **1.2.2.3.1 ACE_INT.1.1E**

1439 **The evaluator shall confirm that the information provided meets all requirements for**
1440 **content and presentation of evidence.**

1441

1442 **1.3 PP-Module conformance claims (ACE_CCL)**

1443 **1.3.1 Objectives**

1444 The objective of this family is to determine the validity of the conformance claim and con-
1445 formance statement. Unlike standard Protection Profiles, a PP-Module cannot claim con-
1446 formance to another PP or PP-Module.

1447

1448 **1.3.2 ACE_CCL.1 PP-Module conformance claims**

1449 Dependencies: ACE_INT.1 PP-Module introduction

1450 ACE_ECD.1 PP-Module extended components definition

1451 ACE_REQ.1 PP-Module stated security requirements or ACE_REQ.2 PP-Mod-
1452 ule security requirements

1453

1454 **1.3.2.1.1 ACE_CCL.1.1D**

1455 **The developer shall provide a conformance claim.**

1456

1457 **1.3.2.1.2 ACE_CCL.1.2D**

1458 **The developer shall provide a conformance statement.**

1459

1460 **1.3.2.2 Content and presentation elements**

1461 **1.3.2.2.1 ACE_CCL.1.1C**

1462 **The conformance claim shall contain an ISO/IEC 15408 conformance claim that iden-**
1463 **tifies the ISO/IEC 15408-1 edition to which the PP-Module claims conformance.**

1464

1465 **1.3.2.2.2 ACE_CCL.1.2C**

1466 **ISO/IEC 15408 conformance claim shall describe the conformance of the PP-Module**
1467 **to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 ex-**
1468 **tended.**

1469

1470 **1.3.2.2.3 ACE_CCL.1.3C**

1471 **The ISO/IEC 15408 conformance claim shall describe the conformance of the PP-Mod-**
1472 **ule to this document as either “ISO/IEC 15408-3 conformant” or ISO/IEC 15408-3 ex-**
1473 **tended.”**

1474

1475 **1.3.2.2.4 ACE_CCL.1.4C**

1476 **ISO/IEC 15408 conformance claim shall be consistent with the extended components**
1477 **definition.**

1478

1479 **1.3.2.2.5 ACE_CCL.1.5C**

1480 **The conformance claim shall identify all security requirement packages to which the**
1481 **PP claims conformance.**

1482

1483 **1.3.2.2.6 ACE_CCL.1.6C**

1484 **The conformance claim shall describe any conformance of the PP-Module to a pack-**
1485 **age as either package-conformant or package-augmented.**

1486

1487 **1.3.2.2.7 ACE_CCL.1.7C**

1488 **The conformance statement shall describe the conformance required of any PP-Con-**
1489 **figuration/ST to the PP-Module as one of exact, strict, or demonstrable.**

1490

1491 **1.3.2.2.8 ACE_CCL.1.8C**

1492 **The conformance statement shall identify the set of PPs and PP-Modules to which, in**
1493 **combination with the PP-Module under evaluation, exact conformance is allowed to**
1494 **be claimed.**

1495

1496 **1.3.2.2.9 ACE_CCL.1.10C**

1497 **The conformance statement shall identify the set of derived Evaluation Methods and**
1498 **Evaluation Activities (if any) that shall be used with the PP-Module under evaluation.**
1499 **This list shall contain any Evaluation Methods and Evaluation Activities that are spec-**
1500 **ified in the PP-Module but also any Evaluation Activities and Evaluation Methods**
1501 **specified in the base PPs and/or PP-modules and/or in the packages (if any) for**
1502 **which conformance is being claimed by the PP-Module under evaluation.**

1503

1504 **1.3.2.3 Evaluator action elements**

1505 **1.3.2.3.1 ACE_CCL.1.1E**

1506 **The evaluator shall confirm that the information provided meets all requirements for**
1507 **content and presentation of evidence.**

1508

1509 **1.4 PP-Module Security problem definition (ACE_SPD)**

1510 **1.4.1 Objectives**

1511 This part of the PP-Module defines the security problem to be addressed by the TOE and the
1512 operational environment of the TOE.

1513 Evaluation of the security problem definition is required to demonstrate that the security
1514 problem intended to be addressed by the TOE and its operational environment, is clearly
1515 defined.

1516

1517 **1.4.2 ACE_SPD.1 PP-Module Security problem definition**

1518 Dependencies: No dependencies.

1519

1520 **1.4.2.1 Developer action elements**

1521 **1.4.2.1.1 ACE_SPD.1.1D**

1522 **The developer shall provide a security problem definition.**

1523

1524 **1.4.2.2 Content and presentation elements**

1525 **1.4.2.2.1 ACE_SPD.1.1C**

1526 **The security problem definition shall describe the threats.**

1527

1528 **1.4.2.2.2 ACE_SPD.1.2C**

1529 **All threats shall be described in terms of a threat agent, an asset, and an adverse ac-**
1530 **tion.**

1531

1532 **1.4.2.2.3 ACE_SPD.1.3C**

1533 **The security problem definition shall describe the OSPs.**

1534

1535 **1.4.2.2.4 ACE_SPD.1.4C**

1536 The security problem definition shall describe the assumptions about the operational envi-
1537 ronment of the TOE.

1538

1539 **1.4.2.3 Evaluator action elements**

1540 **1.4.2.3.1 ACE_SPD.1.1E**

1541 **The evaluator shall confirm that the information provided meets all requirements for**
1542 **content and presentation of evidence.**

1543

1544 **1.5 PP-Module Security objectives (ACE_OBJ)**

1545 **1.5.1 Objectives**

1546 The security objectives are a concise statement of the intended response to the security
1547 problem defined through the **Erreur ! Source du renvoi introuvable.** family.

1548 Evaluation of the security objectives is required to demonstrate that the security objectives
1549 adequately and completely address the security problem definition and that the division of
1550 this problem between the TOE and its operational environment is clearly defined.

1551

1552 **1.5.2 Component levelling**

1553 The components in this family are levelled on whether they prescribe only security objec-
1554 tives for the operational environment (see ACE_OBJ.1), or also security objectives for the
1555 TOE (see ACE_OBJ.2).

1556

1557 **1.5.3 ACE_OBJ.1 Direct Rationale PP-Module Security objectives**

1558 Dependencies: No dependencies.

1559

1560 **1.5.4 Application notes**

1561 If the PP-Module uses the Direct Rationale approach then all the elements defined in
1562 ACE_OBJ.1 hold.

1563

1564 **1.5.4.1 Developer action elements**

1565 **1.5.4.1.1 ACE_OBJ.1.1D**

1566 **The developer shall provide a statement of security objectives for the PP-Module.**

1567

1568 **1.5.4.2 Content and presentation elements**

1569 **1.5.4.2.1 ACE_OBJ.1.1C**

1570 **The statement of security objectives shall describe the security objectives for the op-**
1571 **erational environment.**

1572

1573 **1.5.4.3 Evaluator action elements**

1574 **1.5.4.3.1 ACE_OBJ.1.1E**

1575 **The evaluator shall confirm that the information provided meets all requirements for**
1576 **content and presentation of evidence.**

1577

1578 **1.5.5 ACE_OBJ.2 PP-Module Security objectives**

1579 Dependencies: ACE_SPD.1 PP-Module security problem definition.

1580

1581 **1.5.6 Application notes**

1582 If the PP-Module does not use the Direct Rationale approach then all elements of ACE_OBJ.2
1583 hold.

1584

1585 **1.5.6.1 Developer action elements**

1586 **1.5.6.1.1 ACE_OBJ.2.1D**

1587 **The developer shall provide a statement of security objectives for the PP-Module.**

1588

1589 **1.5.6.1.2 ACE_OBJ.2.2D**

1590 **The developer shall provide a security objectives rationale for the PP-Module.**

1591

1592 **1.5.6.2 Content and presentation elements**

1593 **1.5.6.2.1 ACE_OBJ.2.1C**

1594 **The statement of security objectives shall describe the security objectives for the TOE**
1595 **and the security objectives for the operational environment.**

1596

1597 **1.5.6.2.2 ACE_OBJ.2.2C**

1598 **The security objectives rationale shall trace each security objective for the TOE back**
1599 **to threats countered by that security objective and OSPs enforced by that security ob-**
1600 **jective.**

1601

1602 **1.5.6.2.3 ACE_OBJ.2.3C**

1603 **The security objectives rationale shall trace each security objective for the opera-**
1604 **tional environment back to threats countered by that security objective, OSPs en-**
1605 **forced by that security objective, and assumptions upheld by that security objective.**

1606

1607 **1.5.6.2.4 ACE_OBJ.2.4C**

1608 **The security objectives rationale shall demonstrate that the security objectives counter all threats.**

1610

1611 **1.5.6.2.5 ACE_OBJ.2.5C**

1612 **The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.**

1614

1615 **1.5.6.2.6 ACE_OBJ.2.6C**

1616 The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

1618

1619 **1.5.6.3 Evaluator action elements**

1620 **1.5.6.3.1 ACE_OBJ.2.1E**

1621 **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

1623

1624 **1.6 PP-Module extended components definition (ACE_ECD)**

1625 **1.6.1 Objectives**

1626 Extended security functional requirements are requirements that are not based on components from **ISO/IEC 15408-2**, but are based on extended components: components defined by the PP-Module author.

1629

1630 Evaluation of the definition of extended functional components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they may not be clearly expressed using existing **ISO/IEC 15408-2** components.

1633

1634 **1.6.2 ACE_ECD.1 PP-Module extended components definition**

1635 Dependencies: No dependencies.

1636

1637 **1.6.2.1 Developer action elements**

1638 **1.6.2.1.1 ACE_ECD.1.1D**

1639 **The developer shall provide a statement of security requirements for the PP-Module.**

1640

1641 **1.6.2.1.2 ACE_ECD.1.2D**

1642 **The developer shall provide an extended components definition for the PP-Module.**

1643

1644 **1.6.2.2 Content and presentation elements**

1645 **1.6.2.2.1 ACE_ECD.1.1C**

1646 **The statement of security requirements shall identify all the extended security re-**
1647 **quirements.**

1648

1649 **1.6.2.2.2 ACE_ECD.1.2C**

1650 **The extended components definition shall define an extended component for each**
1651 **extended security requirement.**

1652

1653 **1.6.2.2.3 ACE_ECD.1.3C**

1654 **The extended components definition shall describe how each extended component is**
1655 **related to the existing ISO/IEC 15408 components, families, and classes.**

1656

1657 **1.6.2.2.4 ACE_ECD.1.4C**

1658 **The extended components definition shall use the existing ISO/IEC 15408 compo-**
1659 **nents, families, classes, and methodology as a model for presentation.**

1660

1661 **1.6.2.2.5 ACE_ECD.1.5C**

1662 **1.6.2.2.6 The extended components shall consist of measurable and objective**
1663 **elements such that conformance or nonconformance to these elements can be**
1664 **demonstrated.**

1665 **1.6.2.3 Evaluator action elements**

1666 **1.6.2.3.1 ACE_ECD.1.1E**

1667 **The evaluator shall confirm that the information provided meets all requirements for**
1668 **content and presentation of evidence.**

1669

1670 **1.6.2.3.2 ACE_ECD.1.2E**

1671 **The evaluator shall confirm that no extended component may be clearly expressed**
1672 **using existing components.**

1673

1674 **1.7 PP-Module security requirements (ACE_REQ)**

1675 **1.7.1 Objectives**

1676 The SFRs form a clear, unambiguous and well-defined description of the expected security
1677 behaviour of the TOE. The SARs form a clear, unambiguous and well-defined description of
1678 the expected activities that will be undertaken to gain assurance in the TOE.

