



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 5th WD 22216 — Information technology — Security techniques — Evaluation Criteria for IT security — Introductory guidance on evaluation for IT security

SOURCE: Project editor

DATE: 2019-08-19

PROJECT: 22216

STATUS: In accordance with WG recommendation 12 and 13 (contained in SC 27 N19523) of 58th SC 27/WG 3 meeting held in Tel-Aviv, Israel, April 1st – 5th 2019, this document is being circulated to experts and liaison organizations for study and comment closing by **2019-09-27** (due date is extended because of late submission of WD).

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: 2019-09-27

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

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

NO. OF PAGES: 1 + 40

1 **ISO/IEC JTC 1/SC 27/WG 3 N19504**

2 **Date: 2019-07-12**

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
39

© 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. The details of the definition can be found in CD3 of ISO/IEC 15408-1, ISO/IEC 15408-3 and ISO/IEC 18405.

These conventions will be removed in the final document.

40	Contents	
41	1 Scope.....	1
42	2 Normative references	1
43	3 Terms and definitions.....	2
44	3.1 Terms	2
45	3.2 Abbreviations.....	2
46	4 Overview.....	2
47	4.1 Structure of this guide.....	2
48	4.2 Impacts of the revision on the structure and partition of the documents.....	2
49	4.3 Using this guide for transitional information.....	2
50	4.4 Using the standard for specific needs.....	2
51	5 Major new concepts introduced in the standard.....	3
52	5.1 Approaches to security evaluation	3
53	5.1.1 The specification-based approach.....	4
54	5.1.2 The attack-based approach	5
55	5.2 Modularity	7
56	5.2.1 Composition mechanisms.....	7
57	5.2.2 Packages.....	9
58	5.2.3 Modular Protection Profiles.....	10
59	5.2.4 Multi-assurance evaluations.....	11
60	5.3 Consistent Standard's Language.....	16
61	5.4 Differentiation of ISO/IEC 15408: Evaluation Methods	16
62	6 Applying the standard to specific needs	17
63	6.1 Refining and deriving requirements.....	17
64	6.1.1 Refinements and Application Notes.....	17
65	6.1.2 Extended requirements.....	17
66	6.2 Refining and deriving evaluation methods.....	17
67	6.2.1 Attack-based approach.....	17
68	6.2.2 Specification-based approach.....	17
69	6.3 In practice: Supporting documents	17
70	7 Mapping of evolutions between ISO/IEC 15408 and ISO/IEC 18045 and the new revision.....	17
71	7.1 Categorization of study periods and other inputs	18
72	7.2 Summary	19
73	7.3 ISO/IEC 15408-1	20
74	7.4 ISO/IEC 15408-2	24
75	7.5 ISO/IEC 15408-3	25
76	7.6 ISO/IEC 15408-4.....	26
77	7.7 ISO/IEC 15408-5.....	28
78	7.8 ISO/IEC 18045.....	28
79	A.1 Vulnerability Assessment.....	30
80	A.2 Clarify & Streamline Evidence Requirements.....	31
81	A.3 Consistent Standard Metrics	31
82	A.4 Better use of development models and process.....	32
83	A.4.1 Incremental development.....	32
84	A.4.2 Other topics to be discussed.....	32
85	A.5 Reposition CEM.....	32
86	A.6 Review Tools and Techniques.....	32
87	A.7 New requirements.....	32

89 **Foreword**

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

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

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

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

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

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

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

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

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

118 Introduction

119 The current version of this document proposes a new structure for the Transition Guide aimed at users of the
120 standard. Sections 4 and 6 have been newly added and their content will be provided in the next draft stage. Ex-
121 perts are invited to provide feedback on the document's structure

122 The introduction will be updated to include information about the *Goal of the revision of the ISO/IEC 15408 and*
123 *ISO/IEC 18045 documents.*

124

125 This Technical Report provides guidance and support to those responsible for implementing the Fourth
126 edition of the ISO/IEC 15408 and ISO/IEC 18045 standards. This edition of the ISO/IEC 15408 and
127 ISO/IEC 18045 standards includes substantial changes from the third edition.

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

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

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

137 After publication of the standard, this Technical Report will provide guidance and support to users of
138 the Fourth edition of the ISO/IEC 15408 and ISO/IEC 18045 standards. The audience for this document
139 include:

- 140 — Security assurance consumers;
- 141 — IT product developers and those authoring Security Targets;
- 142 — Technical community subject matter experts (SMEs) developing Packages, Protection Profiles,
143 evaluation methodologies, and other supportive documents;
- 144 — Evaluators;
- 145 — Evaluation schemes, and validators;
- 146 — Consultants supporting ISO/IEC 15408 and 18045 work, including developers of supportive
147 tools;
- 148 — Others, including those involved with mutual recognition arrangements and academia.

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

151 IT Security techniques — Introductory guidance on evaluation for 152 IT security

153 1 Scope

154 The scope statement is, for now, the statement defined in the New Work Item Proposal (N16885) for this docu-
155 ment. This section will be updated in the next draft stage.

156 This document will:

- 157 — Follow and track the revision of ISO/IEC 15048 and ISO/IEC 18045;
- 158 — Map the evolutions between the initial version and the revised version;
- 159 — Cross reference and consolidate inputs from study periods and subsequent revision
160 contributions for ISO/IEC 15408/18045 and it will provide a rationale for their inclusion or not
161 in the revised standard;
- 162 — Introduce the break down between ISO/IEC 15408 and ISO/IEC 18045 and new parts of the
163 standard;
- 164 — Propose an evolution path and guidance on how to move from ISO/IEC 15408:2009 and ISO/IEC
165 18045:2008 to the revised new versions.

166 2 Normative references

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

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

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

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

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

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

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

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

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

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

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

190 **3 Terms and definitions**

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

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

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

196 **3.1 Terms**

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

198 **3.2 Abbreviations**

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

200 **4 Overview**

201 Section 4 has been newly added to the document. Experts are invited to provide feedback on its structure and to
202 contribute to the content.

