



REPLACES: 1589

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 3rd WD 22216 — Information technology — Security techniques — Evaluation Criteria for IT security — Introductory guidance on evaluation for IT security

SOURCE: Project editor

DATE: 2018-07-18

PROJECT: 1.27.127 (TR 22216)

STATUS: In accordance with WG recommendation 10 and 11 (contained in SC 27 N18471) of 56th SC 27/WG 3 meeting held in Wuhan, China, 16th – 20th April 2018, this document is being circulated to experts and liaison organizations for study and comment closing by **2018-08-31**.

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.

PLEASE also note the following notice from the editors:

As discussed during last WG3 meeting in Wuhan, a new concept (multi assurance) has been introduced in the ISO15408 standard. This concept was only outlined during the meeting, so experts might have different visions of what to expect. It is now described with much more details in the standard. Therefore, we would like to draw the attention of all interested experts on this topic, so it can be discussed thoroughly in Gjovik. Multi assurance is introduced in ISO 15408 Part 1 and Part 3, but experts are invited to read first the TR22216 (section 6.2.7 and Annex B), where the concept is described in its entirety, alongside some examples.

ACTION: COMM

DUE DATE: 2018-08-31

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

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

NO. OF PAGES: 1 + 92

ISO/IEC JTC 1/SC 27/WG 3 N1492

Date: 2018-07-17

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

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

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

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

WD stage

Warning for WDs and CDs

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

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

© 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	Types of compositions.....	8
59	6.2.3	Evaluation mechanisms for composition	9
60	6.2.4	Modularity within a TOE	9
61	6.2.5	Packages.....	9
62	6.2.6	Modular Protection Profiles.....	11
63	6.2.7	Multi-assurance Evaluations	11
64	6.3	Consistent Standard's Language.....	14
65	6.4	Differentiation of ISO/IEC 15408: Evaluation Methods.....	14
66	7	Mapping of evolutions with ISO/IEC 15408 and ISO/IEC 18045	15
67	7.1	Summary.....	15
68	7.2	Detailed evolutions.....	16
69	8	Migration from the third to the fourth edition of the ISO/IEC 15408 series	21
70	Annex A	(informative) Study Periods Overview	22
71	A.1	Vulnerability Assessment.....	22
72	A.2	Clarify & Streamline Evidence Requirements.....	23
73	A.3	Consistent Standard Metrics	23
74	A.4	Better use of development models and process	24
75	A.4.1	Incremental development	24
76	A.4.2	Other topics to be discussed.....	24
77	A.5	Reposition CEM.....	24
78	A.6	Review Tools and Techniques	24
79	A.7	New requirements.....	24
80	Annex B	(informative) Multi-assurance evaluation.....	25
81	1	Introduction	26
82	1.1	Executive summary	26
83	1.2	Scope	26
84	1.3	Audience	26

85	1.4	Normative references.....	26
86	1.5	Terms and definitions	27
87	1.6	Abbreviated terms	27
88	1.7	Notation.....	27
89	2	ISO/IEC 15408-1 update.....	27
90	2.1	Multi-assurance evaluation.....	27
91	2.2	Security Targets.....	28
92	2.3	Protection Profiles, PP-Modules and PP-Configurations.....	29
93	2.3.1	Introduction.....	29
94	2.3.2	Protection Profiles	29
95	2.3.3	PP-Modules	29
96	2.3.4	PP-Configurations	30
97	2.3.5	Usage of PPs and PP-Configurations in Security Targets.....	31
98	2.4	Evaluation and evaluation results.....	32
99	2.4.1	Conformance claims	32
100	2.4.2	Evaluation of PPs and PP-Configurations.....	32
101	2.4.3	Evaluation of STs and TOEs.....	32
102	2.5	Annex A – Specification of STs	33
103	2.6	Annex B – Specification of PPs	33
104	2.7	Overview.....	33
105	2.8	Class ACE	33
106	2.8.1	Introduction.....	33
107	2.8.2	ACE_INT.1	33
108	2.8.3	ACE_CCL.1	34
109	2.8.4	ACE_SPD.1.....	36
110	2.8.5	ACE_OBJ.1	37
111	2.8.6	ACE_OBJ.2	38
112	2.8.7	ACE_ECD.1	38
113	2.8.8	ACE_REQ.1 & 2	40
114	2.8.9	ACE_REQ.1	40
115	2.8.10	ACE_REQ.2.....	42
116	2.8.11	ACE_MCO.....	44
117	2.8.12	ACE_CCO	47
118	2.9	Class APE	50
119	2.10	Class ASE.....	51
120	Annex C	(informative) Concept approach to the ISO/IEC 15408 & 18045 Terminology	52
121	1	Background	52
122	2	The concept approach introduction to ISO/IEC 15408-1	54
123	2.1	General action plan (GAP) to get the objective	54
124	2.2	What would be the impact of the GAP on the project timetable?	55
125	3	Identification of concepts	55
126	3.1	General.....	55
127	3.3	Concepts.....	57
128	3.3.1	Security Model.....	57
129	3.3.2	Assurance	58
130	3.3.3	Target of Evaluation, TOE.....	59
131	3.3.4	Evaluation techniques	60
132	3.3.5	Taxonomy.....	60
133	4	Assignment of Terms.....	61
134		Bibliography	85
135			

Foreword

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

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

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

Editors' note:

This guide provides insight into the multi-assurance level concept in clause 6.2.7 and provides the original contribution in Annex B to facilitate the expert review.

IT Security techniques — Introductory guidance on evaluation for IT security

1 Scope

The scope statement is, for now, the statement defined in the New Work Item Proposal (N16885) for this document.

This document will:

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

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

235 **3 Terms and definitions**

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

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

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

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

241 **3.1 Terms**

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

243 **3.2 Abbreviations**

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

245 **4 Using this guidance**

246 **4.1 Using this guidance during the revision of ISO/IEC 15408 and ISO/IEC 18045**

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

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

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

255 **4.2 Using this guidance for transitional information**

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

258 **5 History of this revision of ISO/IEC 15408 and ISO/IEC 18045**

259 **5.1 Key documents**

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

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

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

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

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

5.2 Categorization of study periods, and other inputs

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

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

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

5.3 General

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

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

6 Main changes to the standard

6.1 Approaches to security evaluation

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

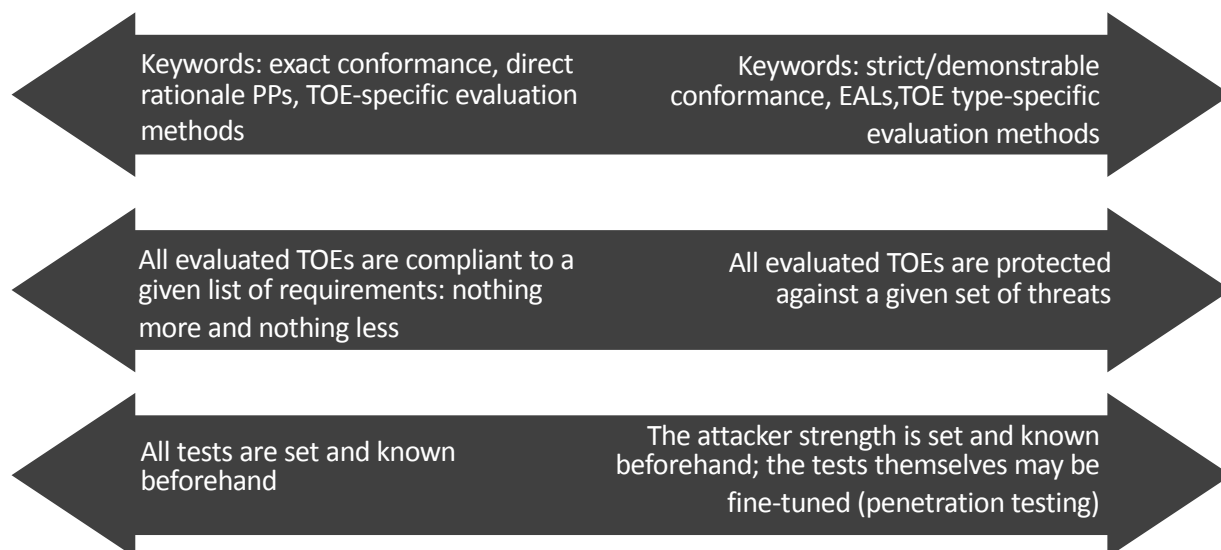


Figure 1 — Specification-based and attack-based approaches

The main differences between them are as follows:

- A new approach, which is called hereafter the “specification-base 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;

- still uses standard Protection Profiles and Security Targets.

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

6.1.1 The “specification-based” approach

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

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

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

6.1.1.1 Conformance

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

It should be noted that “optional features” in exact conformance PPs are addressed by packages (see section 5.2.2.2).

6.1.1.2 Evaluation methodology

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

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

6.1.1.3 Edition of Protection Profiles and Security Targets

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

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

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

- Less emphasis on the analysis of the security problem, which has a limited impact on the evaluations since there is no need to perform TOE-specific vulnerability analysis;
 - Maximizing the use of selection-based SFRs, and minimizing the use of open-ended assignments;
- EXAMPLE Identification of required versions of protocols and cryptographic algorithms in SFRs.
- Making extensive use of extended SFRs to specify the expected characteristics of the TOE;
 - Making extensive use of application notes to describe the intended technology-specific adaptation of SFRs;

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

6.1.2 The “attack-based” approach

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

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

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

6.1.2.1 Conformance

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

6.1.2.2 Evaluation methodology

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

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

6.1.2.3 Edition of Protection Profiles and Security Targets

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

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

6.2 Modularity

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

- a) Splitting a product between **different TOEs**, resulting in several Security Targets, and evaluating the complete product via a composition mechanism. This includes typically two main mechanisms:
 - Composition using the ACO assurance class;
 - Composite product evaluation using _COMP assurance components;
- b) Within a **single TOE**, the following mechanisms may help taking into account the notion of modularity:
 - Functional and assurance packages (notably EALs);

- Modular Protection Profiles, which provide additional means to define optional features and extended TOEs through PP-Modules and standard PPs combined in PP-Configurations;
- Multi-assurance evaluation paradigm, which allows addressing heterogeneous products or systems;
- Requirement bundling¹, i.e. the structuring of functional and assurance requirements in dedicated subsections dependent on their purpose.

The new version introduces new mechanisms for modularity. Other items might be introduced during this revision.

EXAMPLES:

- Architectural Patterns for the definition of security domains;

- More generally, how the standards can be used when evaluating complex products, as opposed to simple and hierarchical composition situations (smartcards).

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

Expert contributions are welcome on this topic.

6.2.1 Composition mechanisms

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

6.2.2 Types of compositions

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

- Layered,
- Network, or bi-directional,
- Embedded,
- Top-to-bottom.

They are described in detail in Clause 13 of ISO/IEC 15408-1. The next sections provide some guidance on how and when to use each one of these models.