1679

1680 Evaluation of the security requirements is required to ensure that they are clear, unambigu-
1681 ous and well-defined.

1682

1683 **1.7.2 Component levelling**

1684 The components in this family are levelled on whether they are stated as is (see
1685 ACE_REQ.1), or whether the SFRs are derived from security objectives for the TOE (see
1686 ACE_REQ.2.).

1687

1688 **Editor's note:**

1689 The title of ACE_REQ.1 is confusing. We propose to rename it as "Direct rationale PP-Module security
1690 requirements".

1691 Unless experts pronounce themselves against this proposal, this change will be made in the next
1692 draft.

1693 The same applies to the title of APE_REQ.1

1694 **1.7.3 ACE_REQ.1 PP-Module stated security requirements**

1695 Dependencies: **Erreur ! Source du renvoi introuvable.**

1696 ACE_SPD.1 PP-Module security problem definition

1697

1698 **1.7.3.1 Developer action elements**

1699 **1.7.3.1.1 ACE_REQ.1.1D**

1700 **The developer shall provide a statement of security requirements for the PP-Module.**

1701

1702 **1.7.3.1.2 ACE_REQ.1.2D**

1703 **The developer shall provide a security requirements rationale for the PP-Module.**

1704

1705 **1.7.3.2 Content and presentation elements**

1706 **1.7.3.2.1 ACE_REQ.1.1C**

1707 **The statement of security requirements shall describe the SFRs and the SARs.**

1708

1709 **1.7.3.2.2 ACE_REQ.1.2C**

1710 **All subjects, objects, operations, security attributes, external entities and other terms**
1711 **that are used in the SFRs and the SARs shall be defined.**

1712

1713 **1.7.3.2.3 ACE_REQ.1.3C**

1714 **The statement of security requirements shall include a natural language description,**
1715 **part of which describes how the SFRs combine together to provide security function-**
1716 **ality in terms of the architecture that is observable to Administrators and other us-**
1717 **ers, or in terms of internal features or properties.**

1718

1719 **1.7.3.2.4 ACE_REQ.1.4C**

1720 **The statement of security requirements shall identify all operations on the security**
1721 **requirements.**

1722

1723 **1.7.3.2.5 ACE_REQ.1.5C**

1724 **All operations shall be performed correctly.**

1725

1726 **1.7.3.2.6 ACE_REQ.1.6C**

1727 **Each dependency of the security requirements shall either be satisfied, or the secu-**
1728 **rity requirements rationale shall justify the dependency not being satisfied.**

1729

1730 **1.7.3.2.7 ACE_REQ.1.7C**

1731 **The security requirements rationale shall trace each SFR back to the threats coun-**
1732 **tered by that SFR and the OSPs enforced by that SFR.**

1733

1734 **1.7.3.2.8 ACE_REQ.1.8C**

1735 **The security requirements rationale shall trace each security objective for the opera-**
1736 **tional environment back to the threats countered by that security objective, the OSPs**
1737 **enforced by that security objective, and the assumptions upheld by that security ob-**
1738 **jective.**

1739

1740 **1.7.3.2.9 ACE_REQ.1.9C**

1741 **The security requirements rationale shall demonstrate that the SFRs (in conjunction**
1742 **with the security objectives for the environment) counter all the threats for the TOE.**

1743

1744 **1.7.3.2.10 ACE_REQ.1.10C**

1745 **The security requirements rationale shall demonstrate that the SFRs (in conjunction**
1746 **with the security objectives for the environment) enforce all the OSPs for the TOE.**

1747

1748 **1.7.3.2.11 ACE_REQ.1.11C**

1749 **The security requirements rationale shall demonstrate that the security objectives**
1750 **for the operational environment uphold all assumptions.**

1751

1752 **1.7.3.2.12 ACE_REQ.1.12C**

1753 The statement of security requirements shall be internally consistent.

1754

1755 **1.7.3.3 Evaluator action elements**

1756 **1.7.3.3.1 ACE_REQ.1.1E**

1757 **The evaluator shall confirm that the information provided meets all requirements for**
1758 **content and presentation of evidence.**

1759

1760 **1.7.4 ACE_REQ.2 PP-Module derived security requirements**

1761 Dependencies: ACE_ECD.1 PP-Module extended components definition

1762 ACE_OBJ.1 PP-Module Security objectives

1763

1764 **1.7.4.1 Developer action elements**

1765 **1.7.4.1.1 ACE_REQ.2.1D**

1766 **The developer shall provide a statement of security requirements for the PP-Module.**

1767

1768 **1.7.4.1.2 ACE_REQ.2.2D**

1769 **The developer shall provide a security requirement rationale for the PP-Module.**

1770

1771 **1.7.4.2 Content and presentation elements**

1772 **1.7.4.2.1 ACE_REQ.2.1C**

1773 **The statement of security requirements shall describe the SFRs and the SARs.**

1774

1775 **1.7.4.2.2 ACE_REQ.2.2C**

1776 **All subjects, objects, operations, security attributes, external entities and other terms**
1777 **that are used in the SFRs and the SARs shall be defined.**

1778

1779 **1.7.4.2.3 ACE_REQ.2.3C**

1780 **The statement of security requirements shall include a natural language description,**
1781 **part of which describes how the SFRs combine together to provide security function-**
1782 **ality in terms of the architecture that is observable to Administrators and other us-**
1783 **ers, or in terms of internal features or properties.**

1784

1785 **1.7.4.2.4 ACE_REQ.2.4C**

1786 **The statement of security requirements shall identify all operations on the security**
1787 **requirements.**

1788

1789 **1.7.4.2.5 ACE_REQ.2.5C**

1790 **All operations shall be performed correctly.**

1791

1792 **1.7.4.2.6 ACE_REQ.2.6C**

1793 **Each dependency of the security requirements shall either be satisfied, or the secu-**
1794 **rity requirements rationale shall justify the dependency not being satisfied.**

1795

1796 **1.7.4.2.7 ACE_REQ.2.7C**

1797 **The security requirements rationale shall trace each SFR back to the security objec-**
1798 **tives for the TOE and OSPs enforced by that SFR.**

1799

1800 **1.7.4.2.8 ACE_REQ.2.8C**

1801 **The security requirements rationale shall demonstrate that the SFRs meet all secu-**
1802 **rity objectives for the TOE.**

1803

1804 **1.7.4.2.9 ACE_REQ.2.9C**

1805 **The security requirements rationale shall demonstrate that the SFRs enforce all**
1806 **OSPs.**

1807

1808 **1.7.4.2.10 ACE_REQ.2.10C**1809 **The security requirements rationale shall explain why the SARs were chosen.**

1810

1811 **1.7.4.2.11 ACE_REQ.2.11C**

1812 The statement of security requirements shall be internally consistent.

1813

1814 **1.7.4.3 Evaluator action elements**1815 **1.7.4.3.1 ACE_REQ.2.1E**1816 **The evaluator shall confirm that the information provided meets all requirements for**
1817 **content and presentation of evidence.**

1818

1819 **1.8PP-Module consistency (ACE_MCO)**1820 **1.8.1 Objectives**

1821 The objective of this family is to determine the consistency of the PP-Module.

1822

1823 **1.8.2 ACE_MCO.1 PP-Module consistency**

1824 Dependencies: ACE_INT.1 PP-Module introduction

1825 ACE_SPD.1 PP-Module Security problem definition

1826 ACE_OBJ.1 Direct Rationale PP-Module Security objectives for the environ-
1827 ment or ACE_OBJ.2 PP-Module Security objectives1828 ACE_REQ.1 PP-Module stated security requirements or ACE_REQ.2 PP-
1829 Module security requirements

1830

1831 **1.8.2.1 Developer action elements**1832 **1.8.2.1.1 ACE_MCO.1.1D**1833 **The developer shall provide a consistency rationale of the PP-Module for each of the**
1834 **alternative sets of Base-PPs and PP-Modules identified in the PP-Module introduc-**
1835 **tion.**

1836

1837 **1.8.2.2 Content and presentation elements**1838 **1.8.2.2.1 ACE_MCO.1.1C**1839 **The consistency rationale shall demonstrate that the TOE type of the PP-Module and**
1840 **the TOE types of its base PPs and PP-Modules are consistent.**

1841

1842 **1.8.2.2.2 ACE_MCO.1.2C**

1843 **Editor's Note:** this is also meaningful for APE and ASE when the ST claims conformance to more than
 1844 one PP or when the ST adds elements to the PPs it conforms to: The change has not been proposed
 1845 yet in ASE/APE, but if experts agree, we suggest cascading this change in the next CD.

1846 **The consistency rationale shall identify the assets of the PP-Module that also belong**
 1847 **to some of its base PP(s) and/or PP-Module(s) and amongst them those for which the**
 1848 **PP-Module and the base PP(s) and PP-Module(s) define different security problems.**

1849

1850

- CEM:

1851

1852

1853

- The evaluator shall check that the consistency rationale contains the set of assets shared between the PP-Module and its base PPs and PP-Modules, and that this set is unambiguous and complete.

1854

1855

1856

1857

- The evaluator shall check that the consistency rationale contains the subset of shared assets that hold different security properties and/or are subject to different threat agents or threats scenarios, and that this subset is unambiguous and complete.

1858

1859

1860

Editor's Note: A multi-assurance ST must conform to one and only one multi-assurance PP-Configuration, which leads to a consistency check at PP-Configuration level, i.e. through ACE, without modification of APE or ASE.