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

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

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

211 **4.1 Structure of this guide**

212 **4.2 Impacts of the revision on the structure and partition of the documents**

213 **4.3 Using this guide for transitional information**

- 214 Guidance for consumers (risk owners)
- 215 Guidance for developers
- 216 Guidance for evaluators

217 **4.4 Using the standard for specific needs**

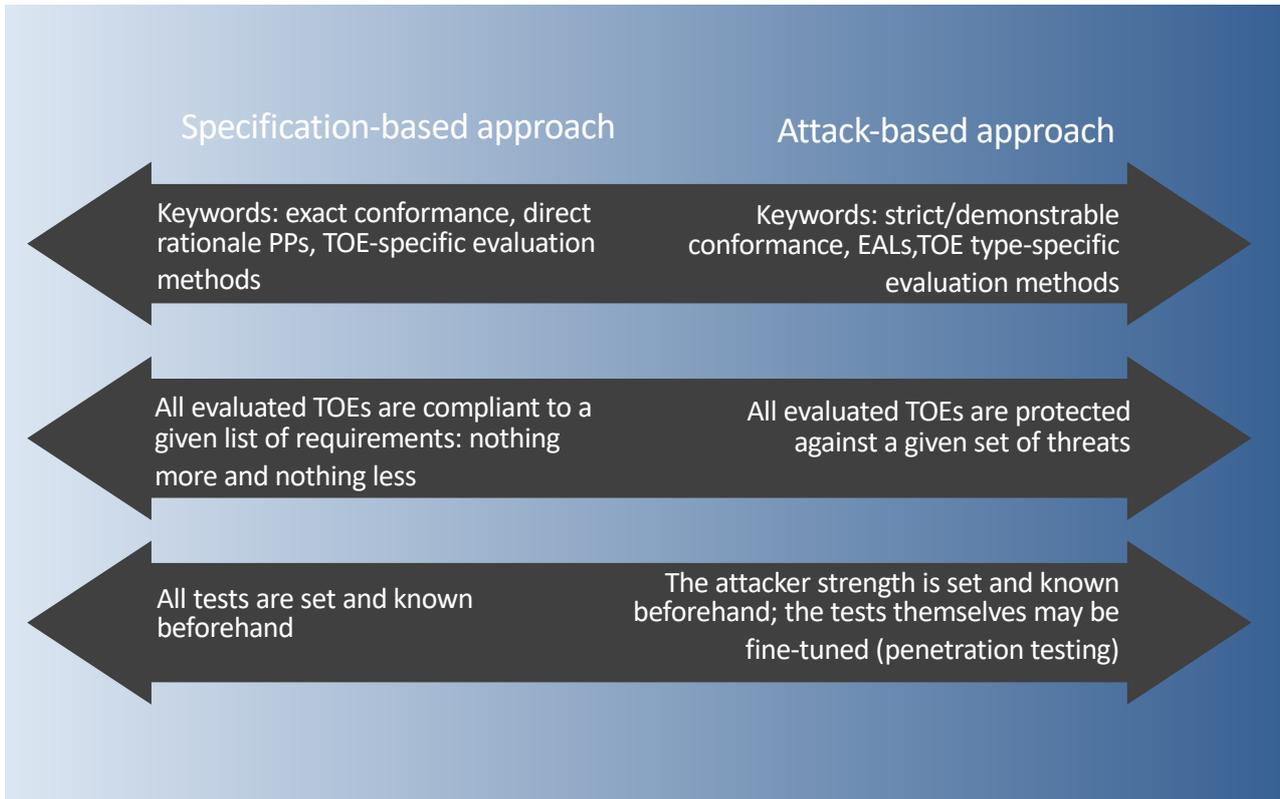
- 218 Adapting security components
- 219 Adapting evaluation methods

220

221 5 Major new concepts introduced in the standard

222 5.1 Approaches to security evaluation

223 The Fourth revision of the standard now supports two different approaches to evaluation, as shown in
 224 **Erreur ! Source du renvoi introuvable.** hereafter:



225 **Figure 5-1 — Specification-based and attack-based approaches**

226 The main differences between them are as follows:

- 227 • A new approach, which is called hereafter the “specification-based approach”, consists in defin-
 228 ing, at the PP level, the requirements, and the corresponding evaluation activities. This ap-
 229 proach:
 230
 - 231 – uses exact conformance to Protection Profiles;
 - 232 – does not use EALs;
 - 233 – may use Direct Rationale Protection Profiles and Security Targets.

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

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

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

255

256 5.1.1 The specification-based approach

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

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

262 This approach is intended to define minutely, at the PP level, the requirements to be met and the corre-
 263 sponding evaluation activities. This approach relies on a requirement-setting body to define the de-
 264 tailed Evaluation Activities and clear pass/fail criteria ahead of actual evaluations, which allows to
 265 achieve a high degree of consistency in the application of the assurance requirements.

266 5.1.1.1 Exact Conformance

267 The “specification-based” approach uses exact conformance PPs, which ensures that the conformant ST
 268 does not change or even add anything to the PP’s requirements. This concept is intended to support
 269 procurement processes, since it ensures that products will not claim additional features that are not
 270 relevant to the interests of the PP owner. The approach also aims at making it easier for potential
 271 customers to compare products and ensuring that the assurance consumers can see the details of the
 272 Evaluation Activities that have been successfully carried out

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

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

281

282 5.1.1.2 Edition of Protection Profiles and Security Targets

283 The “specification-based” approach may use standard or Direct Rationale PPs and STs. Direct Rationale
284 PPs and STs do not use security objectives for the TOE; they include instead a direct mapping from
285 threats to SFRs underpinned by a rationale on the mapping appropriateness.

286 Direct Rationale PPs and STs were previously called “low assurance” PPs and STs because they were
287 only allowed for EAL1 evaluations. These simplified PPs and STs are appropriate for the “specification-
288 based” approach, which does not use EALs.

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

- 290 • Less emphasis on the analysis of the security problem, which has a limited impact on the evalua-
291 tions since there is no need to perform TOE-specific vulnerability analysis;
- 292 • Maximizing the use of selection-based SFRs, and minimizing the use of open-ended assign-
293 ments;
- 294 EXAMPLE Identification of required versions of protocols and cryptographic algorithms in SFRs.
- 295 • Making extensive use of extended SFRs to specify the expected characteristics of the TOE;
- 296 • Making extensive use of application notes to describe the intended technology-specific adapta-
297 tion of SFRs;

298 Defining Evaluation Activities using ISO/IEC 15408-4, i.e. derived from the SARs in ISO/IEC 15408-3
299 and the evaluator actions in ISO/IEC 18045 to specifically address the details of the known TOE context
300 and the individual SFRs.