At the moment, composition is practically supported only for the layered model. Expert contributions are welcome, either for referencing initiatives of supporting documents for other composition models, or for suggesting additions to the standard in that direction.

The layered model is the most often used of the models. This is typically used in the smartcard context, where a product can consist of:

- An Integrated Circuit and its dedicated embedded software;
- An execution environment, or platform, allowing the use of high-level programming languages for the applicative layer;
- Some applications running on the platform.

Each of these layers can lead to a Protection Profile for the composite TOE consisting of the base layer(s) plus the dependent layer(s).

This model is particularly relevant in a context where each layer is developed by a different actor within the supply chain. For example, different application developers may use the same evaluated platform. In

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

the same manner, an actor developing both the platform and applications can source different evaluated ICs.

6.2.2.1 Network, or bi-directional

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

6.2.2.2 Embedded

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

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

6.2.2.3 Top-to-bottom

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

6.2.3 Evaluation mechanisms for composition

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

- The evaluation methodology defined in ISO/IEC 18405 for the ACO assurance class;
- The composite evaluation methodology defined in [16].

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

6.2.4 Modularity within a TOE

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

6.2.5 Packages

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

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

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

Packages may be *optional*. When a PP editor defines an optional package, they must define the conditions in which ST editors are mandated to use them. As described in Annex C of ISO/IEC 15408-1, the SFR or SAR section “provides the rationale for the selection of the requirements”.

Packages may be either:

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

Both types of packages adhere to a structure that includes:

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

Additionally, a functional package may include a Security Problem Definition (SPD) and Security Objectives (for the TOE and the operational environment) derived from that SPD.

EXAMPLE 1

- An optional package for some security behaviour that is not required to claim conformance to a PP;
- Alternative packages driven by a selection that is operated in an SFR.

EXAMPLE 2

- **Using packages as a consistent set of assurance requirements:** EALs are an example of assurance packages, which are widely used;
- **Using packages as a consistent set of functional requirements:** A given community may want to define a functional package to cover specific security objectives, such as secure channels using a given proprietary protocol, for example. This protocol can be broken down into several SFRs, e.g. authentication, information flow control policy, and corresponding cryptographic capacities. Such a package could then be reused within the community by "copying and pasting" it in different STs or PPs, without having to re-analyze which SFRs are needed;
- **Optional packages:** A given type of TOE may provide a selection-based alternative for some of its SFRs. However, such selections may require the inclusion of different dependencies. For example, keys used in an IPSec tunnel may either be distributed or created by the equipment itself, after a negotiation. In the first case, a single cryptographic SFR is needed. In the second case, a PP editor might want to define requirements on the whole negotiation protocol. In both cases, the ST writer using the PP must be able to select only one of those two sets of SFRs. In this case, these sets may be described as optional packages²;
- **Inclusion of an SPD in a package:** depending on the richness of the functionalities offered by the package, the editor might consider including a specific SPD in the package itself. In the previous example, a PP for an IPSec tunnel will include a "key distribution" package and a "negotiation and key generation" package. Each package comes with its specific threats, that are not relevant to the other:
 - In the "key distribution" package, assumptions will be needed to cover interception threats during the distribution,
 - In the "negotiation and key generation" package, threats of key leakage or deduction have to be considered.

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

- COMP is meant to facilitate the evaluation of composite products;
- PPA (Protection Profile Assurance) provides assurance packages for Direct Rationale PPs and standard PPs evaluation;

2

It has to be noted that optional packages are compatible with the notion of exact conformance PPs. Such PPs can not only define optional requirements, but they may also include optional packages due to selections in SFRs leading to different dependencies.

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

6.2.6 Modular Protection Profiles

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

- Packages may be used to expose possible functional variations of a TOE type/TOE but do not modify the TOE type/TOE defined in the PP/ST.
- PP-Modules are mostly intended to describe TOEs built out of modules, including modules that are sourced from different developers and/or are evaluated separately. PP-Modules rely on one or more base PPs and may introduce changes to their TOE types.
- Moreover, a PP-Module may carry a specific assurance level for the module (see multi-assurance levels in clause 6.2.7).

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

PP-Modules can be used for representing:

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

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

6.2.7 Multi-assurance Evaluations

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

The previous section already outlined the benefits of modular PPs. In addition, multi-assurance evaluations allow addressing heterogeneous products/systems and evaluating modular TOEs that require different levels of security assurance for different parts of their functionality. The main benefit hereby is that the complete TOE is assessed within one evaluation. Hence, the soundness of the security claims can be ensured.

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

Annex B contains the entire contribution on multi-assurance evaluation, which includes the definition of the concept (for 15408-1) and the extension of ACE assurance class (for 15408-3).

6.2.7.1 Example 1: High-assurance selected functions

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

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

With the multi-assurance approach, a PP/ST author identifies the bigger TOE and the sub-TOEs including their boundaries and assigns a combination of both SFR- and SAR-packages to each (sub-)TOE. In this manner the PP/ST identifies clearly what functionality is implemented, where it is implemented, and at which assurance level that functionality is checked.

EXAMPLE

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

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

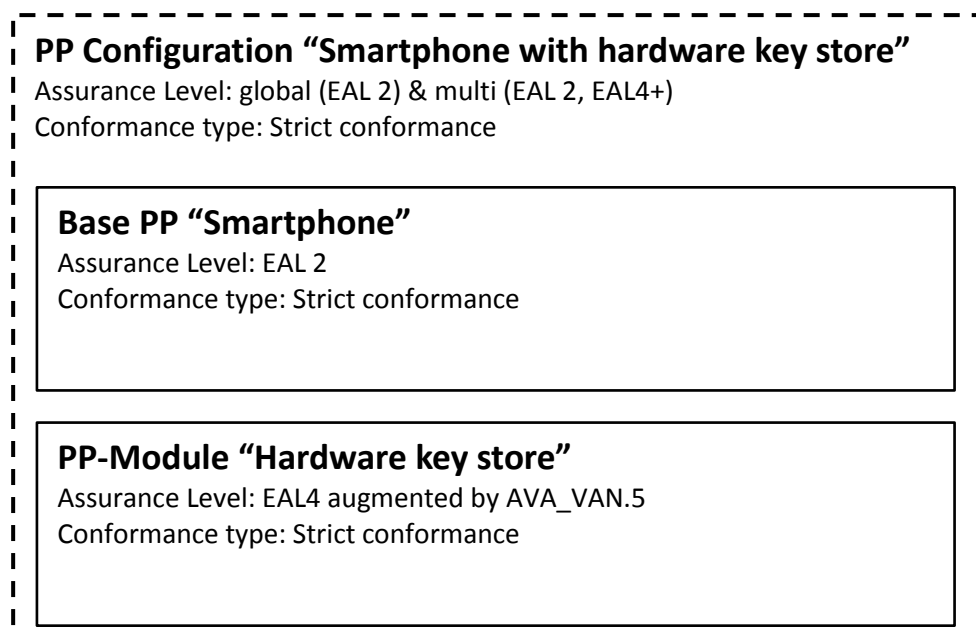


Figure 2 Smartphone with hardware key store

6.2.7.2 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-TOEs that allow a lower assurance level.

With the multi-assurance approach, a PP/ST author identifies the bigger TOE and the sub-TOEs including their boundaries and assigns a combination of both SFR- and SAR-packages to each (sub-)TOE. In this manner, the PP/ST clearly shows what functionality is implemented, where it is implemented, and at which assurance level that functionality is checked.

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 3 hereafter.

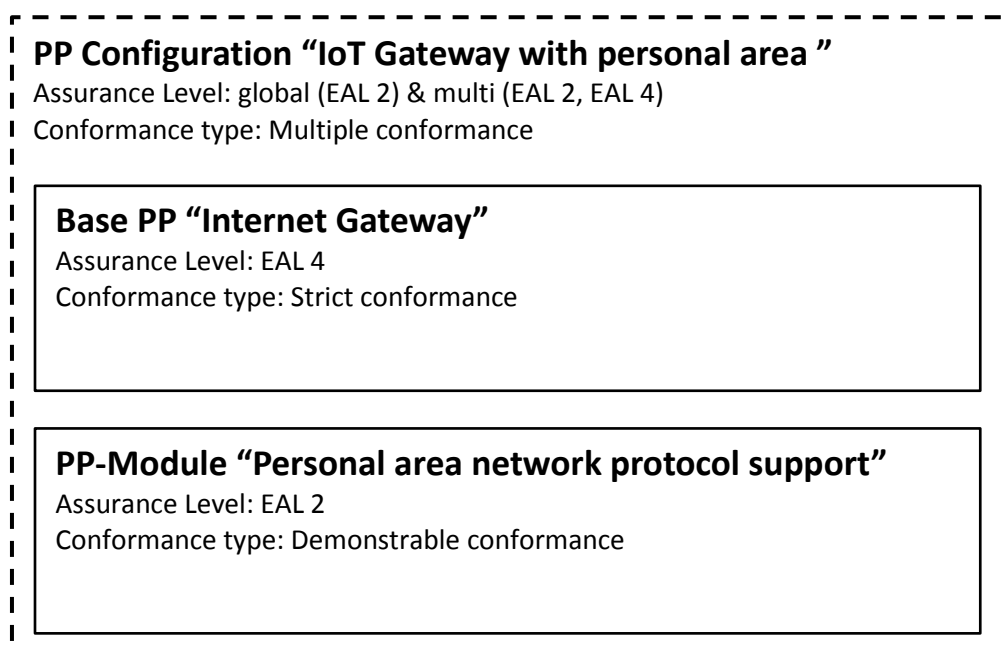


Figure 3 — IoT gateway with personal area

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-TOE 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-TOEs 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-TOEs 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 and PP-Modules are consistent.), because
- the outside threat is exclusively handled by the gateway (typically via an information flow control SFR, which ensures that connections to these sub-TOEs are not possible from outside the personal area network).

6.3 Consistent Standard's Language

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

In order to improve the standard language for all communities,

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

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

To be completed

Some update proposals concerning SARs have been discussed and finally not integrated into the revision. Nevertheless, expert contributions are welcome to improve the standard language or make it more consistent.

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

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

6.4 Differentiation of ISO/IEC 15408: Evaluation Methods

6.4.1.1 Introduction

As highlighted by the Study Period, there is a concern about how the standard can address more technology areas.

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

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

6.4.1.2 Evaluation methods for exact conformance

The notion of exact conformance aims at completely defining requirements and tests before an evaluation begins. These requirements and tests are approved within a community (this community may be a set of suppliers for a given customer, a national certification scheme, an MRA ...) and are typically supplied in the form factor of a PP and supporting documents. Examples of this can be found in currently used collaborative Protection Profiles and their corresponding supporting documents (see documents [8] to [15]).

To be completed

The option of directly inserting the evaluation methods in the PP itself are not yet formally approved, but this should eventually be mentioned here.

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

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

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

6.4.1.3 Evaluation methods outside exact conformance contexts

Currently, SARs and CEM refinements are performed through supporting documents. In particular, efforts have been made in some technical communities such as the smartcard community to refine the ISO/IEC 15408 and ISO/IEC 18045.