1861

1862 **1.8.2.2.3 ACE_MCO.1.3C**

1863 **The consistency rationale shall demonstrate that the security problem definition of**
 1864 **the PP-Module and the security problem definition of its base PPs and PP-Modules**
 1865 **are consistent.**

1866

- CEM:

1867

1868

1869

1870

1871

- For all the assets that are shared between the PP-Module and one or more base PP(s) or PP-Module(s), the evaluator determines that all the differences in the security problem definitions are justified. For instance, the asset resides in different locations or at different times or is subject to different operational environment conditions.

1872

1873 **1.8.2.2.4 ACE_MCO.1.4C**

1874 **The consistency rationale shall demonstrate that the security objectives of the PP-**
 1875 **Module and the security objectives of its base PPs and PP-Modules are consistent.**

1876

1877 **1.8.2.2.5 ACE_MCO.1.5C**

1878 **The consistency rationale shall demonstrate that the security functional require-**
 1879 **ments of the PP-Module and the security functional requirements of its base PPs and**
 1880 **PP-Modules are consistent.**

1881

1882 **1.8.2.2.6 ACE_MCO.1.6C**

1883 **The consistency rationale shall demonstrate that the security assurance require-**
 1884 **ments of the PP-Module and the security assurance requirements of its base PPs and**
 1885 **PP-Modules are consistent.**

1886

1887

- CEM:

1888

- The evaluator shall check that the PP-Module does not undermine

 1889

- the expected security of the assets of the base PPs and PP-

 1890

- Modules. If the PP-Module and a base PP or PP-Module share an

 1891

- asset which is subject to an equivalent security problem in both

 1892

- places, then the PP-Module AP is consistent with the base PP or

 1893

- PP-Module AP.

1894

- The evaluator shall check that the base PPs and PP-Modules do

 1895

- not undermine the expected security of each other. If an asset is

 1896

- shared by two base PPs or PP-Modules and this asset is subject to

 1897

- an equivalent security problem in both places, then the APs of

 1898

- these PPs or PP-Modules are consistent.

1899

1900 **1.8.2.3 Evaluator action elements**1901 **1.8.2.3.1 ACE_MCO.1.1E**

1902 **The evaluator shall confirm that the information provided meets all requirements for**
 1903 **content and presentation of evidence. If the PP-Module specifies alternative sets of**
 1904 **Base-PPs and PP-Modules, the evaluator shall perform this action for each con-**
 1905 **sistency rationale.**

1906

1907 **1.9 PP-Configuration consistency (ACE_CCO)**1908 **1.9.1 Objectives**

1909 The objective of this family is to determine the well-formedness and the consistency of the
 1910 PP-Configuration.

1911

1912 **1.9.2 ACE_CCO.1 PP-Configuration consistency**

1913 Dependencies: ACE_INT.1 PP-Module introduction

- 1914 ACE_CCL.1 PP-Module conformance claims
- 1915 ACE_SPD.1 PP-Module security problem definition
- 1916 ACE_OBJ.1 Direct Rationale PP-Module security objectives for the environ-
1917 ment or ACE_OBJ.2 PP-Module Security objectives
- 1918 ACE_ECD.1 PP-Module extended component definition
- 1919 ACE_REQ.1 PP-Module stated security requirements or ACE_REQ.2 PP-
1920 Module security requirements
- 1921 ACE_MCO.1 PP-Module consistency
- 1922 APE_*
- 1923
- 1924 **1.9.2.1 Developer action elements**
- 1925 **1.9.2.1.1 ACE_CCO.1.1D**
- 1926 **The developer shall provide the reference of the PP-Configuration.**
- 1927
- 1928 **1.9.2.1.2 ACE_CCO.1.2D**
- 1929 **The developer shall provide a components list.**
- 1930
- 1931 **1.9.2.1.3 ACE_CCO.1.3D**
- 1932 **The developer shall provide a TOE overview.**
- 1933
- 1934 **1.9.2.1.4 ACE_CCO.1.4D**
- 1935 **The developer shall provide a conformance claim.**
- 1936
- 1937 **1.9.2.1.5 ACE_CCO.1.5D**
- 1938 **The developer shall provide a conformance statement.**
- 1939
- 1940 **1.9.2.1.6 ACE_CCO.1.7D**
- 1941 **The developer shall provide a consistency rationale.**
- 1942
- 1943 **1.9.2.2 Content and presentation elements**
- 1944 **1.9.2.2.1 ACE_CCO.1.1C**
- 1945 **The PP-Configuration reference shall uniquely identify the PP-Configuration.**

1946

1947 **1.9.2.2.2 ACE_CCO.1.2C**

1948 **The components list shall uniquely identify the PPs and PP-Modules that compose the**
1949 **PP-Configuration.**

1950

1951 **1.9.2.2.3 ACE_CCO.1.3C**

1952 **For each PP-Module identified in the components list of the PP-Configuration, the list**
1953 **contains at least one of its sets of base PPs and PP-Modules.**

1954

1955 **1.9.2.3 ACE_CCO.1.4C**

1956 **The TOE overview shall identify the TOE type.**

1957

1958 **1.9.2.4 ACE_CCO.1.5C**

1959 **The TOE overview shall describe the organisation of the TOE in terms of the sub-TSFs**
1960 **(TSF parts) defined in the PPs and PP-Modules that belong to the components list.**

1961

1962 **1.9.2.5 ACE_CCO.1.6C**

1963 **The conformance claim shall contain an ISO/IEC 15408 conformance claim that iden-**
1964 **tifies the ISO/IEC 15408-1 edition(s) to which the PPs and PP-Modules that compose**
1965 **the PP-Configuration claim conformance.**

1966

1967 **1.9.2.6 ACE_CCO.1.7C**

1968 **ISO/IEC 15408 conformance claim shall describe the conformance of the PP-Configu-**
1969 **ration to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2**
1970 **extended.**

1971

1972 **1.9.2.7 ACE_CCO.1.8C**

1973 **The ISO/IEC 15408 conformance claim shall describe the conformance of the PP-Con-**
1974 **figuration to this document as either “ISO/IEC 15408-3 conformant” or ISO/IEC**
1975 **15408-3 extended.”**

1976

1977 **1.9.2.8 ACE_CCO.1.9C**

1978 **ISO/IEC 15408 conformance claim shall be consistent with the extended components**
1979 **definition of the composing PPs and PP-Modules.**

1980

1981 **1.9.2.9 ACE_CCO.1.10C**

1982 **The conformance statement shall specify the required conformance to the PP-Config-**
 1983 **uration as one of exact, strict, demonstrable, or list of strict and demonstrable types**
 1984 **inherited from its composing PPs and PP-Modules.**

1985

1986 **1.9.2.10 ACE_CCO.1.11C**

1987 **The conformance statement of a PP-Configuration of strict, demonstrable, or strict**
 1988 **and demonstrable conformance shall define the applicable SARs/assurance pack-**
 1989 **ages:**

- 1990 • **The global set of SARs/assurance package that applies to the entire TOE.**
- 1991 • **For each sub-TSF (TSF part) defined in the composing PPs and PP-Modules, the**
 1992 **applicable set of SARs/assurance package.**

- 1993 • **CEM:**

- 1994 • **For demonstrable, strict or exact conformance, the evaluator shall**
 1995 **check that all the PPs and PP-Modules that belong to the PP-**
 1996 **Configuration declare the same conformance type, i.e.**
 1997 **demonstrable, strict or exact conformance type, respectively.**

- 1998 • **Otherwise, the evaluator shall check that the PP-Configuration**
 1999 **declares a list of demonstrable and strict conformance that maps**
 2000 **to the conformance types inherited from the PPs and PP-Modules**
 2001 **that belong to the PP-Configuration.**

- 2002 • **The evaluator shall check that the conformance statement does not**
 2003 **combine exact conformance with other types of conformance.**

2004

2005 **1.9.2.11 ACE_CCO.1.12C**

2006 **The conformance statement of a PP-Configuration of exact conformance type shall**
 2007 **identify the set of derived Evaluation Methods and Evaluation Activities (if any) that**
 2008 **shall be used with the PP under evaluation. This list shall contain any Evaluation**
 2009 **Methods and Evaluation Activities that are specified in the PP it but also any Evalua-**
 2010 **tion Activities and Evaluation Methods specified in PPs and/or PP-modules and/or**
 2011 **packages for which conformance is being claimed by the PP under evaluation.**

2012

2013 **1.9.2.1 ACE_CCO.1.13C**

2014 **The consistency rationale shall demonstrate that the TOE type defined in the PP-Con-**
 2015 **figuration is consistent with the TOE types defined in the PPs and PP-Modules that**
 2016 **belong to the PP-Configuration components list.**

2017

2018 **1.9.2.2 ACE_CCO.1.14C**

2019 **The consistency rationale shall demonstrate that the union of all the SPDs, security**
 2020 **objectives and security functional requirements defined in the PPs and PP-Modules**
 2021 **of the PP-Configuration components list is consistent.**

2022 • CEM:

2023 • The same evaluation units defined in ACE_MCO for PP-Modules
 2024 apply to the complete set of elements.

2025

2026 **1.9.2.3 ACE_CCO.1.15C**

2027 **The consistency rationale of a PP-Configuration of strict, demonstrable, or strict and**
 2028 **demonstrable conformance type shall demonstrate**

2029 • **the consistency of the global set of SARs/assurance package with regard to the**
 2030 **threat models as defined in the SPDs of the component PPs and PP-Modules,**
 2031 **and**

2032 • **the consistency of the global set of SARs/assurance package and all the sets of**
 2033 **SARs/assurance packages for the sub-TSFs (TSF parts) with each other.**

2034 **1.9.2.4 Evaluator action elements**2035 **1.9.2.4.1 ACE_CCO.1.1E**

2036 **The evaluator shall confirm that the information provided meets all requirements for**
 2037 **content and presentation of evidence.**

2038

2039 **1.9.2.4.2 ACE_CCO.1.2E**

2040 **The evaluator shall check that the PP-Configuration consisting of all the PPs and PP-**
 2041 **Modules identified in the components list is consistent.**

2042 74

2043 **3.1 Other assurance classes**

2044 75 The following paragraphs have been added in [CC-3-CD2]:

2045

2046 ADV, lines 2070 – 2083:

2047 In case of a **multi-assurance evaluation** the requirements for the descrip-
 2048 tion (at the various levels of abstraction) of the design and implementation
 2049 of the SFRs (ADV_FSP, ADV_TDS, ADV_IMP and ADV_COMP) will be pre-
 2050 sented for the **sub-TSF** of the TOE. The architecture family (Security Archi-
 2051 tecture (ADV_ARC)) provides for requirements and analysis of the TOE
 2052 based on properties of domain separation, self-protection, and non-bypassa-
 2053 bility which also may hold for boundaries between the **sub-TSF**.