301

302 5.1.1.3 Evaluation methodology – ISO/IEC 15408-4

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

- 308 — Reproducibility, repeatability, and availability of tests are ensured by the fact that they are
309 completely defined in the PP or its supporting documents, the specification of which requires a
310 substantial involvement of domain experts;
- 311 — A given product type can be evaluated following this approach *only if* a PP is already defined;
- 312 — Evolutions in the state-of-the-art can be considered by updating the PP or the supporting
313 documents describing the requirements and the evaluation methodology.

314 5.1.2 The attack-based approach

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

316 This approach is based on evaluations carried out in situations where the implemented security
317 functionality may vary, e.g. according to technology choices or IP constraints, provided they enforce the
318 protection of the assets as expected. Such evaluations may be carried out without reference to a PP or
319 may be based on PPs that do not define the details of their intended TOE type or deployment context.
320 This maximizes the number of different realizations of the requirements that may be accepted as
321 conformant. The pre-defined packages of security assurance requirements and generic evaluator
322 actions, given in ISO/IEC 18045, are interpreted for each TOE type and specialized to the characteristics
323 of each actual TOE to confirm the assurance level. This assurance is derived from a sound/well-defined
324 hierarchy of assurance requirements and evaluation work units by using TOE-related evidence, which

325 allows the evaluator to specialize the generic evaluation work units and thereby to define the most
326 suitable set of tests for this specific product.

327 This approach is commonly deployed where there is an advantage in having flexibility in the application
328 of the assurance requirements.

329

330 5.1.2.1 Conformance

331 The “attack-based” approach uses demonstrable or strict conformance, which results in the possibility
332 to add SFRs and SARs to an individual ST (such additions may be organized in a package). However, the
333 approach does not forbid the use of the exact conformance concept whenever appropriate.

334

335 5.1.2.2 Edition of Protection Profiles and Security Targets

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

340 • Allows customization and adaptation of SPDs, objectives, and SFRs at the ST stage; this differen-
341 tiation may be of benefit to innovation by allowing vendors to complete their own require-
342 ments, as opposed to unified PPs;

343 EXAMPLE Open-ended assignments in PPs’ SFRs allow to make the most suitable instantiations
344 within the STs.

345 • Implies a limited use of extended SFRs, but does not prevent it;

346 • Favors approaches where evaluators define test plans based on ISO/IEC 18045 activities; when-
347 ever a technical domain is mature enough, ISO/IEC 15408-4 or standard refinement and ex-
348 tended components techniques can also be used to derive dedicated evaluation methods.

349

350 5.1.2.3 Evaluation methodology

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

355 • Reproducibility, repeatability, and availability of tests are ensured partly by ISO/IEC 18405
356 (which provides common notions such as the attack potential), and by the evaluation schemes
357 that use the standard (which are in charge of ensuring that evaluators have similar approaches,
358 and that developers are appropriately informed); for mature technologies, dedicated evaluation
359 methods can also be defined;

360 • All product types can be evaluated, as long as the evaluator is deemed competent for the assur-
361 ance level and/or type of technology considered. As a consequence, the evaluator has to con-
362 sider the state-of-the-art of attacks for the selected AVA_VAN, regardless of the functional fea-
363 tures described in the underlying PPs;

364 • Tests are not defined in advance, so that evaluators are allowed to introduce independent and
365 reasoned analysis in the process, which leads to:

366 – fine-tuning tests depending on the TOE itself (for example, language-specific tests: Python
367 and C do not lead to the same type of vulnerabilities);

- 368 – fine-tuning tests depending on evaluation findings: the evaluator is typically simulating an
 369 attacker in a limited timeframe; in this context, based on their knowledge of the TOE,
 370 evaluators define a suitable set of tests;
- 371 – fine-tuning tests depending on the evolution of the state-of-the-art (for example, if new
 372 attacks have been discovered in the field or in the academic literature).

373

374 5.2 Modularity

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

- 378 a) Modularity of the evaluation process: Splitting a product between **different TOEs**, resulting in
 379 several STs, and evaluating the complete product via a composition mechanism. This includes
 380 typically two main mechanisms:
- 381 • Composition of evaluated products using the ACO assurance class;
 - 382 • Composite product evaluation using _COMP assurance components;
- 383 b) Modularity of requirements within a **single TOE**, through the following mechanisms:
- 384 • Functional and assurance packages (notably EALs);
 - 385 • Modular PPs, which provide additional means to define optional features and extended
 386 TOEs through PP-Modules and standard PPs combined in PP-Configurations;
 - 387 • Multi-assurance evaluation paradigm, which allows addressing heterogeneous products
 388 or systems;
 - 389 • Requirement bundling¹, i.e. the structuring of functional and assurance requirements in
 390 dedicated subsections dependent on their purpose.

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

392 **EXAMPLES:**

393 - Architectural Patterns for the definition of security domains;

394 - More generally, how the standards can be used when evaluating complex products, as opposed to hierarchical
 395 composition situations, e.g. smartcards.

396 This transition guide should, whenever possible, clarify how these mechanisms can be used, in actual products,
 397 and whether they can be used in complex mass-market products such as cars, mobile systems, cloud-based sys-
 398 tems, etc.

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

400

401 5.2.1 Composition mechanisms

402 The first step that can be used to manage complexity is to break down a product into different parts that
 403 can be evaluated separately. This is typically performed by composition mechanisms.

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

- 405 — Layered,

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.

406 — Network or bi-directional,

407 — Embedded.

408 They are described in detail in Clause 14 of ISO/IEC 15408-1. The next sections provide some guidance
409 on how and when to use each one of these models.

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

411

412 **5.2.1.1 Composition models**

413 **Layered composition model**

414 In the layered model the product is composed of a base component and a dependent component. The
415 base component is independent of the dependent component. On the contrary, the dependent compo-
416 nent relies on the base component.

417 **Network or bi-directional composition model**

418 The network model is more relevant to integrators that build systems upon several evaluated products,
419 which rely on each other in a bi-directional way.

420 **Embedded composition model**

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

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

427

428 **5.2.1.2 Evaluation mechanisms for composition**

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

431 — The evaluation methodology defined in ISO/IEC 18405 for the ACO assurance class;

432 — The composite evaluation methodology originally defined in [16] and introduced in ISO/IEC
433 18405 for the _COMP assurance components.