EXAMPLE

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

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

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

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

7.1 Summary

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

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

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

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

ISO/IEC 15408-3 has been modified to include changes related to CC 3.1 R5 and to the multi-assurance concept. Text relating to EAL and CAP security assurance packages has been moved to ISO/IEC 15408-5.

Editor's Note:

In CD1, packages are evaluated as part of the PPs/ST.

As requested in the comment US/NIAP64 on ISO/IEC 15408-1 WD2, package evaluation criteria should be developed in ISO/IEC 15408-3 and ISO/IEC 18045. In the next draft, the SARs should be added to Part 3 and the appropriate work units for verifying these SAR's should be added to ISO/IEC 18045.

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

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

7.2 Detailed evolutions

The following tables provide an overview of the changes leading to current CD 1.

Table 1 — Changes to the ISO/IEC 15408 structure

Topic	Edition 3	Edition 4 CD 1
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 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>	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> 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 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.

765

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

Topic	Edition 4 CD 1
Structure of ISO/IEC 15408-1	This part of ISO/IEC 15408 has been restructured to allow the grouping of related topics appropriately.
Terminology	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

	<p>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	<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>Text that describes the multi-assurance evaluation paradigm has been proposed.</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.

767

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

Topic	Edition 4 CD 1
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>

769

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

Topic	Edition 4 CD 1
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.

771

772 **Table 5 – New ISO/IEC 15408-4**

Topic	Edition 4 CD 1
General	<p>This is a new part of ISO/IEC 15408.</p> <p>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.</p>
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	7.1 Overview 7.2 Specification of an evaluation activity 7.2.1 Unique Identification of the evaluation activity 7.2.2 Objective of the evaluation activity 7.2.3 Relation of the evaluation activity to SFRs, SARs, and other evaluation activities 7.2.4 Rationale for the evaluation activity 7.2.5 Tool types required to perform the activity 7.2.6 Required evaluator competences 7.2.7 Required input from the developer or other entities 7.2.8 Assessment strategy 7.2.9 Pass/fail criteria 7.2.10 Requirements for reporting
Clause 7 Structure of an Evaluation Method	7.1 Overview 7.2 Description of an Evaluation Method 7.2.1 Overview 7.2.2 Scope of the evaluation method 7.2.3 Dependencies 7.2.4 Set of evaluation activities 7.2.5 Required tools 7.2.6 Required evaluator competences 7.2.7 Justification of the completeness of the evaluation method 7.2.8 Additional verb definitions 7.2.9 Requirements for reporting

773

774 **Table 6 — New ISO/IEC 15408-5**

Topic	Edition 4 CD 1
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)

775

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

Topic	Edition 4 CD 1
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

777

778 **8 Migration from the third to the fourth edition of the ISO/IEC 15408 series**

779 To be completed

780

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

781

Annex A (informative) Study Periods Overview

This annex presents the experts contributions to the Study Period and an overview per categories.

This Annex merges previous Annexes B and C.

The current content provides details for the categories for which expert contributions have not been provided or accepted by WG3 experts.

A.1 Vulnerability Assessment

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

- Currently, ISO/IEC 15408 allows low assurance evaluations (up to EAL2), and also allows adding SARs on top of any EAL, which makes CC valuable among communities that have no need for focused vulnerability analysis;
- At the same time, ISO/IEC 15408 allows grading EALs evaluations up to EAL7, which is of benefit to communities that have a need for high assurance, and need a scale based upon increasing levels of vulnerability and conformity assessment.

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

Experts opinions on vulnerability assessment

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

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

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

More generally, additional expert contributions are welcome.

Experts opinions on CEM completion for EAL5+ and higher

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

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

Expert opinions are welcome on this topic.

Experts opinions on improvements for vulnerability assessment

The Study Period proposed that additional guidelines and examples might further improve the standard. For example, the standard could address:

- static, dynamic, or memory analysis techniques that may be used during vulnerability assessment on top of usual penetration testing techniques and manual source code analysis;
- Semi-automated dynamic techniques, such as fuzzing, may also be used.

The revised standards may provide examples and guidance for communities willing to define supporting documents, in order to help them integrate such techniques in vulnerability assessment activities. Alternatively, experts could consider a supporting technical report to cover this matter.

As a sidenote, a contribution on fuzzing for developers has already been suggested in WD1, but was ultimately rejected because it did not give enough perspective on the complete set of relevant development activities that can be used alongside fuzzing, and did not clarify how this would be taken into account from an evaluation methodology point of view. Consequently, experts contributions are welcome but should make sure that they provide suggestions that are generic enough, and that include all relevant CEM activities.

A.2 Clarify & Streamline Evidence Requirements

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

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

Experts opinions The study period identified the following issues:

- This document may also provide guidelines to clarify how other kinds of evidences may be used during the evaluation. As an example, static, dynamic, or memory analysis techniques may be used on top of documentation evidences. Changes introduced at the moment in ALC_CMC and ALC_TAT are still modest.
- Developers would like to reuse test evidences compliant to other standards, for example by using supporting documents.
- More generally, explanations on how the new standard will allow the reuse of compliance to other standards.

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

More generally, expert contributions are welcome on this topic.

A.3 Consistent Standard Metrics

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

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

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

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

Experts opinions on metrics

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

A.4 Better use of development models and process**A.4.1 Incremental development**

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

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

A.4.2 Other topics to be discussed

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

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

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

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

Experts opinions

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

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

A.5 Reposition CEM

To be completed

Contributions to the project are encouraged

A.6 Review Tools and Techniques

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

To be completed

Contributions to the project are encouraged

A.7 New requirements

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

906
907
908

Annex B
(informative)
Multi-assurance evaluation

909 This Annex contains the integral contribution on the multi-assurance evaluation concept, as
910 submitted to the WG 3 editors.

911

912 **Foreword**

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

1 Introduction

1.1 Executive summary

- 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.

1.2 Scope

- 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.
- 3 These elements supplement CC Part 1, CC Part 3 and CEM and should eventually be integrated to the standard.

1.3 Audience

- 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.

1.4 Normative references

- 5 The following references apply to this document.
- | | |
|------------|--|
| [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. |
| [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. |
| [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. |
| [CEM] | Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 5, April 2017. Evaluation methodology. CCMB-2017-04-004. |
| [CC-1-WD2] | ISO/IEC 15408-1 WD2 |
| [CC-1-CD1] | ISO/IEC 15408-1 CD1, FR draft 2018-06-06 |
| [CC-2-WD2] | ISO/IEC 15408-2 WD2 |
| [CC-3-WD2] | ISO/IEC 15408-3 WD2 |
| [CC-3-CD1] | ISO/IEC 15408-3 CD1, draft 2018-05-28 |
| [CC-4-WD2] | ISO/IEC 15408-4 WD2 |
| [CC-5-WD2] | ISO/IEC 15408-5 WD2 |
| [CEM-WD2] | ISO/IEC 18045 WD2 |

1.5 Terms and definitions

(To be added to sub-clause [CC-1-CD1] §4.1 „Terms and definitions common in the CC“)

- 6 **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.
- 7 **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.
- 8 **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.

1.6 Abbreviated terms

(To be added to sub-clause [CC-1-CD1] §5 „Symbols and abbreviated terms“)

- a) **AL** Assurance Level

1.7 Notation

- b) The first occurrence of new or modified normative elements introduced for the definition of the multi-assurance evaluation approach is written in **bold** police.

2 ISO/IEC 15408-1 update

15408-1 WD2 and CD1 draft 2018-06-06 have been used

2.1 Multi-assurance evaluation

(new sub-clause in [CC-1-CD1] §6 „General model“, before the new sub-clause clause 6.3 „Security Target“)

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

- 10 Note: The standard provides an alternative framework for defining dedicated evaluation methods and activities using ISO/IEC 15408-4.

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

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

988 2 and ensuring that the multiple assurance levels are sound with regard to the secu-
 989 rity needs for the product/system.

990 12 Examples where the multi-assurance paradigm is relevant are the following:

- 991 • A device where some security functionality requires higher assurance than
 992 the rest, for instance, a key storage and processing unit, a secure boot
 993 module, etc.
- 994 • A device where some parts of the security functionality do not require the
 995 same high evaluation assurance as other more exposed parts of the device,
 996 for instance an internet gateway with support for personal area network
 997 protocols.
- 998 • A device where some security functionality can be implemented in differ-
 999 ent ways for different use cases, requiring different levels of assurance for
 1000 the different implementations, for instance
 - 1001 - tamper-resistant module
 - 1002 - software module
 - 1003 - (third-party) black-box components.

1004 2.2 Security Targets

1005 *(completes sub-clause [CC-1-CD1]§ 6.3.1 „General“)*

1006

- 1007 c) A Security Target may be defined as standalone document for the specif-
 1008 ic TOE or may comply with one or more preexistent Protection Profiles
 1009 and thereby reuse and specialize their generic definitions to the meet the
 1010 specific TOE. In the second case, the ST must meet the conformance
 1011 conditions set forth in the PPs.

1012 *(completes sub-clause [CC-1-CD1]§ 6.3.2 „Correctness of the TOE“)*

- 1013 13 A Security Target must claim a global set of SAR for the entire TOE and may
 1014 additionally structure the TOE in various modules and claim a specific set of
 1015 SARs for each of the modules. The second case can be achieved through the con-
 1016 formance to two or more PPs with different Assurance Levels and/or to multi-
 1017 assurance PP-Configurations.

1018 14 Note: When multi-assurance is relevant although there is no PP-Configuration to
 1019 rely on or the pre-defined PP-Configurations do not fully cover the TOE's securi-
 1020 ty problem, the ST writer can take any of the two following paths:

- 1021 • Define a PP-Configuration that is fully appropriate for the ST. This is not
 1022 a limitation and does not represent additional effort since an ST is a spe-
 1023 cial type of PP, where all the SFRs are instantiated and the TSS provides
 1024 the relationship with the actual implementation : if an ST evaluates suc-
 1025 cessfully against ASE requirements then the same ST evaluates success-
 1026 fully against APE requirements.

- 1027 • Associate the ST specific SFRs to the ST global Assurance Level (AL),
 1028 which by definition must be identical or lower than all the global ALs of
 1029 the PPs/PP-Configurations that are used.

1030 **2.3 Protection Profiles, PP-Modules and PP-Configurations**

1031 **2.3.1 Introduction**

1032 *(completes [CC-1-WD2]§8.1)*

- 1033 15 A PP-Configuration is an operation on a set of PPs and PP-Modules whose result
 1034 is semantically equivalent to a standard PP and meant to be used as such. That is,
 1035 a PP-configuration is a way to build a PP out of a set of PPs and PP-Modules.

- 1036 16 Therefore, unless stated otherwise, a PP denotes either a standard PP that is de-
 1037 fined without making use of the configuration operation or a PP-Configuration.