2054

2055 ADV_ARC, lines 2123-2124:

2056 In case of a **multi-assurance evaluation** the properties of self-protection,
2057 domain separation, and non-bypassability may also be described for bounda-
2058 ries between the **sub-TSF**.

2059

2060 AVA_VAN, lines 5273-5274:

2061 76 In case of a **multi-assurance evaluation** the vulnerability analysis will as-
2062 sess the defined **sub-TSF** as well as the TOE as a whole.

2063

2064
2065
2066

Annex C
(informative)
Concept approach to the ISO/IEC 15408 & 18045 Terminology

2067
2068
2069
2070

Editor note:

This is the text submitted to previous round of consultation. Updated, separated editors' contribution will be provided soon.

2071

1 Background

2072
2073
2074

According to the ISO/IEC JTC1 Directives, Part 2, Clause 16.4, "*Terms and definitions should preferably be listed according to the hierarchy of the concepts (i.e. systematic order). Alphabetical order is the least preferred order.*"

2075
2076
2077
2078
2079
2080

The current version of ISO/IEC 15408 series of standards and ISO/IEC 18045 have all their terms presented in alphabetical order, which works in English only. Hence all translated versions do not follow even the least preferable order as dictated by the Directives. Additionally, presenting hundreds of terms in alphabetical order does not help users understanding the idea behind since definitions of adjacent terms can refer to completely different concepts.

2081
2082
2083
2084

Further, by the decision taken at the Berlin meeting (October 2017) ALL terms related to the ICT security evaluation are to be gathered in one document, ie. ISO/IEC 15408-1. It means special attention should be paid to Clause 3 to present terms in a clear and easy-to-follow way for all potential users of the series of the 15408 standards.

2085
2086

Concept approach is described in several international standards related to terminology developed by the ISO Technical Committee TC37 *Language and terminology*.

2087
2088

A basic principle for this approach is that one term corresponds to one concept and only one concept corresponds to one term in a given domain or subject in a given language.

2089

For this document relevant terms are defined as follows⁴:

2090
2091
2092
2093
2094
2095
2096
2097

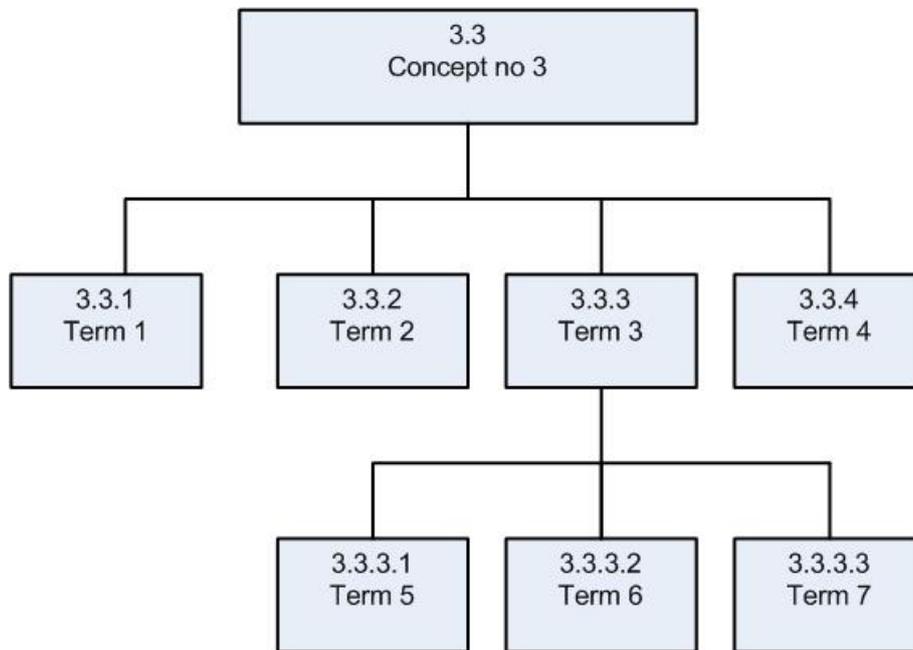
- **concept** means a unit of knowledge created by a unique combination of *characteristics*
- **term** means the verbal designation of a general concept in a specific domain or subject
- **designation** means a representation of a concept by a sign which denotes it
- **definition** means a representation of a concept by a descriptive statement which serves to differentiate it from related concepts.

2098
2099

The systematic order requires identification of distinguished concepts and further determining terms which relate to the concept and provide necessary characteristics. The

⁴ Adopted from ISO/IEC 10241-1:2011 Terminological entries in standards — Part 1: General requirements and examples of presentation

2100 concept can have its definition, but it is not always the case. The systematic order is
 2101 achieved by proper numbering in the hierarchy of terms (see Fig.1).



2102
 2103 **Fig. 1 Numbering of terms within the concept (example)**
 2104

2105 It is recommended⁵ to minimise the number of concepts to produce a clear picture of rela-
 2106 tionships inside one concept map and limit cross-relations between concepts.

2107 Although the systematic approach is used in ISO standards for terminology presentation for
 2108 many years (see, for example, ISO/IEC 9000, to name the most eminent one, in my opinion)
 2109 it has not been applied in SC27 documents yet. However, when one considers:

- 2110 – the complexity of the IT security evaluation domain which resulted in hundreds of
- 2111 terms, often used in a different context than usual dictionary meaning,
- 2112 – deep revision of 15408 & 18045 set of standards currently underway,
- 2113 – needs for opening the Common Criteria world for new users, new applications,
- 2114 new technologies, and new evaluation techniques, and simultaneously, legacy
- 2115 needs for preserving current applications (existing evaluation and certification
- 2116 schemes with their practices, skills and experience),
- 2117 – new regulatory/ legal frameworks, like European cybersecurity certification
- 2118 framework⁶,

⁵ ISO/IEC 704:2009, Principles and methods

⁶ <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505737096808&uri=CELEX:52017PC0477>

2119 a clear request for working out the terminology issue is emerging (if not now – when? If not
2120 us –who?).

2121 Therefore, by identifying concepts and re-arrange current presentation of terms in ISO/IEC
2122 15408 part 1 we could meet the challenges as described above and:

- 2123 – fulfil the ISO requirements for correct presentation of terms,
- 2124 – clarify terms and their definitions in the ICT security evaluation context, and in
2125 consequence
 - 2126 ○ identify and then remove from Clause 3 these terms which are not neces-
2127 sary to define,
 - 2128 ○ improve current definitions (e.g. shortening them or removing circular ref-
2129 erences among several definitions).

2130 **2 The concept approach introduction to ISO/IEC 15408-1**

2131 **2.1 General action plan (GAP) to get the objective**

2132 To achieve complete systematic order with regards to all terms finally included in Clause 3
2133 of ISO/IEC 15408-1 an action plan is proposed with the following prerequisites:

- 2134 1. Clause 3 of ISO/IEC CD 15408-1 contains all terms in alphabetical order; experts
2135 can comment on the content, and regular housekeeping work is being done;
- 2136 2. In parallel, ISO/IEC TR 22216 is used as a temporary incubator for developing
2137 the concept system and reordering the set of terms by assigning them to relevant
2138 concepts;
- 2139 3. The reconstruction will be divided into 2 major parts, ie.
 - 2140 a. the Pilot – developing only some, the most obvious concepts (see next
2141 Clause), assigning terms to these concepts, and leaving the rest of the
2142 terms untouched for the time being;
 - 2143 b. the Implementation – based on experience gained during the Pilot the rest
2144 of concept is being developed, accepted and rest of terms assigned accord-
2145 ingly.

2146 Thus, the action plan is formulated as follows:

- 2147 A. The limited reconstruction (the Pilot) is placed in the current draft of ISO/IEC
2148 22216 subject to the revision by experts,
- 2149 B. Depending on the results of revision separate session/workshop could be
2150 organised at the meeting in Norway (Autumn, 2018), possibly with the help of
2151 external expert(s),
- 2152 C. Upon the editing group approval proven/validated approach would be deployed
2153 on the whole set of terms,

- 2154 D. The full reconstruction (Implementation) will appear in next version of ISO/IEC
- 2155 TR 22216 issued after the meeting held in Norway, again subject to the revision
- 2156 by experts,
- 2157 E. Housekeeping on terms and their definition is being done in parallel, and its re-
- 2158 sults are mutually reflected in both documents, ISO/IEC 15408-1 Clause 3 and
- 2159 ISO/IEC TR 22216.
- 2160 F. Another round of review is possible before the project gets DIS stage;
- 2161 G. Upon successful implementation of the concept approach, the results would be
- 2162 moved to Clause 3 of ISO/IEC 15408-1 replacing alphabetically ordered set of
- 2163 terms and definitions.

2164 The plan is presented in Fig. 2.

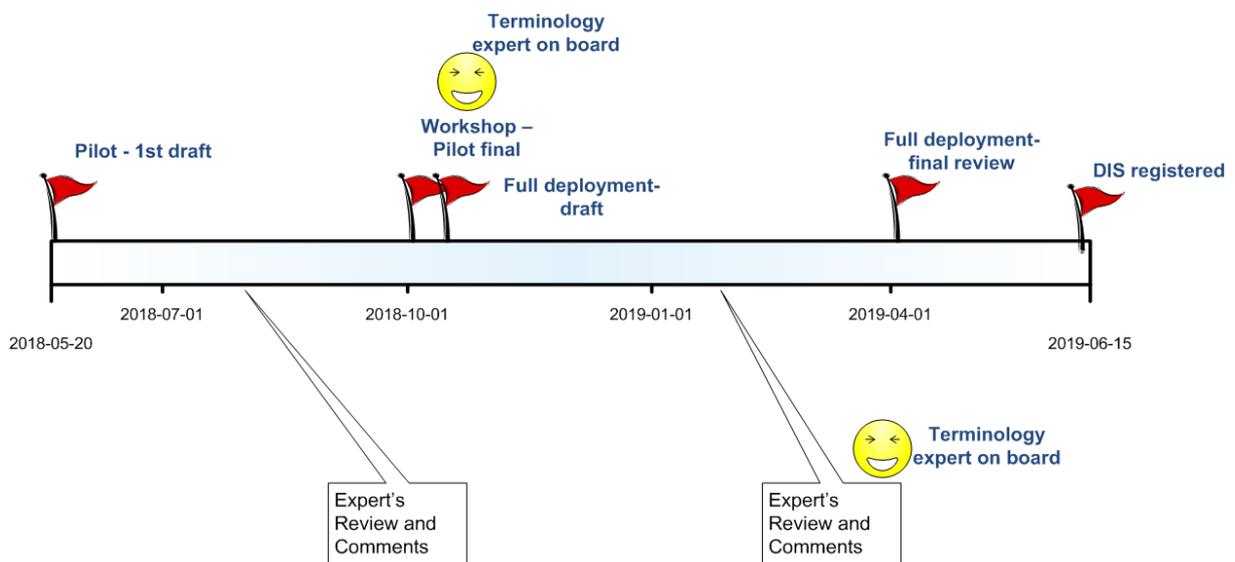


Fig. 2 The action plan timetable

2165
2166
2167

2168 **2.2 What would be the impact of the GAP on the project timetable?**

- 2169 – Minor, it does not touch the structure, not being an obstacle for progressing ISO/IEC
- 2170 15408-1 to next stages (should be done unless the project reaches DIS stage),
- 2171 – There is always a roll-back possibility, some not all results (e.g. at least housekeeping)
- 2172 could be implemented if the adventure would not reach its all objectives.