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

436 ACO allows to evaluate a product composed of two evaluated products by reusing the results of the two
437 evaluations and by evaluating the interaction between them.

438 COMP allows to evaluate a composite product made of an evaluated base component and a dependent
439 component by reusing the evaluation of the base component. The composite approach is suitable in the
440 context of a complete product evaluation when the product's components are developed by multiple,
441 different entities.

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

444 — An Integrated Circuit (IC) and its dedicated embedded software, which is evaluated first;

445 — An execution environment, or platform, running on top of the IC and allowing the use of high-
446 level programming languages for the applicative layer, which is evaluated using _COMP;

447 — Some applications running on the platform, which are evaluated using _COMP.

448

449 **5.2.2 Packages**

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

- 452 • They are intended to be reusable (this is why they are named);
- 453 • They are typically written or validated by a community. For example, the EAL packages are
454 adopted in the standard itself;
- 455 • As a consequence, they are not only intended to improve understanding, but are meant to in-
456 clude requirements that are “useful and effective in combination” (as explained in ISO/IEC
457 15408-1).

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

459 Packages may be either:

- 460 • Assurance packages, containing only assurance components or requirements, or
- 461 • Functional packages, containing functional components or requirements.

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

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

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

474 It is not mandatory for packages to include all dependent components. However, all dependencies must
475 be met in a PP or a ST using the package. Otherwise, for any dependency that is not met, a rationale
476 must be provided.

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

480 **EXAMPLE 1**

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

482 **EXAMPLE 2**

- 483 • Using packages as a consistent set of assurance requirements: EALs are an example of
484 assurance packages, which are widely used;
- 485 • Using packages as a consistent set of functional requirements: A given community may want to
486 define a functional package to cover specific security objectives, such as secure channels using a
487 given proprietary protocol, for example. This protocol can be broken down into several SFRs,
488 e.g. authentication, information flow control policy, and corresponding cryptographic

489 capacities. Such a package could then be reused within the community by “copying and pasting”
490 it in different STs or PPs, without having to re-analyze which SFRs are needed;

491 • Inclusion of an SPD in a package: depending on the richness of the functionalities offered by the
492 package, the editor might consider including a specific SPD in the package itself. In the previous
493 example, a PP for an IPSec tunnel will include a “key distribution” package and a “negotiation
494 and key generation” package. Each package comes with its specific threats, that are not relevant
495 to the other:

496 ○ In the “key distribution” package, assumptions will be needed to cover interception
497 threats during the distribution,

498 ○ In the “negotiation and key generation” package, threats of key leakage or deduction
499 have to be considered.

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

501 • COMP is meant to facilitate the evaluation of composite products;

502 • PPA (Protection Profile Assurance) provides assurance packages for Direct Rationale PPs and
503 standard PPs evaluation;

504 • STA (Security Target Assurance) provides assurance packages for ST evaluation.

505

506 5.2.3 Modular Protection Profiles

507 When compared to functional packages, modular PPs provide an additional level of control for PP
508 editors:

509 • Packages may be used to expose possible functional variations of a TOE type/TOE but do not
510 modify the TOE type/TOE defined in the PP/ST.

511 • PP-Modules are mostly intended to describe TOEs built out of modules, including modules that
512 are sourced from different developers and/or are evaluated separately. PP-Modules rely on one
513 or more base PPs and may introduce changes to their TOE types. PP-Modules may use other PP-
514 Modules as a base.

515 • PP-Modules may identify a set of selection-based SFRs provided that such SFRs do not introduce
516 changes to the TOE and the TOE boundaries. Otherwise, it may be more suitable to define sev-
517 eral PP-Modules.

518 • Moreover, a PP-Module claiming demonstrable or strict conformance may carry a specific set of
519 assurance components for the module (see multi-assurance evaluation in clause 5.2.4).

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

525 PP-Modules can be used for representing:

526 • alternative architecture choices (for example, a smart meter exposing wired and/or wireless
527 interfaces for the same functionality);

528 • optional features or modules (for example, a payment terminal providing a magnetic stripe
529 reader and/or a smartcard reader and/or contactless payment via a smartphone...).

530 EXAMPLE An editor may want to define a PP for an application that is found in different ecosystems, for exam-
531 ple, smartcards and mobile devices. Modular PPs allow addressing the specific threats of each underlying

532 platform. Mandatory PP-Modules may typically be used with alternative sets of base PPs, each corresponding to a
533 given platform.

534

535 **5.2.4 Multi-assurance evaluations**

536 In addition to PP-Modules and PP-Configurations, the standard defines a flexible framework for the
537 multi-assurance evaluation of IT products using predefined EALs from ISO/IEC 15408-5 or assurance
538 components from ISO/IEC 15408-3, which allows claiming a global set of assurance requirements/as-
539 surance package for the entire TOE, and possibly multiple different sets of assurance requirements/as-
540 surance packages for different parts of the TSF, called the sub-TSFs.

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

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

546 **Erreur ! Source du renvoi introuvable.** contains the entire contribution on multi-assurance evalua-
547 tion, which includes the definition of the concept (for 15408-1), the extension of ACE assurance class
548 (for 15408-3) and the interpretation of the standard assurance classes in the context of a multi-evalua-
549 tion.

550 **5.2.4.1 Example 1: High-assurance selected functions**

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

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

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

559

560 **EXAMPLE**

561 For example, a smartphone with a secure hardware-backed key store could be such a TOE. The risk
562 owner has determined that the assurance for the whole smartphone needs to be at EAL2 level as there
563 is sufficient mitigation (ownership of the phone by the user, good monitoring of attacks, quick response
564 times, effective patching) to allow authorization of transactions to be performed by the phone. How-
565 ever, the risk owner has also determined that the hardware-backed key store needs a higher assur-
566 ance (e.g. EAL4 with AVA_VAN.5) so that long term keys are not compromised.

567 The bigger TOE might then have SFRs encoding user authentication and authorization of a transaction
568 verified at EAL2 level, and a sub-TSF with SFRs for the key store at EAL4+ level. The sub-TSF's SFRs
569 would encode the access control to the long-term keys as not allowing anyone to export them out of the
570 sub-TSF and requiring authorization from the user via the bigger TOE to perform the cryptographic sig-
571 nature operation. This example is illustrated in Figure 5-2 hereafter.