1038 **2.3.2 Protection Profiles**

1039 *(completes [CC-1-WD2]§8.2.5: introduces PP Assurance Level)*

- 1040 17 A standard PP of demonstrable or strict conformance must define its Assurance
 1041 Level (AL), i.e. the set of SAR that applies to the entire TOE.

- 1042 • If the **PP AL** is an (augmented) predefined EAL (EAL1 to EAL7) or an
 1043 (augmented) assurance package defined in an applicable external refer-
 1044 ence, then the same name should be used.

- 1045 • Otherwise a new **name** must be provided for the PP AL.

1046 **2.3.3 PP-Modules**

1047 *(completes [CC-1-WD2]§8.3.3: introduces PP-Module conformance type, PP-Module AL and*
 1048 *rationale)*

- 1049 18 A PP-Module must declare its **conformance type**, which must be one of demon-
 1050 strable, strict or exact:

- 1051 • For demonstrable and strict conformance, there is no restriction on the
 1052 conformance type of the base PPs. The combination of demonstrable and
 1053 strict conformance, must be solved in the PP-Configuration evaluation.
 1054 The combination of exact with other types of conformance is not allowed.

- 1055 • For exact conformance, the base PPs must all declare exact conformance
 1056 type.

- 1057 19 Note: such explicit declaration of demonstrable or strict conformance allows
 1058 sponsors to make the most appropriate statement in each PP-Module.

- 1059 20 A PP-Module of demonstrable or strict conformance must define its AL, i.e. the
 1060 set of SAR that applies to the part of the TOE that is introduced in the PP-Module
 1061 and the name given to it:

- 1062 • If the **PP-Module AL** is an (augmented) predefined EAL (EAL1 to
 1063 EAL7) or an (augmented) assurance package defined in an applicable ex-
 1064 ternal reference, then the same name should be used.

- 1065 • Otherwise a new **name** must be provided for the PP-Module AL.
- 1066 21 A PP-Module of demonstrable or strict conformance must provide an **AL rationale** that justifies
- 1067
- 1068 • the adequacy of the PP-Module AL with regard to the underlying threat
- 1069 model as defined in the SPD, and
- 1070 • the consistency of the PP-Module AL with all the base PP ALs that are
- 1071 different from the PP-Module AL, if any.
- 1072 22 Note: The PP-Module AL rationale contributes to ensuring that using multiple
- 1073 assurance levels does not undermine the security expected for the assets that are
- 1074 shared between the PP-Module and the base PPs (if shared assets exist).
- 1075 **2.3.4 PP-Configurations**
- 1076 *(completes [CC-1-WD2]§8.3.4.1: updates PP-Configuration multi-conformance type and con-*
- 1077 *figuration statement, introduces PP-Configuration AL and rationale)*
- 1078 23 A PP-Configuration must define a **components list** that uniquely identifies all the
- 1079 PPs and PP-Modules that compose the PP-Configuration. A PP-Configuration
- 1080 must contain two or more components and one of the components must be a PP.
- 1081 24 Note: Recall that PP denotes a standard PP or a PP-Configuration; that is, the
- 1082 components list may include PP-Configurations as well. Alternatively, the PP-
- 1083 Configuration may unfold all the component PP-Configurations and include only
- 1084 standard PPs and PP-Modules.
- 1085 25 A PP-Configuration must declare its conformance type, which must be one of
- 1086 demonstrable, strict, exact or **multiple** conformance:
- 1087 • For demonstrable, strict or exact conformance, all the components of the
- 1088 PP-Configuration must declare the same conformance type, i.e. demon-
- 1089 strable, strict or exact conformance type, respectively.
- 1090 • For multiple conformance, the PP-Configuration must provide the list of
- 1091 demonstrable and strict conformance types inherited from each its compo-
- 1092 nents. This type of conformance is meaningful when the PP-Configuration
- 1093 contain both demonstrable components and strict components. The com-
- 1094 bination of demonstrable and strict conformance, must be solved in the ST
- 1095 evaluation. The combination of exact with other types of conformance is
- 1096 not allowed.
- 1097 26 A PP-Configuration of demonstrable, strict or multiple conformance must define
- 1098 the **PP-Configuration AL**, which consists of:
- 1099 • The set of PP ALs and PP-Modules ALs inherited from the PPs and PP-
- 1100 Modules that transitively belong to the PP-Configuration, possibly aug-
- 1101 mented.

- 1102 • The global AL, i.e. the set of SARs that applies to the entire TOE. This
- 1103 can be an (augmented) predefined EAL (EAL1 to EAL7), an (augmented)
- 1104 assurance package defined in an applicable external reference or an assur-
- 1105 ance package defined within the PP-Configuration.

1106 27 The PP-Configuration AL must carry a new distinctive **name**, unless the global

1107 AL and the component ALs are all identical to the same (augmented) predefined

1108 EAL (EAL1 to EAL7) or (augmented) assurance package defined in an applicable

1109 external reference.

1110 Editor's Note: Whether the global Assurance Level of a PP-Configuration should

1111 include a predefined EAL requires expert discussion.

1112 28 A PP-Configuration of demonstrable, strict or multiple conformance must provide

1113 an **AL rationale** that justifies

- 1114 • The adequacy of the global AL with regard to the threat models as defined
- 1115 in the components' SPD, and
- 1116 • The consistency of the global AL and all the component ALs with each
- 1117 other

1118 29 Note: The PP-Configuration AL rationale contributes to ensuring that using mul-

1119 tiple assurance levels does not undermine the security expected for the assets that

1120 are shared between the PPs and PP-Modules that compose the PP-Configuration.

1121 The PP-Configuration AL rationale should rely on the PP-Modules AL rationales.

1122 2.3.5 Usage of PPs and PP-Configurations in Security Targets

1123 *(completes [CC-I-WD2]§8.2.6 and 8.3.4.2. In fact, all the usage clauses should be put*

1124 *together in the same new clause 8.4)*

1125 30 A Security Target may claim conformance with one or more PPs and PP-

1126 Configurations, thereby complying with their conformance types. The combina-

1127 tion of demonstrable and strict conformance must be solved in the ST evaluation.

1128 The combination of exact conformance with other conformance types is not al-

1129 lowed, i.e. an ST cannot claim conformance to an exact PP and to a demonstrable

1130 or strict PP.

1131 31 A Security Target that claims conformance with one or more PPs or PP-

1132 Configurations of demonstrable, strict or multiple conformance type must define

1133 the **ST AL**, which consists of:

- 1134 • The set of PP ALs and PP-Modules ALs inherited from the PPs and PP-
- 1135 Configurations the ST claims conformance with, possibly augmented.
- 1136 • The global AL, i.e. the set of SARs that applies to the entire TOE. This
- 1137 can be an (augmented) predefined EAL (EAL1 to EAL7), an (augmented)
- 1138 assurance package defined in an applicable external reference or an assur-
- 1139 ance package defined within the ST.

1140 32 The ST AL must carry a new distinctive **name**, unless

- 1141 • The global AL and the component ALs are all identical to the same (aug-
1142 mented) predefined EAL (EAL1 to EAL7) or (augmented) assurance
1143 package defined in an applicable external reference.
- 1144 • The ST conforms with a standard PP only, and the global ST AL is identi-
1145 cal to the PP AL.
- 1146 • The ST conforms with a PP-Configuration only, and the ST AL is identi-
1147 cal to the PP-Configuration AL.

1148 Editor's Note: Whether the global Assurance Level of an ST should include a
1149 predefined EAL requires expert discussion.

1150 33 A Security Target that defines an ST AL must provide an **AL rationale** that justi-
1151 fies

- 1152 • The adequacy of the global AL with regard to the threat model as defined
1153 in the SPD, and
- 1154 • The consistency of the global AL and all the component ALs with each
1155 other

1156 34 Note: The ST AL rationale contributes to ensuring that using multiple assurance
1157 levels does not undermine the security expected for the ST's assets that are shared
1158 with the PPs and PP-Configurations to which the ST claims conformance with.
1159 The ST AL rationale should rely on the PP-Configurations AL and PP-Modules
1160 AL rationales.

1161 35 Note: If the ST global AL is simply the lowest of the components ALs, then the
1162 consistency holds implicitly and does not require a rationale.

1163 2.4 Evaluation and evaluation results

1164 2.4.1 Conformance claims

1165 *(completes [CC-1]§10.3)*

1166 Editor's Note: In fact, this clause should be merged with the description of PPs or merged
1167 with the annex. The [CC-1-WD2] has a lot of redundancy. The supplementary descrip-
1168 tions necessary for multi-assurance will be provided once the corresponding section of
1169 ISO 15408 has been revised to remove the redundancy.

1170 2.4.2 Evaluation of PPs and PP-Configurations

1171 *(completes [CC-1]§10.4)*

1172 36 For a multi-assurance PP-Configuration, the ACE requirements ensure that the
1173 combination of different ALs does not undermine the expected security level of
1174 the underlying assets, as defined in the SPDs of the component PPs and PP-
1175 Modules.

1176 2.4.3 Evaluation of STs and TOEs

1177 *(completes [CC-1]§10.5)*

1178 37 For a multi-assurance ST, the ASE requirements ensure that

- 1179 • The combination of different ALs does not undermine the expected security level of the underlying assets, as defined in the SPD.
- 1180
- 1181 • Each AL belonging to the ST AL is mapped to a well-defined set of SFRs.

1182 2.5 Annex A – Specification of STs

1183 Editor's Note: this section is to be completed (as in section 2.2 above), once the corresponding section of ISO 15408 is stable.

1184

1185 2.6 Annex B – Specification of PPs

1186 Editor's Note: this section is to be completed (as in section 2.3 above), once the corresponding section of ISO 15408 is stable.

1187

1188 ISO/EC 15408-3 update

1189 2.7 Overview

1190 38 This section presents the update of classes ACE, APE and ASE to address multi-assurance evaluation framework.

1191

1192 39 The document [CC-3-CD1] has been used.

1193 40 The notation is as follows:

- 1194 • *Text in italics* comes from [CC-3-CD1]
- 1195 • ~~*Text in italics*~~ must be removed
- 1196 • Standard text is new text to be included in CC-3
- 1197 d) In this version of the document, the indications for the CEM are attached
- 1198 to the statement of the component.

1199 2.8 Class ACE

1200 2.8.1 Introduction

1201 (*completes [CC-3]§8.1*)

1202 41 The evaluator shall decide the order in which the unevaluated components of a PP-Configuration (PPs and PP-Modules) are evaluated. Class APE addresses the evaluation of PPs. The present class ACE defines the requirements for

1203

1204

- 1205 • Evaluating PP-Modules under the assumption that its basis is internally consistent.
- 1206
- 1207 • Evaluating the consistency of the combination of all the PPs and PP-Modules that transitively belong to the PP-Configurations.
- 1208
- 1209

1210 42 Note: Two PP-Modules may define each other in their basis, which means that a PP-Configuration that contains one of them also contains the other.