2173 **3 Identification of concepts**

2174 **3.1 General**

2175 As a starting point (pilot) of the concept development following 5 concepts have been iden-

2176 tified:

- 2177 1. Security model

- 2178 2. Target of Evaluation, TOE
- 2179 3. Assurance
- 2180 4. Evaluation techniques
- 2181 5. Taxonomy

2182 Relevant terms, currently included in ISO/IEC 1stCD 15408-1, have been assigned to con-
2183 cepts by analysing respective definitions. As a result, several maps of relationships between
2184 terms are presented in following subchapters. It is not claimed the maps for respective con-
2185 cepts are complete. All presented maps are subject to modification and improvements.

2186 Other terms have not been assigned yet. It is expected to provide relevant maps in the next
2187 step of the development process.

2188 Finally, there are terms recommended to remove (still subject to further consideration).

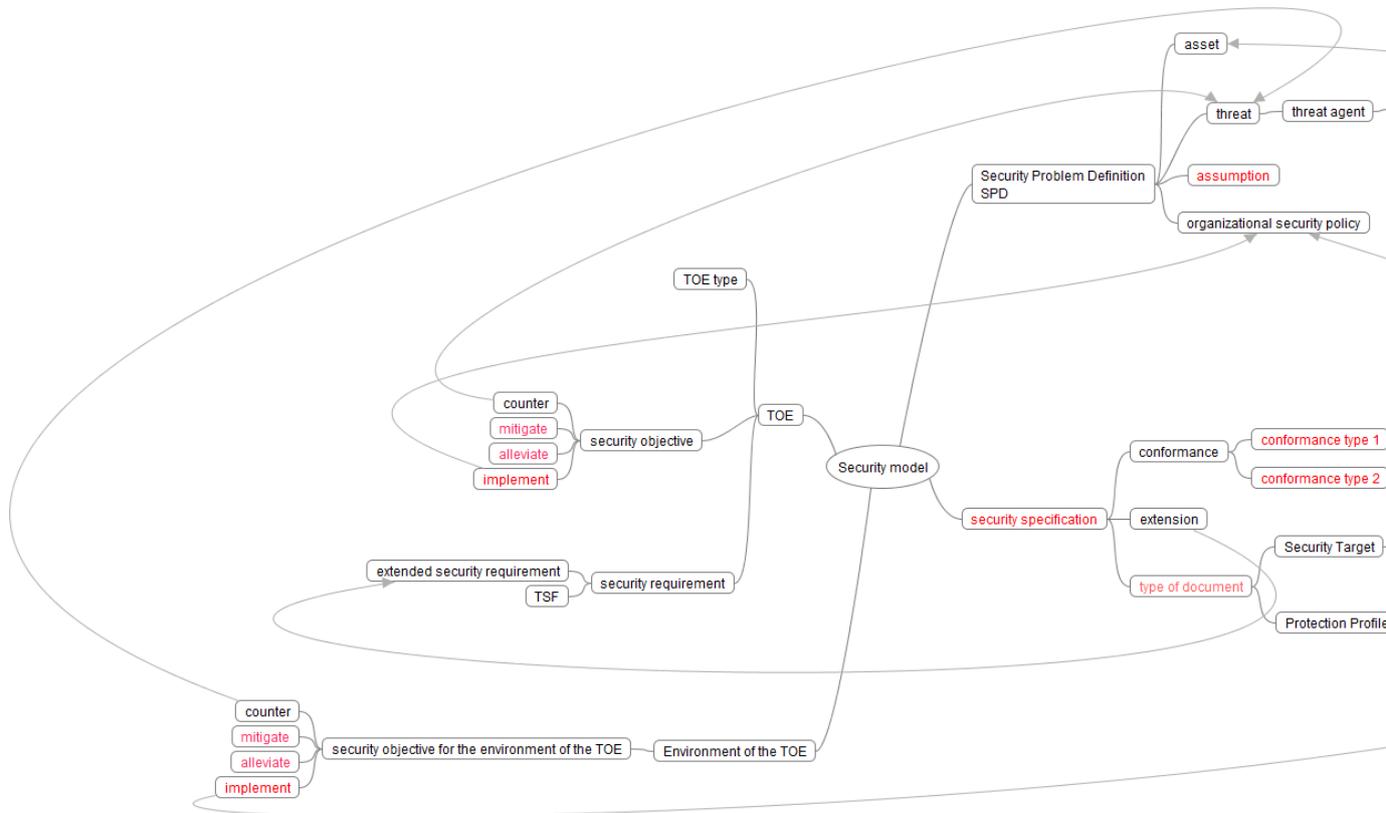
2189 The complete list of terms, their definitions and current status with regards to the concept
2190 assignments are presented in the table located at the end of this Annex.

2191 It is worth to note some maps contain not defined terms. It is not necessary the fault nor
2192 proof of incompleteness. The term is not to be defined if used in common, dictionary mean-
2193 ing however it could be indispensable for completeness of the concept map. Such terms are
2194 indicated in red font. Finally, if we have any doubt with assigning particular terms, it ap-
2195 pears in a yellow box.

2196

2197 3.2 Concepts

2198 3.2.1 Security Model



2199

2200

Fig. 3 Terms related to 'security model' concept

2201 3.2.2 Assurance

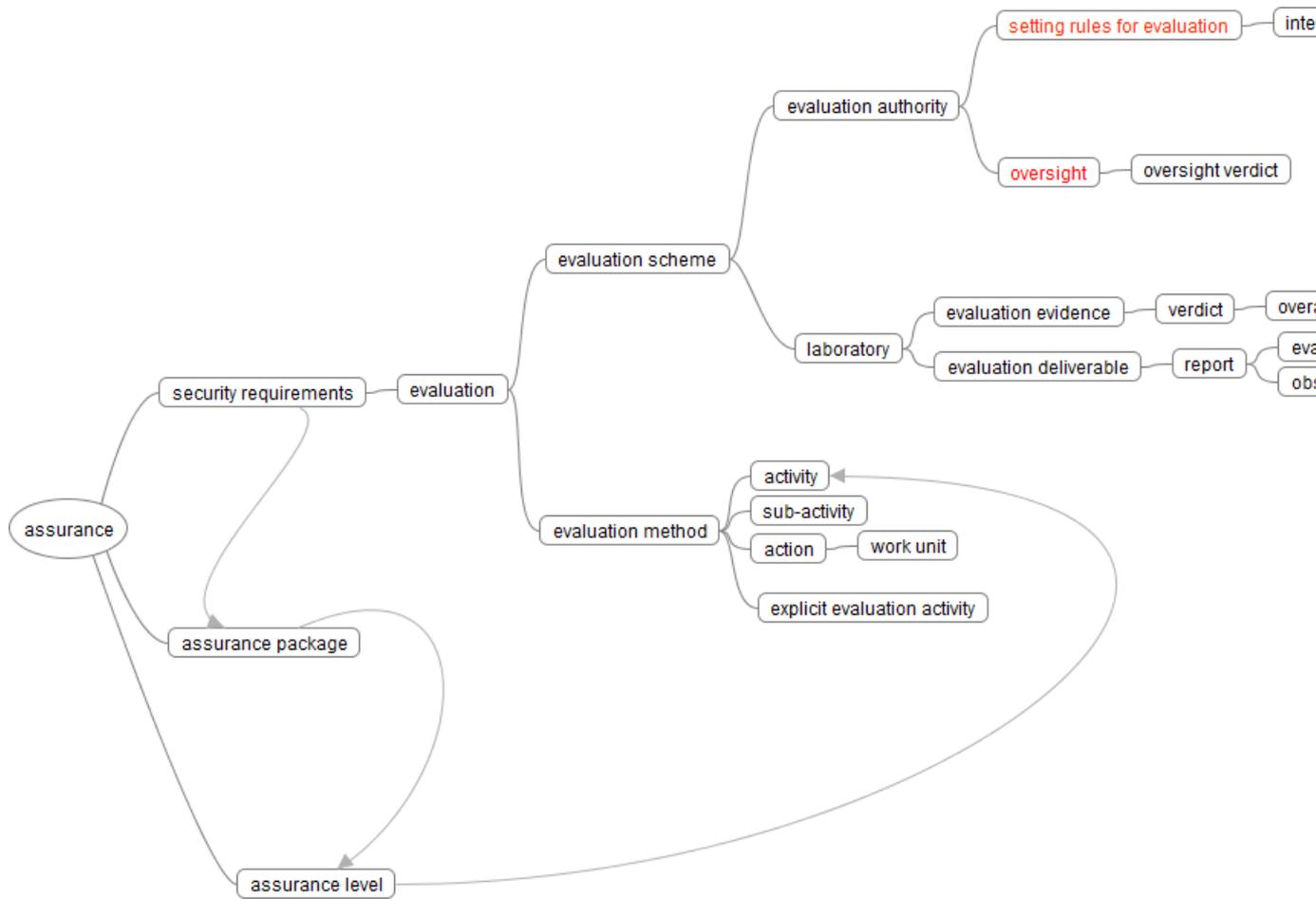
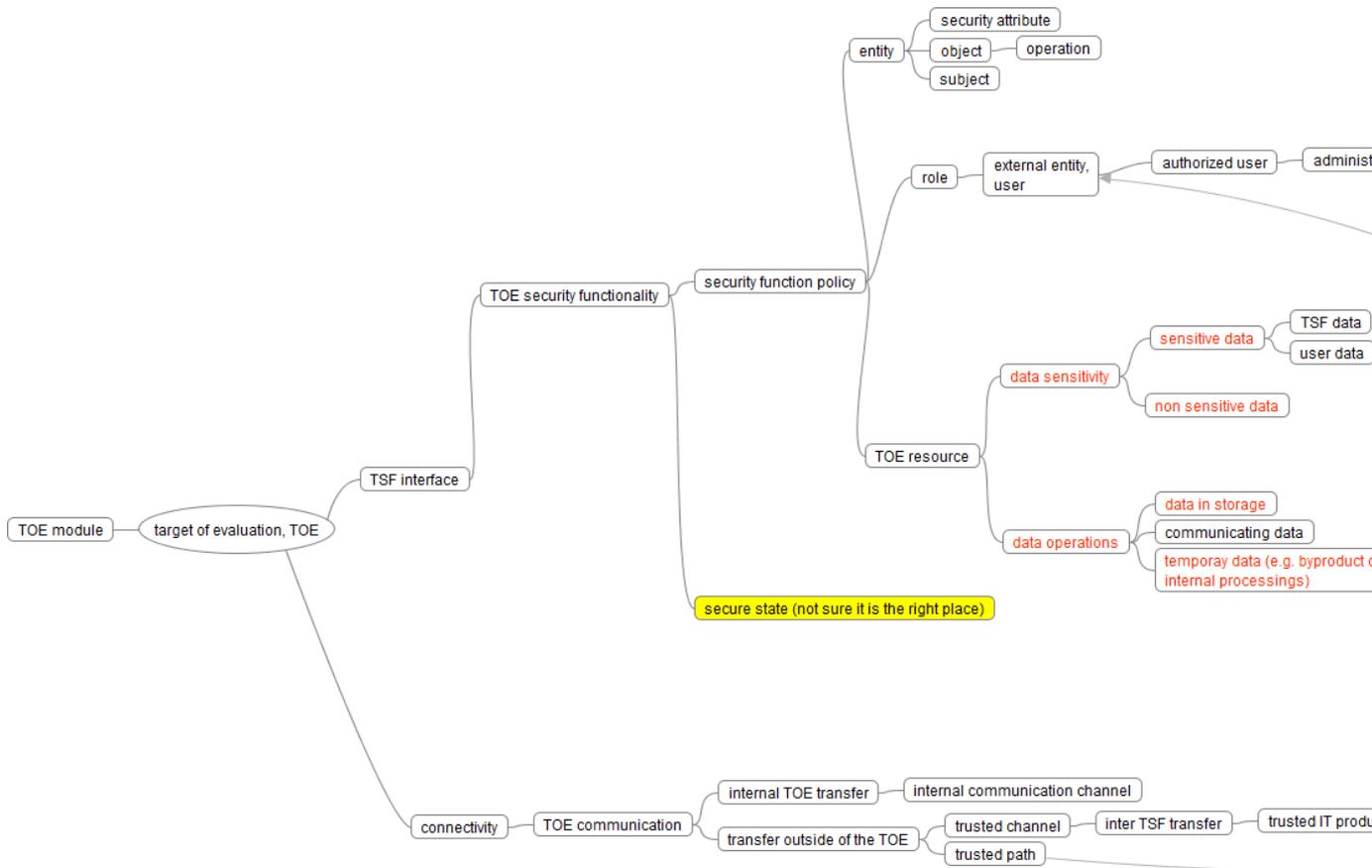