572

573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616

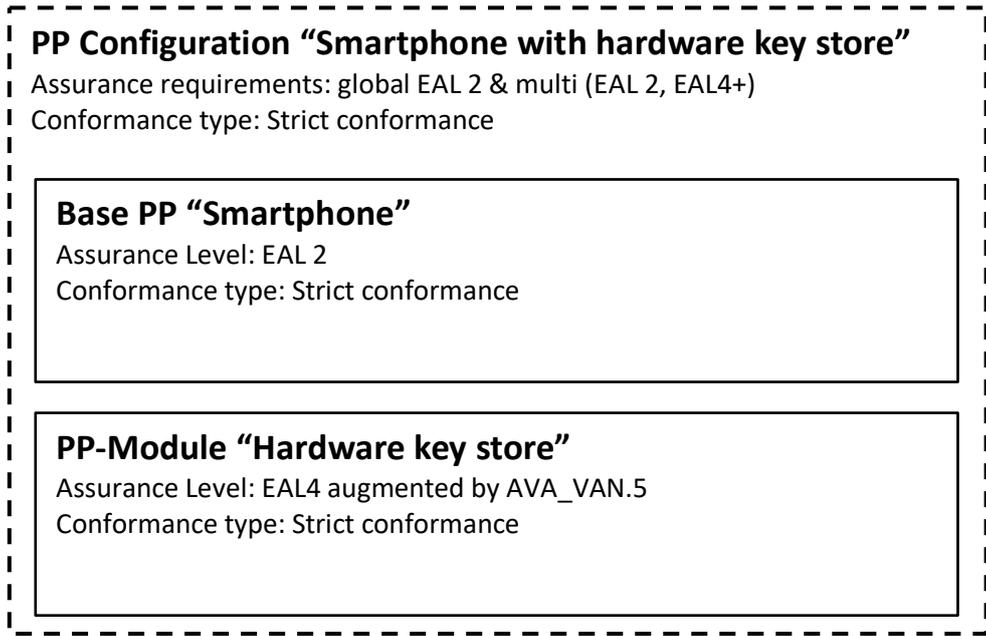


Figure 5-2 Smartphone with hardware key store

5.2.4.2 Example 2: Low assurance selected functions

EXAMPLE

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

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

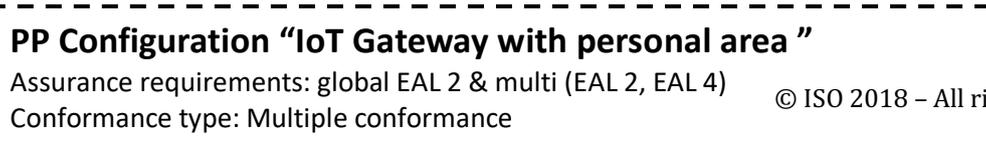
With the multi-assurance approach, a PP/ST author identifies the bigger TOE and the sub-TSFs including their boundaries and assigns a combination of both SFRs and SARs to each (sub-)TSF. In this manner, the PP/ST clearly shows what functionality is implemented, where it is implemented, and at which is the assurance expected for each functionality.

For example, an IoT gateway device could be such a TOE. The risk owner has determined that the assurance on the cloud connection services of the IoT gateway device needs to be at EAL4 level as the device is exposed to the internet. However, on the local area and personal area network the risk owner determined that assurance at EAL2 level is sufficient for checking the implementation of IoT protocols and potential lightweight cryptographic cipher suites. This example is illustrated in Figure 5-3 hereafter.

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

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

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



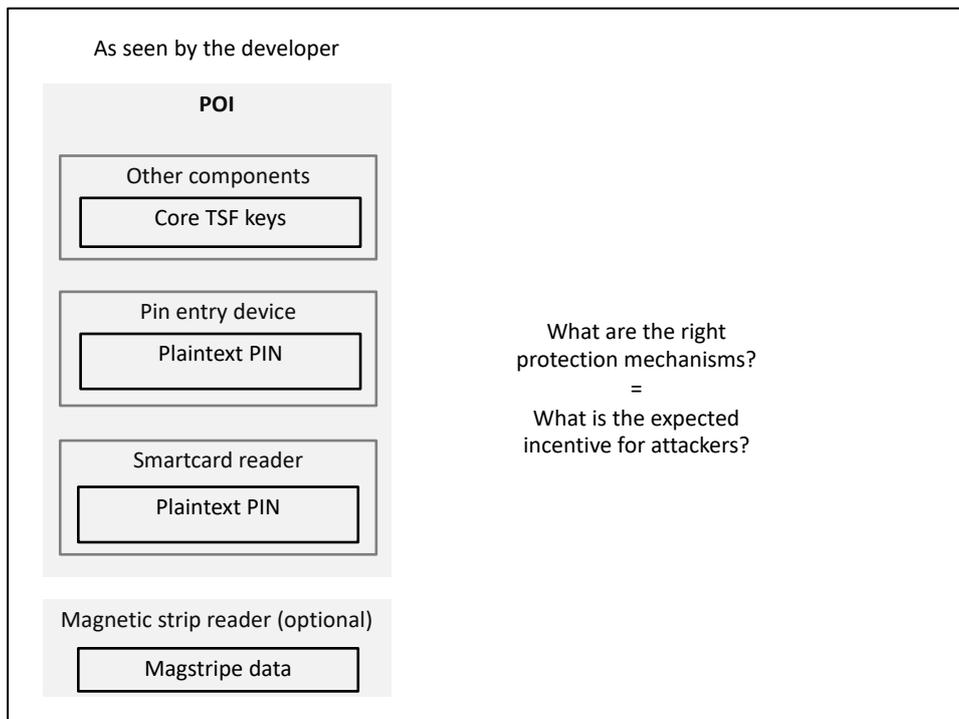
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638