1211

1212 2.8.2 ACE_INT.1

1213 43 Objectives

1214 44 *The objective of this family is to describe the TOE in a narrative way.*

1215	45	<i>The evaluation of the PP-Module introduction is required to demonstrate that the</i>
1216		<i>PP-Module is correctly identified, and that the PP-Module reference and TOE</i>
1217		<i>overview are consistent with each other.</i>
1218	46	ACE_INT.1 PP-Module introduction
1219	47	<i>Dependencies: No dependencies.</i>
1220	48	<i>Application notes: All content and presentation elements of APE_INT.1 hold.</i>
1221	49	<u>Developer action elements</u>
1222	50	<i>ACE_INT.1.1D</i>
1223		<ul style="list-style-type: none"> • <i>The developer shall provide a PP-Module introduction.</i>
1224	51	<u>Content and presentation elements</u>
1225	52	(new) ACE_INT.1.xC
1226		<ul style="list-style-type: none"> • The PP-Module introduction shall meet the content and presentation re-
1227		quirements for PP introduction as defined in APE_INT.1.1C to
1228		APE_INT.1.5C.
1229	53	<i>ACE_INT.1.1C</i>
1230		<ul style="list-style-type: none"> • <i>The PP-Module introduction shall uniquely identify all the Base-PPs on</i>
1231		<i>which the PP-Module relies, including their logical structuring and rela-</i>
1232		<i>tionship to the PP-Module according to ISO/IEC 15408-1 Part 1, section</i>
1233		<i>13.3.2.</i>
1234		<ul style="list-style-type: none"> • (modified) The PP-Module introduction shall uniquely identify the base
1235		PPs and PP-Modules it depends on.
1236	54	(new) ACE_INT.1.xC
1237		<ul style="list-style-type: none"> • The PP-Module introduction shall describe the dependency structure of the
1238		base PPs and PP-Modules.
1239	55	<i>ACE_INT.1.2C</i>
1240		<ul style="list-style-type: none"> • <i>The TOE overview shall identify the differences introduced by the PP-</i>
1241		<i>Module with respect to the TOE overview of its Base-PP(s).</i>
1242		<ul style="list-style-type: none"> • (modified) The TOE overview shall describe the differences of the TOE
1243		with regard to the TOEs defined in the base PPs and PP-Modules.
1244	56	<u>Evaluator action elements</u>
1245	57	<i>ACE_INT.1.1E</i>
1246		<ul style="list-style-type: none"> • <i>The evaluator shall confirm that the information provided meets all re-</i>
1247		<i>quirements for content and presentation of evidence.</i>
1248	2.8.3	ACE_CCL.1
1249	58	<u>Objectives</u>

- 1250 59 ~~The objective of this family is to determine the validity of the conformance claim.~~
 1251 ~~Unlike standard Protection Profiles, a PP-Module cannot claim conformance to~~
 1252 ~~another PP or PP-Module, nor to CC part 3 or any SAR package.~~
- 1253 60 The objective of this family is to determine the validity of the conformance claim
 1254 and conformance statement. Unlike standard Protection Profiles, a PP-Module can-
 1255 not claim conformance to another PP or PP-Module.
- 1256 61 **ACE_CCL.1 PP-Module conformance claims**
- 1257 62 *Dependencies: ACE_INT.1 PP-Module introduction*
- 1258 63 *ACE_ECD.1 PP-Module extended components definition*
- 1259 64 *ACE_REQ.1 PP-Module security requirements*
- 1260 65 Application note: All content and presentation elements of APE_CCL.1 hold, ex-
 1261 cept the requirements about conformance to a PP.
- 1262 66 Developer action elements
- 1263 67 *ACE_CCL.1.1D*
- 1264 • The developer shall provide a conformance claim.
- 1265 68 *ACE_CCL.1.2D*
- 1266 • The developer shall provide a conformance statement.
- 1267 69 Content and presentation elements
- 1268 70 (new) **ACE_CCL.1.xC**
- 1269 • The PP-Module conformance claim shall meet the content and presenta-
 1270 tion requirements for PP conformance claim as defined in APE_CCL.1.1C
 1271 to APE_INT.1.4C and APE_CCL.1.6C
- 1272 Remark: this allows to remove 1.1C, 1.2C, 1.4C, 1.6C
- 1273 71 (new) **ACE_CCL.1.xC**
- 1274 • The PP-Module conformance statement shall meet the content require-
 1275 ments for PP conformance statement as defined in APE_CCL.1.10C to
 1276 APE_INT.1.13C.
- 1277 Remark: This allows to remove 1.5C
- 1278 72 (new) **ACE_CCL.1.xC**
- 1279 • If the PP-Module is one of demonstrable or strict conformance type, then
 1280 the conformance claim shall define the PP-Module AL's name and con-
 1281 tent, i.e. the set of SARs that applies to the TOE.
- 1282 • CEM:
- 1283 • The following applies to PP-Modules which are one of demon-
 1284 strable or strict conformance.

1285		• The evaluator shall check that PP-Module AL is given a distinctive name.
1286		
1287		• The name may not be a new name if the PP-Module AL is identical to an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package.
1288		
1289		
1290	73	<i>ACE_CCL.1.3C</i>
1291		• The conformance claim shall identify all security functional requirement packages to which the PP-Module claims conformance.
1292		
1293		• (modified) The conformance claim shall identify all security requirement packages to which the PP-Module claims conformance.
1294		
1295	74	<i>ACE_CCL.1.1C</i>
1296		• The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the PP-Module claims conformance.
1297		
1298	75	<i>ACE_CCL.1.2C</i>
1299		• The CC conformance claim shall describe the conformance of the PP-Module to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
1300		
1301		
1302	76	<i>ACE_CCL.1.4C</i>
1303		• The CC conformance claim shall be consistent with the extended components definition.
1304		
1305	77	<i>ACE_CCL.1.5C</i>
1306		• The conformance statement shall identify other PP-modules (if any) and PPs (that are not Base-PPs for the PP-Module under evaluation) that, in combination with the module under evaluation, can be used in a PP configuration.
1307		
1308		
1309		
1310	78	<i>ACE_CCL.1.6C</i>
1311		• The conformance claim shall describe any conformance of the PP to a package as either package conformant or package augmented.
1312		
1313	79	<u>Evaluator action elements</u>
1314	80	<i>ACE_CCL.1.1E</i>
1315		• The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
1316		
1317	2.8.4	ACE_SPD.1
1318	81	ACE_SPD.1 PP-Module Security problem definition
1319	82	<i>Dependencies: No dependencies.</i>
1320	83	<i>Application notes</i>

1321	84	<i>All content and presentation elements of APE_SPD.1 hold.</i>
1322	85	<u>Developer action elements</u>
1323	86	(new) ACE_SPD.1.1D
1324		<ul style="list-style-type: none"> The developer shall provide a security problem definition.
1325	87	<u>Content and presentation elements</u>
1326	88	(new) ACE_SPD.1.1C
1327		<ul style="list-style-type: none"> The PP-Module security problem definition shall meet the content and presentation requirements for PP security problem definition as defined in APE_SPD.1.1C to APE_SPD.1.4C.
1328		
1329		
1330	89	<u>Evaluator action elements</u>
1331	90	(new) ACE_SPD.1.1E
1332		<ul style="list-style-type: none"> The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
1333		
1334	2.8.5	ACE_OBJ.1
1335	91	ACE_OBJ.1 Direct Rationale PP-Module Security objectives
1336	92	<i>Dependencies: No dependencies.</i>
1337	93	<i>Application notes</i>
1338	94	<i>If the PP-Configuration uses the Direct Rationale approach (as determined in ACE_CCO.1-2) then all actions of APE_OBJ.1.1E hold, otherwise all content and presentation elements of APE_OBJ.2 hold.</i>
1339		
1340		
1341	95	If the PP-Module uses the Direct Rationale approach (as determined in ACE_CCO.1-2) then all the content and presentation elements of APE_OBJ.1.1C hold.
1342		
1343		
1344	96	<u>Developer action elements</u>
1345	97	(new) ACE_OBJ.1.1D
1346		<ul style="list-style-type: none"> The developer shall provide a statement of security objectives for the environment.
1347		
1348	98	<u>Content and presentation elements</u>
1349	99	(new) ACE_OBJ.1.1C
1350		<ul style="list-style-type: none"> The Direct Rationale PP-Module security objectives shall meet the content and presentation requirements for Direct Rationale PP security objectives as defined in APE_OBJ.1.1C.
1351		
1352		
1353		<ul style="list-style-type: none"> Note: Recall that in the Direct Rationale approach the traceability of the objectives to the SPD is not applicable.
1354		
1355	100	<u>Evaluator action elements</u>

1356	101	(new) ACE_OBJ.1.1E
1357		• The evaluator shall confirm that the information provided meets all re-
1358		quirements for content and presentation of evidence.
1359	2.8.6	ACE_OBJ.2
1360	102	ACE_OBJ.2 PP-Module Security objectives
1361	103	Dependencies: No dependencies.
1362	104	Application notes
1363	105	If the PP-Module does not use the Direct Rationale approach (as determined in
1364		ACE_CCO.1-2) then all content and presentation elements of APE_OBJ.2 hold.
1365	106	<u>Developer action elements</u>
1366	107	(new) ACE_OBJ.2.1D
1367		• The developer shall provide a statement of security objectives.
1368	108	(new) APE_OBJ.2.2D
1369		• The developer shall provide a security objectives rationale.
1370	109	<u>Content and presentation elements</u>
1371	110	(new) ACE_OBJ.2.1C
1372		• The PP-Module security objectives and rationale shall meet the content
1373		and presentation requirements for PP security objectives and rationale as
1374		defined in APE_OBJ.2.1C to APE_OBJ.2.6C.
1375	111	<u>Evaluator action elements</u>
1376	112	(new) ACE_OBJ.2.1E
1377		• The evaluator shall confirm that the information provided meets all re-
1378		quirements for content and presentation of evidence.
1379	2.8.7	ACE_ECD.1
1380	113	<u>Objectives</u>
1381	114	<i>Extended security requirements are requirements that are not based on compo-</i>
1382		<i>nents from ISO/IEC 15408-2 or this part of ISO/IEC 15408, but are based on ex-</i>
1383		<i>tended components: components defined by the PP author.</i>
1384	115	<i>Evaluation of the definition of extended components is necessary to determine that</i>
1385		<i>they are clear and unambiguous, and that they are necessary, i.e. they may not be</i>
1386		<i>clearly expressed using existing ISO/IEC 15408-2 or this part of ISO/IEC 15408</i>
1387		<i>components.</i>
1388	116	APE_ECD.1 Extended components definition
1389	117	<i>Dependencies: No dependencies.</i>
1390	118	Application notes