Fig. 1 Terms related to 'assurance' concept

2202
2203
2204

2205 **3.2.3 Target of Evaluation, TOE**



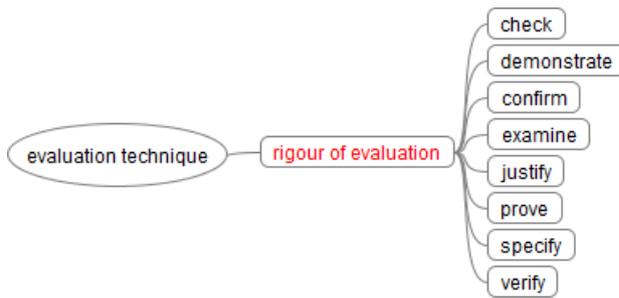
2206

2207

Fig. 5 Terms related to 'TOE' concept

2208

2209 **3.2.4 Evaluation techniques**

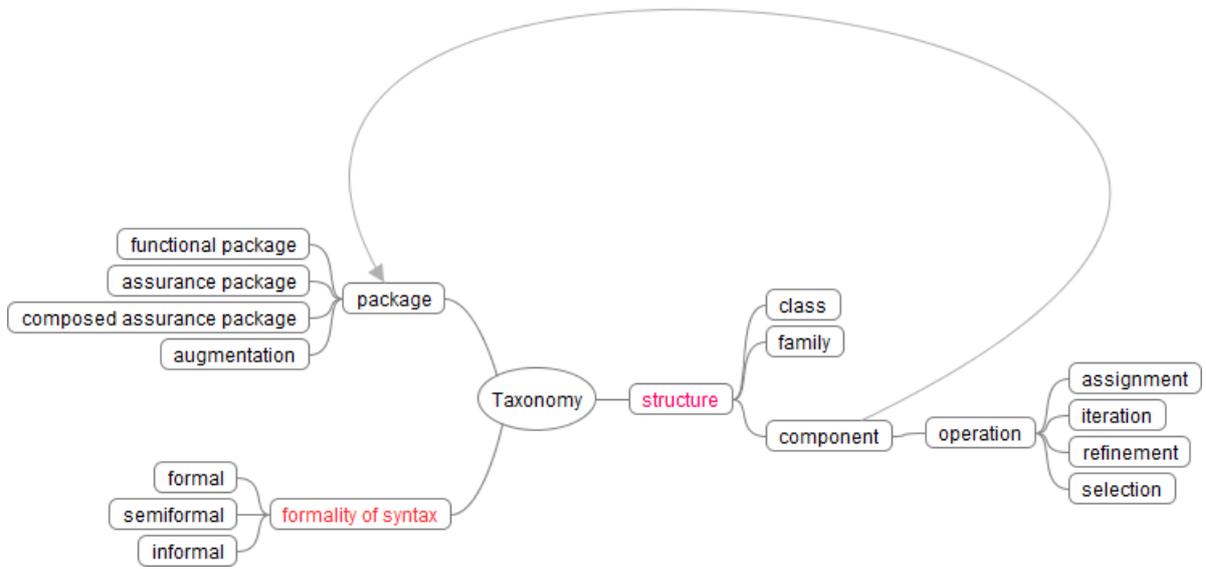


2210

2211

Fig. 6 Terms related to 'evaluation techniques' concept

2212 **3.2.5 Taxonomy**



2213

2214

Fig. 7 Terms related to 'taxonomy' concept

2215 **4 Assignment of Terms**

2216 All terms are presented in Table 1.

2217 **Table 1 List of terms - current content of ISO/IEC 1st CD 15408-1, Clause 3**

ID_no	Term	Current definition	Concept
3.1	acceptance criteria	criteria to be applied when performing the acceptance procedures (e.g. successful document review, or successful testing in the case of software, firmware or hardware)	not assigned yet
3.2	acceptance procedure	<p>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</p> <p>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.</p> <p>There are several types of acceptance situations some of which may overlap:</p> <ul style="list-style-type: none"> a) acceptance of an item into the configuration management system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE (“integration”); b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, quality control of the finished TOE); c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites; d) subsequent to the delivery of the TOE to the consumer; e) subsequent to the integration of the TOE. 	not assigned yet
3.3	action	<p>evaluator action element of ISO/IEC 15408-3</p> <p>NOTE to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.</p>	assurance
3.4	activity	application of an assurance class of ISO/IEC 15408-3	assurance

ID_no	Term	Current definition	Concept
3.5	administrator	entity that has a level of trust with respect to all policies implemented by the TSF Note 1 to entry: Not all PPs or STs assume the same level of trust for administrators. Typically, administrators 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 functionality of the TOE, others may be related to the operational environment.	TOE - role - subordinate
3.6	adverse action	action performed by a threat agent on an asset	security model
3.7	asset	entity that the owner of the TOE presumably places value upon	security model
3.8	assignment	specification of an identified parameter in a functional element component of a given functional or assurance component Note 1 to entry: Such functional element is also called a requirement.	taxonomy
3.9	assurance	grounds for confidence that a TOE meets the SFRs	assurance
3.10	assurance level	set of assurance requirements drawn from CC Part 3, representing the assurance activities necessary to determine the perceived threats to assets are sufficiently mitigated by the TOE	not assigned yet
3.11	assurance package	named set of security assurance requirements EXAMPLE "EAL 3".	taxonomy
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).	not assigned yet
3.13	augmentation	addition of one or more requirements to a package Note 1 to entry: in case of a functional package augmentation such augmentation is considered only in the context of one package, and is not considered in the context with other packages or PPs. Note 2 to entry: in case of an assurance package augmentation refers to one or more SAR.	taxonomy
3.14	authentication data	information used to verify the claimed identity of a user	not assigned yet

ID_no	Term	Current definition	Concept
3.15	authorized user	TOE user who may, in accordance with the SFRs, perform an operation	TOE - role - subordinate
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	not assigned yet
3.17	Base Protection Profile Base PP	Protection Profile used as a basis to build a Protection Profile Configuration	security model - TOE type
3.18	base TOE developer	entity developing the base TOE or sponsoring a base TOE evaluation	not assigned yet
3.19	base TOE evaluation authority	evaluation authority performing its tasks to evaluate the platform base TOE	not assigned yet
3.20	base TOE evaluator	entity performing the base TOE evaluation	not assigned yet
3.21	Base-TOE	Text	not assigned yet
3.22	check	<evaluation verb> generate a verdict by a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.	evaluation technique
3.23	class	<taxonomy>set of ISO/IEC 15408 families that share a common focus	taxonomy
3.24	coherent	logically ordered and having discernible meaning Note 1 to entry: For documentation, this term addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.	recommended to remove
3.25	compatible	<component> property of a component able to provide the services required by the other component, through the corresponding interfaces of each component, in consistent operational environments	not assigned yet
3.26	complete	property where all necessary parts of an entity have been provided Note 1 to entry: In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction.	recommended to remove
3.27	component	<taxonomy> smallest selectable set of elements on which requirements may be based	taxonomy
3.28	component TOE	successfully evaluated TOE that is part of another composed TOE	not assigned yet