Figure 5-3 — IoT gateway with personal area

5.2.4.3 Example 3: Point of Interaction use case

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

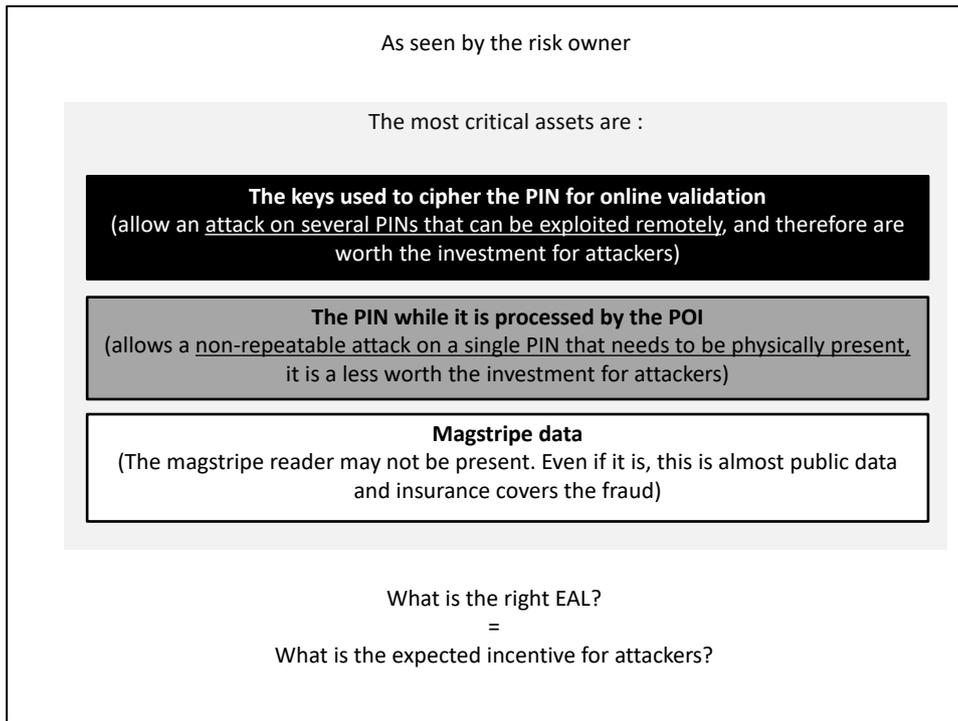
The following diagrams illustrate the motivation behind some of the POI PP-Configurations. The concepts have been simplified to allow non-POI specialist understand the concepts behind this organization of the TSF in parts, each of them associated with a specific AVA_VAN component.



639

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.

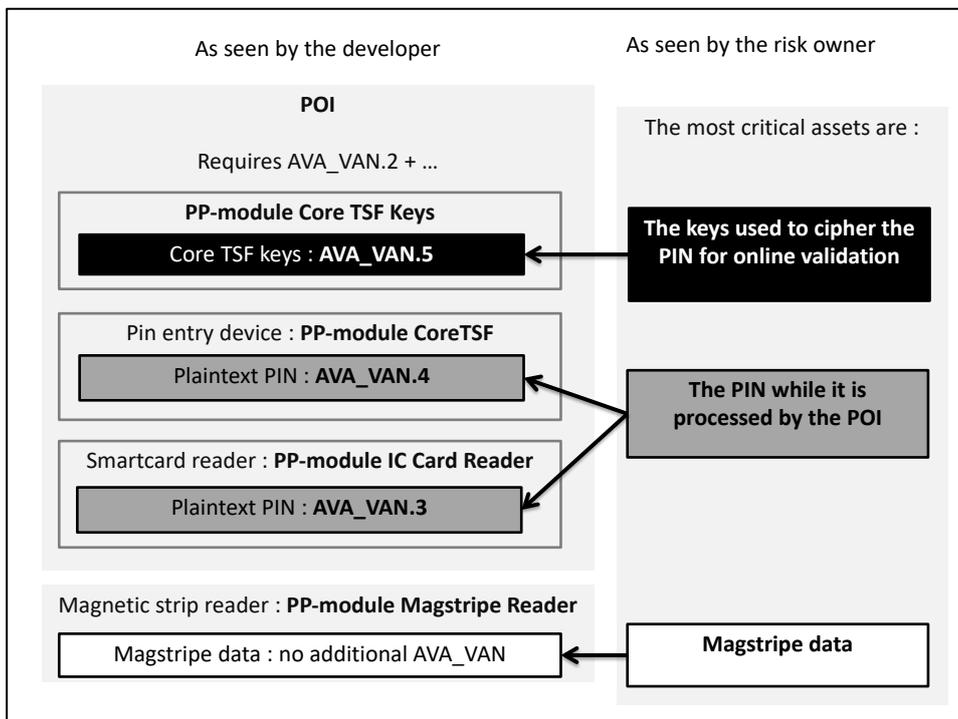
640



641

642

643



		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	...

646

647 **5.3 Consistent Standard's Language**

648 For this document's next version, editors suggest removing the section and moving the content to the overview
649 and section 6.

650 As highlighted by the Study Period, different communities use the ISO/IEC 15408 and ISO/IEC 18045
651 standards, with varying needs and contexts. Two of these are introduced for consideration in section
652 5.1.

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

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

657 The notion of SFR-supporting subsystems and modules is now considered optional. In practice, many developers
658 have legacy ADV_TDS documentation that is still relevant, and there is no reason to force them to refactor the
659 whole documentation to remove the SFR supporting elements. For this reason, the *SFR-supporting* notion has
660 been kept in the standard, so that existing ADV_TDS documentation is still compliant to the standard. However,
661 developers are advised to use only the *SFR-enforcing* and *SFR non-interfering* notions from now on (see ISO/IEC
662 15408-3 for more details).

663 Some update proposals concerning SARs have been discussed and finally not integrated into the revision.

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

- 665 a) how they can adapt the standard to their needs by defining supporting documents;
- 666 b) how they can adapt the standard to their needs by refinements or application notes;
- 667 c) how they can adapt the standard to their needs by defining extended requirements in an ST or
668 PP;
- 669 d) which adaptations of the standard could not be made by these means, and were made by modi-
670 fying the standard.

671 **5.4 Differentiation of ISO/IEC 15408: Evaluation Methods**

672 For this document's next version, editors suggest removing Section 5.4 and redistributing its content in Sections
673 5.1 and 6.2.

674 **5.4.1.1 Introduction**

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

677 The notion of derived evaluation methods in ISO/IEC 15408-4 addresses this concern. It is often re-
678 minded that ISO/IEC 15408 is technology-agnostic, and evaluations following ISO/IEC 15408 require
679 some degree of technology-specific adaptations, in order to match the specifics of the evaluated TOE
680 technology. This new version of ISO/IEC 15408 standardizes how to derive evaluation methods from
681 ISO/IEC 18045.