- 1391 119 All the actions, content and presentation elements of APE_ECD.2 hold.
- 1392 120 Developer action elements
- 1393 121 *ACE_ECD.1.1D*
- 1394 • ~~The developer shall provide a statement of security functional require-~~
1395 ~~ments.~~
- 1396 • (modified) The developer shall provide a statement of security require-
1397 ~~ments.~~
- 1398 122 *ACE_ECD.1.2D*
- 1399 • ~~The developer shall provide an extended functional components defini-~~
1400 ~~tion.~~
- 1401 • (modified) The developer shall provide an extended components defini-
1402 ~~tion.~~
- 1403 123 Content and presentation elements
- 1404 124 (new) **ACE_ECD.1.1C**
- 1405 • The statement of security requirements and the extended components defi-
1406 ~~nition shall meet the content and presentation requirements for PP state-~~
1407 ~~ment of security requirements and the extended components definition as~~
1408 ~~defined in APE_ECD.1.1C to APE_ECD.1.5C.~~
- 1409 • Editor's Note: This allows removing old ACE_ECD.1.1C to
1410 ACE_ECD.1.5C, which apply only to security functional requirements. In
1411 the multi-assurance framework, the PP-Modules can define extended
1412 SARs as well.
- 1413 125 ~~ACE_ECD.1.1C~~
- 1414 • ~~The statement of security functional requirements shall identify all extend-~~
1415 ~~ed security functional requirements.~~
- 1416 126 ~~ACE_ECD.1.2C~~
- 1417 • ~~The extended functional components definition shall define an extended~~
1418 ~~functional component for each extended security functional requirement.~~
- 1419 127 ~~ACE_ECD.1.3C~~
- 1420 • ~~The extended functional components definition shall describe how each ex-~~
1421 ~~tended functional component is related to the existing CC Part 2 compo-~~
1422 ~~nents, families, and classes.~~
- 1423 128 ~~ACE_ECD.1.4C~~
- 1424 • ~~The extended functional components definition shall use the existing CC~~
1425 ~~Part 2 components, families, classes, and methodology as a model for~~
1426 ~~presentation.~~

1427	129	ACE_ECD.1.5C
1428		• The extended functional components shall consist of measurable and ob-
1429		jective elements such that conformance or nonconformance to these ele-
1430		ments can be demonstrated.
1431	130	<u>Evaluator action elements</u>
1432	131	APE_ECD.1.1E
1433		• The evaluator shall confirm that the information provided meets all re-
1434		quirements for content and presentation of evidence.
1435	132	APE_ECD.1.2E
1436		• The evaluator shall confirm that no extended component may be clearly
1437		expressed using existing components.
1438		
1439	2.8.8	ACE_REQ.1 & 2
1440	133	<u>Objectives</u>
1441	134	The SFRs form a clear, unambiguous and well-defined description of the expected
1442		security behaviour of the TOE.
1443	135	Evaluation of the security functional requirements is required to ensure that they
1444		are clear, unambiguous and well-defined.
1445	136	The SFRs form a clear, unambiguous and well-defined description of the expected
1446		security behaviour of the TOE. The SARs form a clear, unambiguous and well-
1447		defined description of the expected activities that will be undertaken to gain as-
1448		surance in the TOE.
1449	137	Evaluation of the security requirements is required to ensure that they are clear,
1450		unambiguous and well-defined.
1451	138	<u>Component levelling</u>
1452	139	The components in this family are levelled on whether they are stated as is, or
1453		whether the SFRs are derived from security objectives for the TOE.
1454	2.8.9	ACE_REQ.1
1455	140	ACE_REQ.1 PP-Module stated security requirements
1456	141	<i>Dependencies: APE_ECD.1 Extended components definition</i>
1457	142	Application notes
1458	143	All the actions, content and presentation elements of APE_REQ.1 hold.
1459	144	<u>Developer action elements</u>
1460	145	ACE_REQ.1.1D
1461		• The developer shall provide a statement of security requirements.
1462	146	ACE_REQ.1.2D

- 1463 • *The developer shall provide a security requirements rationale.*

1464 147 Content and presentation elements

1465 148 (new) **ACE_REQ.1.1C**

- 1466 • The statement of security requirements and the rationale shall meet the
1467 content and presentation requirements for PP statement of security re-
1468 quirements and rationale as defined in APE_REQ.1.1C to
1469 APE_REQ.1.12C.

1470 Editor's Note: This allows removing old ACE_REQ.1.1C to
1471 ACE_REQ.1.12C, which apply only to SFRs. In the multi-assurance
1472 framework, the PP-Modules can define SARs as well.

1473 149 ~~ACE_REQ.1.1C~~

- 1474 • ~~The statement of security requirements shall describe the SFRs that hold~~
1475 ~~on the TOE.~~

1476 150 ~~ACE_REQ.1.2C~~

- 1477 • ~~All subjects, objects, operations, security attributes, external entities and~~
1478 ~~other terms that are used in the SFRs shall be defined.~~

1479 151 ~~ACE_REQ.1.3C~~

- 1480 • ~~The statement of security requirements shall include a natural language~~
1481 ~~description, part of which describes how the SFRs combine together to~~
1482 ~~provide security functionality in terms of the architecture that is visible to~~
1483 ~~Administrators and other users.~~

1484 152 ~~ACE_REQ.1.4C~~

- 1485 • ~~The statement of security requirements shall identify all operations on the~~
1486 ~~security requirements.~~

1487 153 ~~ACE_REQ.1.5C~~

- 1488 • ~~All operations shall be performed correctly.~~

1489 154 ~~ACE_REQ.1.6C~~

- 1490 • ~~Each dependency of the security requirements shall either be satisfied, or~~
1491 ~~the security requirements rationale shall justify the dependency not being~~
1492 ~~satisfied.~~

1493 155 ~~ACE_REQ.1.7C~~

- 1494 • ~~The security requirements rationale shall trace each SFR back to the secu-~~
1495 ~~rity objectives threats countered by that SFR and OSPs enforced by that~~
1496 ~~SFR.~~

1497 156 ~~ACE_REQ.1.8C~~

1498 • ~~The security requirements rationale shall trace each security objective for~~
 1499 ~~the operational environment back to threats countered by that security ob-~~
 1500 ~~jective, OSPs enforced by that security objective, and assumptions upheld~~
 1501 ~~by that security objective.~~

1502 157 — ~~ACE_REQ.1.9C~~

1503 • ~~The security requirements rationale shall demonstrate that the SFRs coun-~~
 1504 ~~ter all threats for the TOE.~~

1505 158 — ~~ACE_REQ.1.10C~~

1506 • ~~The security requirements rationale shall demonstrate that the SFRs en-~~
 1507 ~~force all OSPs.~~

1508 159 — ~~ACE_REQ.1.11C~~

1509 • ~~The security requirements rationale shall demonstrate that the security ob-~~
 1510 ~~jectives for the operational environment uphold all assumptions.~~

1511 160 — ~~ACE_REQ.1.12C~~

1512 • ~~The statement of security requirements shall be internally consistent.~~

1513 161 Evaluator action elements

1514 162 ~~ACE_REQ.1.1E~~

1515 • ~~The evaluator shall confirm that the information provided meets all re-~~
 1516 ~~quirements for content and presentation of evidence.~~

1517 2.8.10 ACE_REQ.2

1518 Editor's Note: We propose to remove the term "derived" from the name of
 1519 ACE_REQ.2 since the « derivation » has a very specific meaning in terms of
 1520 CEM and Part 4. See as well the note in ACE_REQ.1

1521 163 **ACE_REQ.2 PP-Module ~~derived~~ security ~~functional~~ requirements**

1522 164 Dependencies: ~~ACE_ECD.1 PP-Module extended components definition~~

1523 165 ~~ACE_OBJ.1 PP-Module Security objectives~~

1524 166 Application notes

1525 167 All the actions, content and presentation elements of APE_REQ.2 hold.

1526 168 Developer action elements

1527 169 ~~ACE_REQ.2.1D~~

1528 • ~~The developer shall provide a statement of security functional require-~~
 1529 ~~ments.~~

1530 • (modified) The developer shall provide a statement of security require-

1531 ments.

1532 170 ~~ACE_REQ.2.2D~~

- 1533 • ~~The developer shall provide a security functional requirement rationale.~~
- 1534 • (modified) The developer shall provide a security requirements rationale.
- 1535 171 Content and presentation elements
- 1536 172 (new) **ACE_REQ.2.1C**
- 1537 • The statement of security requirements and the rationale shall meet the
- 1538 content and presentation requirements for PP statement of security re-
- 1539 quirements and rationale as defined in APE_REQ.2.1C to
- 1540 APE_REQ.1.15C.
- 1541 Editor's Note: This allows removing old ACE_REQ.2.1C to

1542 ACE_REQ.2.12C, which apply only to SFRs. In the multi-assurance

1543 framework, the PP-Modules can define SARs as well.
- 1544 173 ~~ACE_REQ.2.1C~~
- 1545 • ~~The statement of security functional requirements shall describe the SFRs~~
- 1546 ~~that hold on the TOE.~~
- 1547 174 ~~ACE_REQ.2.2C~~
- 1548 • ~~All subjects, objects, operations, security attributes, external entities and~~
- 1549 ~~other terms that are used in the SFRs shall be defined.~~
- 1550 175 ~~ACE_REQ.2.3C~~
- 1551 • ~~The statement of security requirements shall include a natural language~~
- 1552 ~~description, part of which describes how the SFRs combine together to~~
- 1553 ~~provide security functionality in terms of the architecture that is visible to~~
- 1554 ~~Administrators and other users.~~
- 1555 176 ~~ACE_REQ.2.4C~~
- 1556 • ~~The statement of security functional requirements shall identify all opera-~~
- 1557 ~~tions on the security functional requirements.~~
- 1558 177 ~~ACE_REQ.2.5C~~
- 1559 • ~~All operations shall be performed correctly.~~
- 1560 178 ~~ACE_REQ.2.6C~~
- 1561 • ~~Each dependency of the security functional requirements shall either be~~
- 1562 ~~satisfied, or the security functional requirements rationale shall justify the~~
- 1563 ~~dependency not being satisfied.~~
- 1564 179 ~~ACE_REQ.2.7C~~
- 1565 • ~~The security functional requirements rationale shall trace each SFR back~~
- 1566 ~~to the security objectives for the TOE.~~
- 1567 180 ~~ACE_REQ.2.8C~~