ID_no	Term	Current definition	Concept taxonomy
3.29	composed assurance package, CAP	assurance package consisting of components drawn predominately from the ACO class, representing a point on the pre-defined scale for composition assurance	
3.30	composed TOE	TOE comprised solely of two or more components that have been successfully evaluated	not assigned yet
3.31	composite evaluation	evaluation of a composite TOE	not assigned yet
3.32	composite product	TOE comprised of two or more component TOEs, at least one of which has been successfully evaluated	not assigned yet
3.33	composite product evaluation authority	evaluation authority performing its tasks to evaluated composite product	not assigned yet
3.34	composite product evaluation sponsor	entity in charge of contracting the composite product evaluation	not assigned yet
3.35	composite product evaluator	entity performing the composite product evaluation	not assigned yet
3.36	composite product integrator	entity installing the dependent components on the base TOE	not assigned yet
3.37	composite TOE	TOE composed of a superposition of two layers	not assigned yet
3.38	configuration item	object managed by the CM 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].	not assigned yet

ID_no	Term	Current definition	Concept
3.39	configuration list	<p>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</p> <p>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.</p>	not assigned yet
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	not assigned yet
3.41	configuration management documentation CM documentation	all configuration management documentation including configuration management output, configuration management list (configuration list), configuration management system records, configuration management plan and configuration management usage documentation	not assigned yet
3.42	configuration management evidence	<p>everything that may be used to establish confidence in the correct operation of the CM system</p> <p>EXAMPLE configuration management output, rationales provided by the developer, observations, experiments or interviews made by the evaluator during a site visit</p>	not assigned yet

ID_no	Term	Current definition	Concept
3.43	configuration management output	<p>results, related to configuration management, produced or enforced by the configuration management system</p> <p>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.</p>	not assigned yet
3.44	configuration management plan	<p>description of how the configuration management system is used for the TOE</p> <p>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.</p>	not assigned yet
3.45	configuration management system	<p>set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles</p> <p>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.</p>	not assigned yet

ID_no	Term	Current definition	Concept
3.46	configuration management system record	output produced during the operation of the configuration management system documenting important configuration management activities Note 1 to entry: Examples of configuration management system records are configuration management item change control forms or configuration management item access approval forms.	not assigned yet
3.47	configuration management tool	manually operated or automated tool realising or supporting a configuration management system EXAMPLE Tools for the version management of the parts of the TOE.	not assigned yet
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	not assigned yet
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	evaluation technique
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.	TOE
3.51	counter, verb	act on or respond to a particular threat so that the threat is eradicated or mitigated	security model
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	not assigned yet
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.	not assigned yet
3.54	demonstrable conformance	relation between a ST and a PP, where the ST provides an equivalent or more restrictive solution which solves the generic security problem in the PP	security model - conformance
3.55	demonstrate	<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a “proof”	evaluation technique

ID_no	Term	Current definition	Concept taxonomy
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	not assigned yet
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).	not assigned yet
3.59	dependent TOE developer	entity developing the dependent component running on the base TOE	not assigned yet
3.60	describe	<evaluation verb> provide specific details of an entity	not assigned yet
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	evaluation technique
3.62	developer	organisation responsible for the development of the TOE	not assigned yet
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.	not assigned yet
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.	not assigned yet

ID_no	Term	Current definition	Concept
3.65	development tools	tools (including test software, if applicable) supporting the development and production of the TOE EXAMPLE For a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.	not assigned yet
3.66	direct rationale	type of Protection Profile or Security Target in which the threats and organisational security policies in the SPD are mapped directly to the SFRs and possibly security objectives for the operational environment Note 1 to entry: Direct rationale is simpler solution than mapping via a set of TOE security objectives.	security model - TOE type
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	not assigned yet
3.68	element	<taxonomy> most detailed level of definition of a security need	taxonomy
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	not assigned yet
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.	not assigned yet
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	TOE
3.72	evaluate	assessment of a PP, an ST or a TOE, against defined criteria	assurance
3.73	evaluation activity EA	activities 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.	assurance
3.74	evaluation assurance level EAL	set of assurance requirements defined in ISO/IEC 15408-3 and drawn from ISO/IEC 15408-3, representing a point on the ISO/IEC 15408 predefined assurance scale, that form an assurance package	assurance

ID_no	Term	Current definition	Concept
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	assurance
3.76	evaluation deliverable	any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities	assurance
3.77	evaluation evidence	item used as a factual basis for establishing the verdict of an evaluation activity	assurance
3.78	evaluation method	logical sequence of domain specific analysis steps to build knowledge and assurance of the TOE	assurance
3.79	evaluation scheme	administrative and regulatory framework under which ISO/IEC 15408 is applied by an evaluation authority within a specific community	assurance
3.80	evaluation technical report	report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority	assurance
3.81	evaluator	individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology Note 1 to entry: An example of evaluation standards is ISO/IEC 15408 (all parts) with the associated evaluation methodology given in ISO/IEC 18045 SOURCE: ISO/IEC 19896-1:2018	not assigned yet
3.82	exact conformance	hierarchical relationship between a PP and an ST where all the requirements in the ST are drawn only from the PP Note 1 to entry: an ST is allowed to claim exact conformance to one or more PPs and/or PP configurations.Note 2 to entry: PPs are not allowed to claim exact conformance to other PPs.	security model - conformance
3.83	examine	<evaluation verb> generate a verdict by analysis using evaluator expertise Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is analysed.	evaluation technique

ID_no	Term	Current definition	Concept
3.84	exhaustive	<p><evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan</p> <p>Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is 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.</p>	not assigned yet
3.85	explain	<p><evaluation verb> give argument accounting for the reason for taking a course of action</p> <p>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.</p>	not assigned yet
3.86	exploitable vulnerability	weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE	not assigned yet
3.87	extended security requirement	<p>security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408</p> <p>Note 1 to entry: An extended security requirement may be either an SAR or an SFR.</p> <p>Note 2 to entry: Extended security requirements are defined within extended component definitions.</p>	security model
3.88	Extended TOE	Text	not assigned yet
3.89	Extended TSF	Text	not assigned yet
3.90	external entity user	<p>human or IT entity possibly interacting with the TOE from outside of the TOE boundary</p> <p>Note 1 to entry: An external entity can also be referred to as a user.</p>	TOE - role - subordinate
3.91	family	<taxonomy> set of components that share a similar goal but differ in emphasis or rigour	taxonomy
3.92	formal	expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts	taxonomy
3.93	functional interface	<p>external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements</p> <p>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.</p>	not assigned yet

ID_no	Term	Current definition	Concept taxonomy
3.94	functional package	named set of security functional requirements that may be accompanied by an SPD and security objectives derived from that SPD	taxonomy
3.95	global assurance level	set of assurance requirements drawn from CC Part 3 that are to be applied to the entire TSF in a multi-assurance evaluation.	not assigned yet
3.96	guidance documentation	documentation that describes the delivery, preparation, operation, management and/or use of the TOE	not assigned yet
3.97	identity	representation uniquely identifying an entity within the context of the TOE EXAMPLE An example of such a representation is a string. Note 1 to entry: entities can be diverse such as a user, process, or disk. For a human user, the representation could be the full or abbreviated name or a unique pseudonym. Note 2 to entry: An entity can have more than one identity.	not assigned yet
3.98	implementation representation	least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement Note 1 to entry: Source code that is then compiled or a hardware drawing that is used to build the actual hardware are examples of parts of an implementation representation.	not assigned yet
3.99	informal	expressed in natural language	taxonomy
3.100	installation	procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as “generation” throughout ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.	not assigned yet
3.101	inter TSF transfer	communicating data between the TOE and the security functionality of other trusted IT products	TOE
3.102	interaction	general communication-based activity between entities	not assigned yet

ID_no	Term	Current definition	Concept
3.103	interface	means of communication with an entity	not assigned yet
3.104	internal communication channel	communication channel between separated parts of the TOE	TOE
3.105	internal TOE transfer	communicating data between separated parts of the TOE	TOE
3.106	internally consistent	no apparent contradictions exist between any aspects of an entity Note 1 to entry: In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.	recommended to remove
3.107	interpretation	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or scheme requirement	assurance
3.108	iteration	use of the same component to express two or more distinct requirements	taxonomy
3.109	justify	<evaluation verb> provide a rationale providing sufficient reason Note 1 to entry: The term 'justify' is more rigorous than a 'demonstrate'. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical analysis leading to a conclusion.	not assigned yet
3.110	laboratory	organization with a management system providing evaluation and or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF). [SOURCE ISO/IEC DIS 19896-1 ,3.7]	assurance
3.111	layering	design technique where separate groups of modules (the layers) are hierarchically organised to have separate responsibilities such that one layer depends only on layers below it in the hierarchy for services, and provides its services only to the layers above it Note 1 to entry: Strict layering adds the constraint that each layer receives services only from the layer immediately beneath it, and provides services only to the layer immediately above it.	not assigned yet

ID_no	Term	Current definition	Concept
3.112	life cycle model	description of the stages and their relations to each other that are used in the management of the life-cycle of a certain object, how the sequence of stages looks like and which high level characteristics the stages have Note 1 to entry: See also Figure 1. [SOURCE: ISO/IEC/IEEE 24765:2010 3.1587 modified, note 1 to entry added]	not assigned yet
3.113	life-cycle definition	definition of the life-cycle model	not assigned yet
3.114	methodology	system of principles, procedures and processes applied to IT security evaluations	not assigned yet
3.115	moduleTOE Module	small architectural unit that can be characterized in terms of the properties discussed in TSF internals (ADV_INT)	TOE
3.116	monitoring attacks	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	not assigned yet
3.117	non-bypassability	<(of the TSF) security architecture property whereby all SFR-related actions are mediated by the TSF	not assigned yet
3.118	object	entity in the TOE, that contains or receives information, and upon which subjects perform operations	TOE
3.119	observation report	report written by the evaluator requesting a clarification or identifying a problem during the evaluation	assurance
3.120	operation	<(on an ISO/IEC 15408 component) modification or repetition of a component by assignment, iteration, refinement, or selection	taxonomy
3.121	operation	<(on an object) specific type of action performed by a subject on an object	TOE
3.122	operation	usage phase of the TOE including “normal usage”, administration and maintenance of the TOE after delivery and preparation	not assigned yet
3.123	operational environment	environment in which the TOE is operated	recommended to remove
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.	security model

ID_no	Term	Current definition	Concept
3.125	overall verdict	pass or fail 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”.	assurance
3.126	oversight verdict	statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities	assurance
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	taxonomy
3.128	policy	set of rules, procedures, and guidelines	recommended to remove
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.	not assigned yet
3.130	preparation	activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation which may include such things as booting, initialisation, start-up and progressing the TOE to a state ready for operation	not assigned yet
3.131	production	production life-cycle phase which follows the development phase and 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.	not assigned yet
3.132	Protection Profile configuration PP-Configuration	Protection Profile composed of Base Protection Profile(s) and Protection Profile module(s)	security model
3.133	Protection Profile PP	implementation-independent statement of security needs for a TOE type	security model - 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	security model - TOE type