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

684 **5.4.1.2 Evaluation methods for exact conformance**

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

691 In this context, ISO/IEC 15408-4 is to be used to define the exact set of tests derived from ISO/IEC
692 18045 work units. The objective of such a derivation process is:

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

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

699 **5.4.1.3 Evaluation methods outside exact conformance contexts**

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

703 EXAMPLE

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

705 Similar efforts have been made for the evaluation of payment terminals and Hardware Devices with Se-
706 curity Boxes (see documents [3] to [5]).

707 This new version of the standard does not render these documents obsolete or non-compliant to
708 ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 15408-4 is another way of specifying TOE-specific evalua-
709 tion methods.

710

711 **6 Applying the standard to specific needs**

712 This section is newly added to the document and it is meant to provide practical guidelines for using the standard.

713 Content will be provided during the next draft stage. Experts contribution is welcome.

714 **6.1 Refining and deriving requirements**

715 **6.1.1 Refinements and Application Notes**

716 **6.1.2 Extended requirements**

717 **6.2 Refining and deriving evaluation methods**

718 **6.2.1 Attack-based approach**

719 **6.2.2 Specification-based approach**

720 **6.3 In practice: Supporting documents**

721

722 **7 Mapping of evolutions between ISO/IEC 15408 and ISO/IEC 18045 and the** 723 **new revision**

724 This section will be updated in the next draft stage. Diagrams reflecting the changes of each ISO/IEC 15408 docu-
725 ment will be provided.

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

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

731 After analysis of the contributions by the Study Period rapporteurs, WG 3 initiated a revision of both
732 ISO/IEC 15408 and ISO/IEC 18045. In addition, two additional parts of 15408 were proposed in New
733 Work Item Proposals (NWIPs). These were balloted within ISO and approval for this change was gained.
734 (SC27 N17025, N17026, N17027, N17028, N17029, and N17023).

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

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

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

743 In April 2019, WG 3 decided to move to third Committee Draft (CD3). The present document integrates
744 the CD2 disposition of comments and changes made to the standard in CD3 documents. CD1, CD2 and
745 CD3 have been produced by WG 3.

746 **7.1 Categorization of study periods and other inputs**

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

- 748 a) Approaches to security evaluation
- 749 b) Modularity
- 750 c) Consistent Standard's Language
- 751 d) Vulnerability Assessment
- 752 e) Clarify & Streamline Evidence Requirements
- 753 f) Consistent Standard Metrics
- 754 g) Better use of Development models & Process
- 755 h) Differentiation of ISO/IEC 15408

756 The main changes to the standard correspond to categories a), b), c) and h), which are described in
757 clause 5 of the present document. Categories d) to g) are referred to in the Annex.

758

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

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

765

766 **7.2 Summary**

767 ISO/IEC 15408 has been modified to include two additional parts, ISO/IEC 15408-4 and ISO/IEC 15408-
768 5.

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

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

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

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

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

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

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

787 **Table 7-1 Changes to the ISO/IEC 15408 structure**

Topic	Edition 3	Edition 4 (CD2 and CD3 stages)
Structure of ISO/IEC 15408	<p>Three parts of the standard were defined:</p> <ul style="list-style-type: none"> a) ISO/IEC 15408-1:2009, <i>Information technology — IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general requirements.</i> b) ISO/IEC 15408-2:2008, <i>Information technology — IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.</i> c) ISO/IEC 15408- 3:2008, <i>Information technology — IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.</i> 	<p>Five parts of the standard are defined:</p> <ul style="list-style-type: none"> a) ISO/IEC 15408-1:20XX, <i>IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general requirements.</i> b) ISO/IEC 15408-2:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.</i> c) ISO/IEC 15408- 3:20XX, <i>IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.</i> 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> e) ISO/IEC 15408- 5:20XX, <i>IT Security techniques — Evaluation criteria for IT</i>

		<i>security — Part 5: Pre-defined packages of security requirements.</i>
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.

788

789 **7.3 ISO/IEC 15408-1**

790 This section will be updated in the next draft stage. Diagrams will be provided to reflect the differences between
 791 previous and current PP, ST, PP-Module and PP-Configuration table of contents. The differences between con-
 792 formance types will be explained.

793

794

Table 7-2 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> <p>New definitions for terms related to compositions have been suggested.</p>
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	Text has been proposed that describes the types of modularity supported by ISO/IEC 15408. “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. STs cannot directly claim conformance to PP-Modules. <i>Text that describes the multi-assurance evaluation paradigm has been proposed.</i> Text describing PP-Module Conformance claims and statements, as well as text describing PP-Configuration conformance statements has been updated.
PP-Configurations	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. 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.
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.

795

796

797

Table 7-3 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	<ul style="list-style-type: none"> a) Changes to terminology as a result of the JTC 1 directives. b) Proposals for technical changes in terminology and new terms as a result of other changes in the standards.

	<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	<p>Text has been added for allowing Protection Profiles that require exact conformance to specify (and allow for use) optional requirements.</p>
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	<p>Text has been added for allowing PP-Modules that require exact conformance to specify (and allow for use) optional requirements.</p>
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> <p>The roles related to composite evaluation have been defined.</p>
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>

	<p>Annex A) Specification of Packages</p> <p>Annex B) Specification of Protection Profiles</p> <p>Annex C) Specification of PP-Modules and PP-Configurations</p> <p>Annex D) Specification of Security Targets and Direct Rationale STs</p> <p>Annex E) Guidance for Operations</p> <p>Annex F) PP Conformance</p>
--	--

798

799

Table 7-4 Proposed Changes in ISO/IEC 15408-1

Topic	Edition 4 (CD 3 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.</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>The terminology related to composition has been revised.</p> <p>New definitions for terms related to compositions have been introduced.</p>
Packages	<p>Text discussing the mandatory contents of packages has been added to the sub-clause 9.2 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	Text that describes the multi-assurance evaluation paradigm has been updated. Relation between multi-assurance evaluation and composition has been clarified.
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	The clause related to composition has been restructured and updated.
New Annex numbering and structure	The annexes were re-numbered in order to mirror the order of the main clauses in the normative part. The previous Annex E – Guidance for Operations – has been removed. Currently, the document includes the following informative annexes: 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) PP Conformance

800

801 **7.4 ISO/IEC 15408-2**

802 This section will be updated in the next draft stage. Diagrams and details of the changes to the SFRs will be pro-
803 vided.