- 1568 • ~~The security functional requirements rationale shall trace each security~~
 1569 ~~objective for the operational environment back to threats countered by~~
 1570 ~~that security objective, OSPs enforced by that security objective, and as-~~
 1571 ~~sumptions upheld by that security objective.~~
- 1572 181 — ~~ACE_REQ.2.9C~~
- 1573 • ~~The security functional requirements rationale shall demonstrate that the~~
 1574 ~~SFRs meet all security objectives for the TOE.~~
- 1575 182 — ~~ACE_REQ.2.10C~~
- 1576 • ~~The security functional requirements rationale shall demonstrate that the~~
 1577 ~~SFRs enforce all OSPs.~~
- 1578 183 — ~~ACE_REQ.2.11C~~
- 1579 • ~~The security functional requirements rationale shall demonstrate that the~~
 1580 ~~security objectives for the operational environment uphold all assump-~~
 1581 ~~tions.~~
- 1582 184 — ~~ACE_REQ.2.12C~~
- 1583 • ~~The statement of security functional requirements shall be internally con-~~
 1584 ~~sistent.~~
- 1585 185 Evaluator action elements
- 1586 186 ~~ACE_REQ.2.1E~~
- 1587 • ~~The evaluator shall confirm that the information provided meets all re-~~
 1588 ~~quirements for content and presentation of evidence.~~
- 1589 **2.8.11 ACE_MCO**
- 1590 187 Objectives
- 1591 188 — ~~The objective of this family is to determine the validity of the PP-Module.~~
- 1592 189 The objective of this family is to determine the consistency of the PP-Module.
- 1593 190 ~~ACE_MCO.1 PP-Module consistency~~
- 1594 191 ~~Dependencies: ACE_INT.1 PP-Module introduction~~
- 1595 192 ~~ACE_SPD.1 PP-Module Security problem definition~~
- 1596 193 ~~ACE_OBJ.1 Direct Rationale PP-Module Security objectives~~
- 1597 194 ~~ACE_REQ.1 PP-Module stated security requirements~~
- 1598 195 Developer action elements
- 1599 196 ~~ACE_MCO.1.1D~~

- 1600 • ~~The developer shall provide a consistency rationale of the PP-Module with~~
 1601 ~~respect to its Base-PP(s) identified in the PP-Module introduction. If the~~
 1602 ~~PP-Module specifies alternate sets of Base-PPs, the developer shall pro-~~
 1603 ~~vide as many consistency rationales as the number of alternate sets of~~
 1604 ~~Base-PPs.~~
- 1605 • (modified) The developer shall provide a consistency rationale of the PP-
 1606 Module for each of the alternative sets of base PPs and PP-Modules identi-
 1607 fied in the PP-Module introduction.
- 1608 197 Content and presentation elements
- 1609 198 ACE_MCO.1.1C
- 1610 • ~~The consistency rationale shall demonstrate that the TOE type of the PP-~~
 1611 ~~Module is consistent with the TOE type(s) in the Base-PPs identified in the~~
 1612 ~~PP-Module introduction.~~
- 1613 • (modified) The consistency rationale shall demonstrate that the TOE type
 1614 of the PP-Module and its base PPs and PP-Modules are consistent.
- 1615 199 (new) **ACE_MCO.1.xC**
- 1616 • The consistency rationale shall identify the assets of the PP-Module that
 1617 also belong to one or more base PP or PP-Module and amongst them those
 1618 for which the PP-Module and the base PP and PP-Modules define differ-
 1619 ent security problems.
- 1620 Editor's Note: this is also meaningful for APE and ASE when the ST
 1621 claims conformance to more than one PP or when the ST adds elements to
 1622 the PPs it conforms to: The change has not been proposed yet in
 1623 ASE/APE, but if experts agree, we suggest cascading this change in the
 1624 next CD.
- 1625 • CEM:
- 1626 • The evaluator shall check that the consistency rationale contains
 1627 the set of assets shared between the PP-Module and its base PP
 1628 and PP-Modules, and that this set is unambiguous and complete.
- 1629 • The evaluator shall check that the consistency rationale contains
 1630 the subset of shared assets that hold different security properties
 1631 and/or are subject to different threat agents or threats scenarios,
 1632 and that this subset is unambiguous and complete.
- 1633 200 ACE_MCO.1.2C
- 1634 • ~~The consistency rationale shall demonstrate that the statement of the secu-~~
 1635 ~~rity problem definition is consistent with the statement of the security~~
 1636 ~~problem definition in the Base-PPs identified in the PP-Module introduc-~~
 1637 ~~tion.~~

- 1638 • (modified) The consistency rationale shall demonstrate that the statements
 1639 of the security problem definition of the PP-Module and its base PPs and
 1640 PP-Modules are consistent.
- 1641 • CEM:
- 1642 • For all the assets that are shared between the PP-Module and one
 1643 or more base PP or PP-Module, the evaluator determines that all
 1644 the differences in the security problem definitions are justified.
 1645 For instance, the asset resides in different locations or at different
 1646 times or is subject to different operational environment condi-
 1647 tions.
- 1648 201 *ACE_MCO.1.3C*
- 1649 • ~~The consistency rationale shall demonstrate that the statement of security~~
 1650 ~~objectives is consistent with the statement of security objectives in the~~
 1651 ~~Base PPs identified in the PP-Module introduction.~~
- 1652 • (modified) The consistency rationale shall demonstrate that the statements
 1653 of the security objectives of the PP-Module and its base PPs and PP-
 1654 Modules are consistent.
- 1655 202 *ACE_MCO.1.4C*
- 1656 • ~~The consistency rationale shall demonstrate that the statement of security~~
 1657 ~~requirements is consistent with the statement of security requirements in~~
 1658 ~~the Base PPs identified in the PP-Module introduction.~~
- 1659 • (modified) The consistency rationale shall demonstrate that the statements
 1660 of the security functional requirements of the PP-Module and its base PPs
 1661 and PP-Modules are consistent.
- 1662 203 (new) **ACE_MCO.1.5C**
- 1663 • The consistency rationale shall demonstrate that the statement of the secu-
 1664 rity assurance requirements of the PP-Module is consistent with the state-
 1665 ments of the security assurance requirements in the base PPs and PP-
 1666 Modules identified in the PP-Module introduction.
- 1667 • The consistency rationale shall demonstrate that the statements of the se-
 1668 curity assurance requirements of the PP-Module and its base PPs and PP-
 1669 Modules are consistent.
- 1670 • CEM:
- 1671 • The evaluator shall check that the PP-Module does not under-
 1672 mine the expected assurance level of the assets of the base PPs
 1673 and PP-Modules.

- 1674 • If the PP-Module and a base PP or PP-Module share an as-
1675 set which is subject to an equivalent security problem in
1676 both places, then the PP-Module AL, i.e. the set of SARs, is
1677 identical to the base PP or PP-Module AL.
- 1678 • The evaluator shall check that the base PPs and PP-Modules do
1679 not undermine the expected assurance level of each other.
- 1680 • If an asset is shared by two base PPs or PP-Modules and
1681 this asset is subject to an equivalent security problem in
1682 both places, then the ALs of these PPs or PP-Modules are
1683 identical.

1684 204 Evaluator action elements

1685 205 *ACE_MCO.1.1E*

- 1686 • ~~The evaluator shall confirm that the information provided meets all re-~~
1687 ~~quirements for content and presentation of evidence. If the PP-Module~~
1688 ~~specifies alternate sets of Base PPs, the evaluator shall perform this ac-~~
1689 ~~tion for each consistency rationale with its related Base PPs in the alter-~~
1690 ~~nate set of Base PPs of the PP-Module.~~
- 1691 • (modified) The evaluator shall confirm that the information provided
1692 meets all requirements for content and presentation of evidence. If the PP-
1693 Module specifies alternate sets of base PPs and PP-Modules, the evaluator
1694 shall perform this action for each consistency rationale.

1695

1696 **2.8.12 ACE_CCO**

1697

1698 206 Objectives

1699 207 *The objective of this family is to determine the well-formedness and the consisten-*
1700 *cy of the PP-Configuration.*

1701 208 **ACE_CCO.1 PP-Configuration consistency**

1702 209 *Dependencies: APE_**

1703 210 ACE_INT.1 PP-Module introduction

1704 211 (new) ACE_CCL.1

1705 212 (new) ACE_SPD.1

1706 213 (new) ACE_OBJ.1

1707 214 (new) ACE_ECD.1

1708 215 *ACE_REQ.1 PP-Module security requirements*

1709 216 *ACE_MCO.1 PP-Module consistency*

1710 217 Developer action elements

- 1711 218 *ACE_CCO.1.1D*
- 1712 • *The developer shall provide the reference of the PP-Configuration.*
- 1713 219 *ACE_CCO.1.2D*
- 1714 ~~• The developer shall provide a components statement.~~
- 1715 • (modified) The developer shall provide a components list.
- 1716 220 *ACE_CCO.1.3D*
- 1717 ~~• The developer shall provide a conformance statement and a conformance~~
- 1718 ~~claim.~~
- 1719 • (modified) The developer shall provide a conformance claim.
- 1720 221 ~~*ACE_CCO.1.4D*~~
- 1721 ~~• The developer shall provide a SAR statement.~~
- 1722 222 (new) **ACE_CCO.1.xD**
- 1723 • The developer shall provide a conformance claim rationale.
- 1724 223 (new) **ACE_CCO.1.xD**
- 1725 • The developer shall provide a conformance statement.
- 1726 224 (new) **ACE_CCO.1.xD**
- 1727 • The developer shall provide a consistency rationale.
- 1728 225 Content and presentation elements
- 1729 226 *ACE_CCO.1.1C*
- 1730 • *The PP-Configuration reference shall uniquely identify the PP-*
- 1731 *Configuration.*
- 1732 227 *ACE_CCO.1.2C*
- 1733 ~~• The components statements shall uniquely identify the Protection Profiles~~
- 1734 ~~and the PP-Modules that compose the PP-Configuration.~~
- 1735 • (modified) The components list shall uniquely identify the PPs and PP-
- 1736 Modules that compose the PP-Configuration.
- 1737 228 *ACE_CCO.1.3C*
- 1738 ~~• The conformance statement shall specify the required conformance to the~~
- 1739 ~~PP Configuration as one of exact, strict, or demonstrable. The conform-~~
- 1740 ~~ance claim shall contain a CC conformance claim that identifies the ver-~~
- 1741 ~~sion of the CC to which the PP-Configuration and its underlying Protec-~~
- 1742 ~~tion Profile and PP-Module claim conformance.~~
- 1743 • (modified) The conformance claim shall contain a CC conformance claim
- 1744 that identifies the version(s) of the CC to which the PP-Configuration and
- 1745 its underlying Protection Profile and PP-Module claim conformance.

- 1746 • CEM:
- 1747 • The evaluator shall check there are no conflicts if more than one
- 1748 version of the CC is claimed.
- 1749 229 ACE_CCO.1.4C
- 1750 • ~~The SAR statement shall specify the set of SAR or predefined EAL that ap-~~
- 1751 ~~plies to this PP-Configuration.~~
- 1752 • (modified) If the PP-Configuration is one of demonstrable, strict or multi-
- 1753 ple conformance type, then the conformance claim shall define the PP-
- 1754 Configuration AL's name and content:
- 1755 • The set of PP ALs and PP-Modules ALs inherited from the PPs
- 1756 and PP-Modules that transitively belong to the PP-
- 1757 Configuration's components list, possibly augmented.
- 1758 • The global AL, i.e. the set of SARs that applies to the entire
- 1759 TOE.
- 1760 • CEM:
- 1761 • The following applies to PP-Configurations which are one of
- 1762 demonstrable, strict or multiple conformance.
- 1763 • The evaluator shall check that PP-Configuration AL is given a
- 1764 distinctive name.
- 1765 • The name should not be a new name if the global AL and the
- 1766 component ALs are all identical to the same (augmented) prede-
- 1767 fined EAL (EAL1 to EAL7) or (augmented) assurance package.
- 1768 • The evaluator shall check that the PP-Configuration AL contains
- 1769 all the components ALs.
- 1770 230 ACE_CCO.1.5C
- 1771 • ~~The Base PP(s) on which the PP-Modules relies shall belong to the Pro-~~
- 1772 ~~tection Profiles identified in the components statement of the PP-~~
- 1773 ~~Configuration.~~
- 1774 • (modified) For each PP-Module identified in the components list of the
- 1775 PP-Configuration, the list contains at least one of its sets of base PPs and
- 1776 PP-Modules.
- 1777 231 (new) ACE_CCO.1.xC
- 1778 • The conformance statement shall specify the required conformance to the
- 1779 PP-Configuration as one of exact, strict, demonstrable or multiple.
- 1780 • CEM:

- 1781 • For demonstrable, strict or exact conformance, the evaluator
 1782 shall check that all the PPs and PP-Modules that transitively be-
 1783 long to the components list of the PP-Configuration declare the
 1784 same conformance type, i.e. demonstrable, strict or exact con-
 1785 formance type, respectively.