ID_no	Term	Current definition	Concept
3.135	prove	<evaluation verb> show correspondence by formal analysis in its mathematical sense Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.	evaluation technique
3.136	record	<evaluation verb> retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time	assurance
3.137	refinement	addition of details to a component	taxonomy
3.138	report	<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report	assurance
3.139	residual vulnerability	weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE	not assigned yet
3.140	role	predefined set of rules establishing the allowed interactions between a user and the TOE	TOE
3.141	secret	information that shall be known only to authorised users and/or the TSF in order to enforce a specific SFP	TOE
3.142	secure state	state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs	TOE
3.143	security attribute	property of subjects, users, objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs Note 1 to entry: Users can include external IT products.	TOE
3.144	security domain	environment provided by the TSF for the use by untrusted entities in such a way that the environment is isolated and protected from other environments	not assigned yet
3.145	security function policy	set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs	TOE
3.146	security objective	statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions	security model

ID_no	Term	Current definition	Concept
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.	security model
3.148	security requirement	requirement, stated in a standardised 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.	security model
3.149	Security Target ST	implementation-dependent statement of security needs for a specific identified TOE	security model - TOE type
3.150	selection	specification of one or more items from a list in a component	taxonomy
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 shall be included in a conformant ST if a selection choice identified in the PP indicates that it has an associated selection-based SFR	security model
3.152	semiformal	expressed in a restricted syntax language with defined semantics	taxonomy
3.153	SPD-element	threat, organizational security policy, or assumption	not assigned yet
3.154	specify	<evaluation verb> provide specific details about an entity in a rigorous and precise manner	evaluation technique
3.155	ST-Configuration	Text	not assigned yet
3.156	ST-Module	Text	not assigned yet

ID_no	Term	Current definition	Concept
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.	Concept security model - conformance
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	assurance
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	not assigned yet
3.160	subject	entity in the TOE that performs operations on objects	TOE
3.161	target of evaluation TOE	set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation	TOE
3.162	threat agent	entity that can exercise adverse actions on assets protected by the TOE	security model
3.163	time to exposure	Text	not assigned yet
3.164	TOE resource	anything useable or consumable in the TOE	TOE
3.165	TOE security functionality TSF	combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs	TOE
3.166	TOE type	set of TOEs that have common characteristics Note 1 to entry: The TOE type may be more explicitly defined in a PP. Note 1 to entry: The TOE type may be more explicitly defined in a PP.	security model
3.167	trace	perform an informal correspondence analysis between two entities with only a minimal level of rigour	recommended to remove
3.168	trace	<evaluation verb> simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second	not assigned yet
3.169	transfer outside of the TOE	TSF mediated communication of data to entities not under the control of the TSF	TOE

ID_no	Term	Current definition	Concept
3.170	translation	describes the process of describing security requirements in a standardised language. Note 1 to entry: Use of the term translation in this context is not literal and does not imply that every SFR expressed in standardised language can also be translated back to the security objectives. Note 1 to entry: Use of the term translation in this context is not literal and does not imply that every SFR expressed in standardized language can also be translated back to the Security Objectives.	not assigned yet
3.171	trusted channel	means by which a TSF and another trusted IT product can communicate with necessary confidence Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the confidentiality preservation and protection against replay.	TOE
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.	TOE
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.	TOE
3.174	TSF data	data for the operation of the TOE upon which the enforcement of the SFR relies	TOE
3.175	TSF interface TSFI	means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF,	TOE
3.176	TSF self-protection	security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities	not assigned yet

ID_no	Term	Current definition	Concept
3.177	user data	data that 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.	TOE
3.178	verdict	pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 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.	assurance
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.	evaluation technique
3.180	vulnerability	weakness in the TOE that can be used to violate the SFRs in some environment	not assigned yet
3.181	window of opportunity	period of time that an attacker has access to the TOE	not assigned yet
3.182	work unit	most granular level of evaluation work	assurance
			not assigned yet

2218

2219

Table 2 List of terms - current content of ISO/IEC 2WD 15408-1, Clause 3.8 (former place: ISO/IEC 18045)

ID	Term	Current definition	Concept
3.1	action	evaluator action element of ISO/IEC 15408-3 NOTE These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.	evaluation
3.2	activity	application of an assurance class of ISO/IEC 15408-3	evaluation
3.1.5	attack potential	a measure of the effort to be expended in attacking a TOE expressed in terms of an attacker's expertise, resources, and motivation	not assigned yet

3.1.X	time to exposure	something to do with attack potential	not assigned yet
3.1.x	window of opportunity	the period in which an attacker has access to the TOE	not assigned yet
3.3	check	<evaluation verb> generate a verdict by a simple comparison NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.	evaluation technique
3.1.14	confirm	<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency Note 1 to entry: This term is only applied to evaluator actions. Note 2 to entry: The level of rigour required depends on the nature of the subject matter	evaluation technique
3.1.19	demonstrate	<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a “proof.”	evaluation technique
3.1.21	describe	<evaluation verb> provide specific details of an entity	not assigned yet
3.1.22	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 analysis has already been performed which needs to be reviewed	evaluation technique
3.1.25	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.	not assigned yet
3.8.X	evaluation activity, EA	an explicitly defined work unit that alone or in combination with other Evaluation Activities replaces or supplements (adds to) an existing ISO/IEC 18045 work unit	evaluation

3.4	evaluation deliverable	any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities	evaluation
3.5	evaluation evidence	tangible evaluation deliverable	evaluation
3.6	evaluation technical report	the report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority	evaluation
3.7	examine	<evaluation verb> generate a verdict by analysis using evaluator expertise NOTE The statement that uses this verb identifies what is analysed and the properties for which it is analysed.	evaluation technique
3.1.30	exhaustive	<evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is 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.	not assigned yet
3.1.31	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.	not assigned yet
new	explicit evaluation activity	set of evaluator actions separately defined as an implementation of one or more of the generic Activities, Sub-activities, Actions and Work Units in ISO/IEC 18045, and applied in certain well-defined situations such as for a particular TOE type, or application domain Note 1 to entry: An explicit evaluation activity is defined at a more specific level of detail than its generic antecedent in ISO/IEC 18045, and meets the requirements set out in ISO/IEC 15408-4.	evaluation

3.8	interpretation	clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or scheme requirement	evaluation
3.8.X	justify	<evaluation verb> provide a rationale providing sufficient reason	evaluation technique
3.9	methodology	the system of principles, procedures and processes applied to IT security evaluations	not assigned yet
3.10	observation report	report written by the evaluator requesting clarification or identifying a problem during the evaluation	evaluation
3.11	overall verdict	pass or fail statement issued by an evaluator with respect to the result of an evaluation	evaluation
3.12	oversight verdict	a statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities	evaluation
3.1.53	prove	<evaluation verb> show correspondence by formal analysis in its mathematical sense Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.	evaluation technique
3.13	record	<evaluation verb> retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time	evaluation
3.14	report	<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report	evaluation
3.15	scheme	set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and methodology required to conduct IT security evaluations	evaluation

3.1.66	specify	<evaluation verb> provide specific details about an entity in a rigorous and precise manner	evaluation technique
3.16	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	evaluation
3.17	trace	<evaluation verb> simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second	not assigned yet
3.18	verdict	pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class NOTE Also see overall verdict.	evaluation
	verify	<evaluation verb> rigorously review in detail with an independent determination of sufficiency	evaluation technique
3.19	work unit	most granular level of evaluation work	evaluation

2220

2221

Bibliography

- 2222 This bibliography contains references to further material and standards that the reader of this document may find useful. For undated
2223 references the reader is recommended to refer to the latest edition of the referenced document.
- 2224 [1] JIL - The Application of CC to Integrated Circuits - Version 3.0 - February 2009
- 2225 [2] JIL - Application of Attack Potential to Smartcards - Version 2.9 - January 2013
- 2226 [3] JIL - CEM Refinements for POI Evaluation - Version 1.0 (for trial use) - 27th May 2011
- 2227 [4] JIL - Application of Attack Potential to POIs - Version 1.0 (for trial use) - 9th June 2011
- 2228 [5] JIL - Application of Attack Potential to Hardware Devices with Security Boxes - Version 2.0 (for trial use) - December 2015
- 2229 [6] JIL - Security Architecture requirements (ADV_ARC) - for smart cards and similar devices - Version 2.0 - January 2012
- 2230 [7] JIL - Minimum Site Security Requirements - Version 2.1 (for trial use) - December 2017
- 2231 [8] Supporting Document - Mandatory Technical Document - Full Drive Encryption: Authorization Acquisition - January 2015 - Version 1.0
2232 - CCDB - 2015-01-003
- 2233 [9] Supporting Document - Mandatory Technical Document - Full Drive Encryption: Encryption Engine - January 2015 - Version 1.0 -
2234 CCDB-2015-01-004
- 2235 [10] Supporting Document - Mandatory Technical Document - Evaluation Activities for Stateful Traffic Filter Firewalls cPP - February 2015
2236 - Version 1.0 - CCDB-2015-01-002
- 2237 [11] Supporting Document - Mandatory Technical Document - Evaluation Activities for Network Device cPP - February 2015 - Version 1.0 -
2238 CCDB-2015-01-001
- 2239 [12] collaborative Protection Profile for Network Devices - Version 1.0 - 27-Feb-2015
- 2240 [13] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition - Version 1.0 - January 26, 2015
- 2241 [14] collaborative Protection Profile for Full Drive Encryption - Encryption Engine - Version 1.0 - January 26, 2015

- 2242 [15] collaborative Protection Profile for Stateful Traffic Filter Firewalls - Version 1.0 - 27-Feb-2015
- 2243 [16] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1
- 2244 Revision 5 (CCMB-2017-04-001)
- 2245 [17] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, April 2017, Version 3.1
- 2246 Revision 5 (CCMB-2017-04-002)
- 2247 [18] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, April 2017, Version 3.1
- 2248 Revision 5 (CCMB-2017-04-003)
- 2249 [19] Common Methodology for Information Technology Security Evaluation. Evaluation methodology, April 2017, Version 3.1 Revision 5
- 2250 (CCMB-2017-04-004)
- 2251 [20] CC and CEM addenda. Selection-based SFRs, Optional SFRs, May 2017, Version 0.5 (CCDB-2017-05-XXX)
- 2252
- 2253 Bibliography to be updated
- 2254 Expert contributions are requested
- 2255