804

805

Table 7-5 Proposed Changes in ISO/IEC 15408-2

Topic	Edition 4 (CD 1 stage)
Proposed new families	Families used in existing protection profiles have been added to the standard: <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) Some SFRs are still placeholders and a call for experts’ contributions has been included in the document.

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>

806
807
808

Table 7-6 Proposed Changes in ISO/IEC 15408-2

Topic	Edition 4 (CD 2 and CD3 stages)
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

809
810
811
812
813

7.5 ISO/IEC 15408-3

This section will be updated in the next draft stage. Details of the changes to the SARs will be provided.

Table 7-7 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.

814

815

816

Table 7-8 Proposed Changes in ISO/IEC 15408-3

Topic	Edition 4 (CD 2 and CD 3 stages)
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 and updated.
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.

817

818 7.6 ISO/IEC 15408-4

819 **This section will be updated in the next draft stage. Details regarding Evaluation Methods and Evaluation Activi-**
 820 **ties will be provided.**

821

822

Table 7-9 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	<p>6.1 Overview</p> <p>6.2 Specification of an Evaluation Method</p> <p>6.2.1 Overview</p> <p>6.2.2 Identification of evaluation methods</p> <p>6.2.3 Scope of the evaluation method</p> <p>6.2.4 Dependencies</p> <p>6.2.5 Required input from the developer or other entities</p> <p>6.2.6 Set of evaluation activities</p> <p>6.2.7 Required tool types</p> <p>6.2.8 Required evaluator competences</p> <p>6.2.9 Rationale for the evaluation method</p> <p>6.2.10 Additional verb definitions</p> <p>6.2.11 Requirements for reporting</p>
Clause 7 Structure of Evaluation Activities	<p>7.1 Overview</p> <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>

823

824

Table 7-10 New ISO/IEC 15408-4

Topic	Edition 4 (CD 2 and CD3 stage)
Clause 6	A diagram depicting the content and structure of an evaluation method has been provided.

Structure of an Evaluation Method	
-----------------------------------	--

825

826 **7.7 ISO/IEC 15408-5**

827 This section will be updated in the next draft stage. Diagrams and further details will be provided.

828

829

Table 7-11 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)

830

831

Table 7-12 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.

832

833 **7.8 ISO/IEC 18045**

834 This section will be updated in the next draft stage.

835

836

Table 7-13 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

837

838

Table 7-14 Proposed Changes in ISO/IEC 18045

Topic	Edition 4 (CD 2 stage)
Summary	Work units corresponding to ASE_COMP, ALC_COMP, ADV_COMP, ATE_COMP, and AVA_COMP defined in Appendix 1.1 of JIL <i>Composite product evaluation for Smart Cards and similar devices</i> have been inserted.

	<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>
--	---

839

840 **Annex A**
841 **(informative)**
842 **Study Periods Overview**

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

845 This Annex merges previous Annexes B and C.

846 **A.1 Vulnerability Assessment**

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

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

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

858 **Experts opinions on vulnerability assessment**

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

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

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

871 More generally, additional expert contributions are welcome.

872

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

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

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

880

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

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

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

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

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

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

894 A.2 Clarify & Streamline Evidence Requirements

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

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

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

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

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

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

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

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

911 A.3 Consistent Standard Metrics

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

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

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

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

924 **Experts opinions on metrics**

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

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

927 **A.4.1 Incremental development**

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

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

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

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

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

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

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

948 **Experts opinions**

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

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

952 **A.5 Reposition CEM**

953 To be completed

954 Contributions to the project are encouraged

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

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

957 To be completed

958 Contributions to the project are encouraged

959 **A.7 New requirements**

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

961

Bibliography

962 This bibliography contains references to further material and standards that the reader of
 963 this document may find useful. For undated references the reader is recommended to refer
 964 to the latest edition of the referenced document.

- 965 [1] JIL - The Application of CC to Integrated Circuits - Version 3.0 - February 2009
- 966 [2] JIL - Application of Attack Potential to Smartcards - Version 2.9 - January 2013
- 967 [3] JIL - CEM Refinements for POI Evaluation - Version 1.0 (for trial use) - 27th May 2011
- 968 [4] JIL - Application of Attack Potential to POIs - Version 1.0 (for trial use) - 9th June 2011
- 969 [5] JIL - Application of Attack Potential to Hardware Devices with Security Boxes - Version
 970 2.0 (for trial use) - December 2015
- 971 [6] JIL - Security Architecture requirements (ADV_ARC) - for smart cards and similar devices
 972 - Version 2.0 - January 2012
- 973 [7] JIL - Minimum Site Security Requirements - Version 2.1 (for trial use) – December 2017
- 974 [8] Supporting Document - Mandatory Technical Document - Full Drive Encryption:
 975 Authorization Acquisition - January 2015 - Version 1.0 - CCDB - 2015-01-003
- 976 [9] Supporting Document - Mandatory Technical Document - Full Drive Encryption:
 977 Encryption Engine - January 2015 - Version 1.0 - CCDB-2015-01-004
- 978 [10] Supporting Document - Mandatory Technical Document - Evaluation Activities for
 979 Stateful Traffic Filter Firewalls cPP - February 2015 - Version 1.0 - CCDB-2015-01-002
- 980 [11] Supporting Document - Mandatory Technical Document - Evaluation Activities for
 981 Network Device cPP - February 2015 - Version 1.0 - CCDB-2015-01-001
- 982 [12] collaborative Protection Profile for Network Devices - Version 1.0 - 27-Feb-2015
- 983 [13] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition -
 984 Version 1.0 - January 26, 2015
- 985 [14] collaborative Protection Profile for Full Drive Encryption - Encryption Engine - Version
 986 1.0 - January 26, 2015
- 987 [15] collaborative Protection Profile for Stateful Traffic Filter Firewalls - Version 1.0 - 27-
 988 Feb-2015
- 989 [16] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction
 990 and general model, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-001)
- 991 [17] Common Criteria for Information Technology Security Evaluation. Part 2: Security
 992 functional components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-002)
- 993 [18] Common Criteria for Information Technology Security Evaluation. Part 3: Security
 994 assurance components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-003)

995 [19] Common Methodology for Information Technology Security Evaluation. Evaluation
996 methodology, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-004)

997 [20] CC and CEM addenda. Selection-based SFRs, Optional SFRs, May 2017, Version 0.5
998 (CCDB-2017-05-XXX)

999

1000 Bibliography to be updated

1001 Expert contributions are requested

1002