1786 232 (new) **ACE_CCO.1.xC**

- 1787 • For a multiple conformance PP-Configuration, the conformance statement
 1788 shall specify the list of conformance types inherited from the PPs and PP-
 1789 Modules that transitively belong to the components list of the PP-
 1790 Configuration.
- 1791 • CEM:
- 1792 • For multiple conformance, the evaluator shall check that the list
 1793 of conformance types maps to the conformance types of the PPs
 1794 and PP-Modules that transitively belong to the components list of
 1795 the PP-Configuration.
- 1796 • The evaluator shall check that the list of conformance types con-
 1797 tain only demonstrable and strict types. The combination of exact
 1798 conformance with other types of conformance is not allowed.

1799 233 (new) **ACE_CCO.1.xC**

- 1800 • The consistency rationale shall demonstrate that the union of all the PPs
 1801 and PP-Modules that transitively belong to the PP-Configuration's com-
 1802 ponents list is consistent.
- 1803 • CEM:
- 1804 • The same evaluation units defined in ACE_MCO for PP-
 1805 Modules applies to the complete set of elements.

1806 234 Evaluator action elements

1807 235 **ACE_CCO.1.1E**

- 1808 • *The evaluator shall confirm that the information provided meets all re-*
 1809 *quirements for content and presentation of evidence.*

1810 236 **ACE_CCO.1.2E**

- 1811 • *The evaluator shall check that the PP-Configuration made up of all the Pro-*
 1812 *tection Profiles and PP-Modules identified in the components statement of*
 1813 *the PP-Configuration is consistent.*

1814 **2.9 Class APE**

1815 Editor's Note: The APE class must be extended to cover the conformity of a standard PP
 1816 with one or more PPs/PP Configurations and potentially the addition of supplementary
 1817 security problem, objectives and SFRs. The same kind of check as for PP-Modules and

1818 PP-Configurations apply. These updates will be provided once the proposed updates to
1819 the ACE class (in Section 2.8) have been agreed.

1820 **2.10 Class ASE**

1821 Editor's Note: The ASE class must be extended to cover the conformity with one or more
1822 PPs/PP Configurations and potentially the addition of supplementary security problem,
1823 objectives and SFRs. The same kind of check as for PP-Modules and PP-Configurations
1824 apply. These updates will be provided once the proposed updates to the ACE class (in
1825 Section 2.8) have been agreed.

Annex C

(informative)

Concept approach to the ISO/IEC 15408 & 18045 Terminology

1 Background

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.*”

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.

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.

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

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.

For this document relevant terms are defined as follows³:

- **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.

The systematic order requires identification of distinguished concepts and further determining terms which relate to the concept and provide necessary characteristics. The concept can have its definition, but it is not always the case. The systematic order is achieved by proper numbering in the hierarchy of terms (see Fig.1).

³ Adopted from ISO/IEC 10241-1:2011 Terminological entries in standards — Part 1: General requirements and examples of presentation

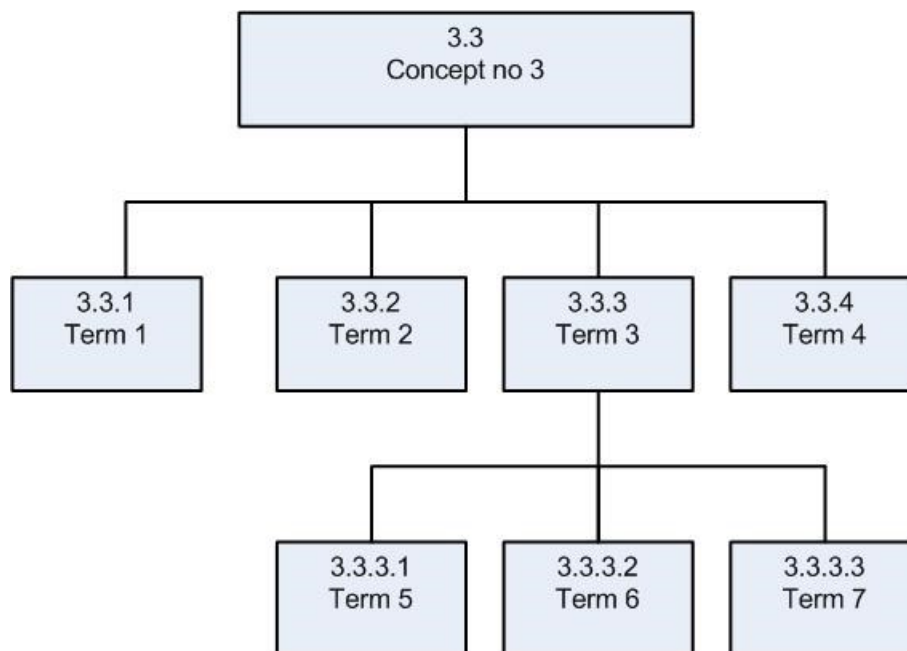


Fig. 1 Numbering of terms within the concept (example)

It is recommended⁴ to minimise the number of concepts to produce a clear picture of relationships inside one concept map and limit cross-relations between concepts.

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

- the complexity of the IT security evaluation domain which resulted in hundreds of terms, often used in a different context than usual dictionary meaning,
- deep revision of 15408 & 18045 set of standards currently underway,
- needs for opening the Common Criteria world for new users, new applications, new technologies, and new evaluation techniques, and simultaneously, legacy needs for preserving current applications (existing evaluation and certification schemes with their practices, skills and experience),
- new regulatory/ legal frameworks, like European cybersecurity certification framework⁵,

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

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

⁴ ISO/IEC 704:2009, Principles and methods

⁵ <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505737096808&uri=CELEX:52017PC0477>

- fulfil the ISO requirements for correct presentation of terms,
- clarify terms and their definitions in the ICT security evaluation context, and in consequence
 - identify and then remove from Clause 3 these terms which are not necessary to define,
 - improve current definitions (e.g. shortening them or removing circular references among several definitions).

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

2.1 General action plan (GAP) to get the objective

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

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

Thus, the action plan is formulated as follows:

- A. The limited reconstruction (the Pilot) is placed in the current draft of ISO/IEC 22216 subject to the revision by experts,
- B. Depending on the results of revision separate session/workshop could be organised at the meeting in Norway (Autumn, 2018), possibly with the help of external expert(s),
- C. Upon the editing group approval proven/validated approach would be deployed on the whole set of terms,
- D. The full reconstruction (Implementation) will appear in next version of ISO/IEC TR 22216 issued after the meeting held in Norway, again subject to the revision by experts,
- E. Housekeeping on terms and their definition is being done in parallel, and its results are mutually reflected in both documents, ISO/IEC 15408-1 Clause 3 and ISO/IEC TR 22216.

- 1918 F. Another round of review is possible before the project gets DIS stage;
 1919 G. Upon successful implementation of the concept approach, the results would be
 1920 moved to Clause 3 of ISO/IEC 15408-1 replacing alphabetically ordered set of
 1921 terms and definitions.

1922 The plan is presented in Fig. 2.

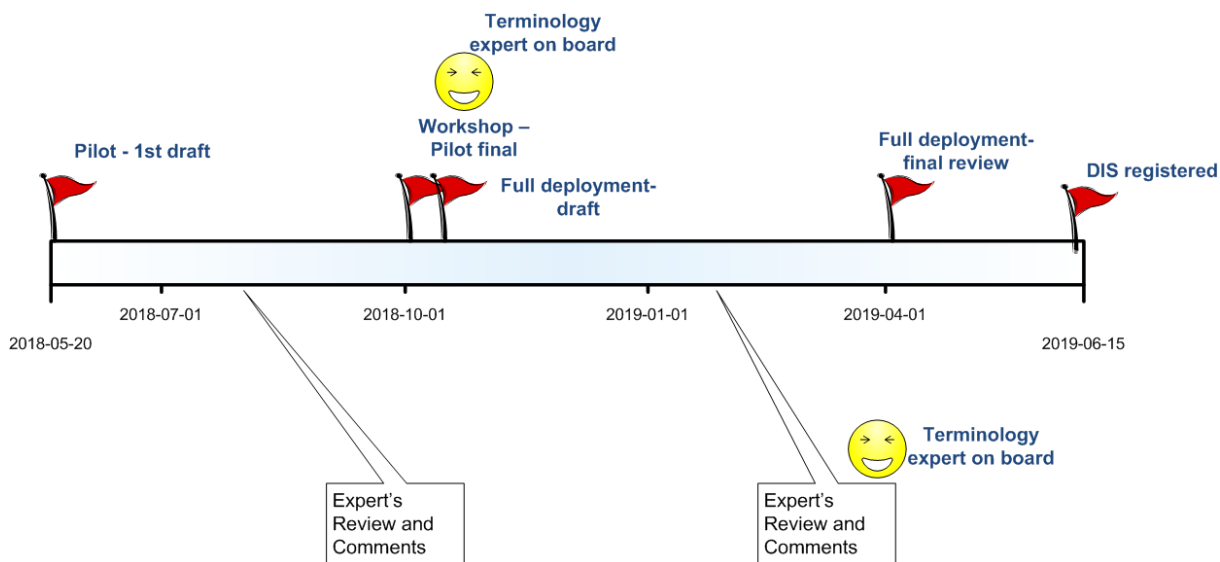


Fig. 2 The action plan timetable

1923
 1924
 1925

1926 2.2 What would be the impact of the GAP on the project timetable?

- 1927 – Minor, it does not touch the structure, not being an obstacle for progressing ISO/IEC
 1928 15408-1 to next stages (should be done unless the project reaches DIS stage),
 1929 – There is always a roll-back possibility, some not all results (e.g. at least housekeeping)
 1930 could be implemented if the adventure would not reach its all objectives.

1931 3 Identification of concepts

1932 3.1 General

1933 As a starting point (pilot) of the concept development following 5 concepts have been iden-
 1934 tified:

- 1935 1. Security model
- 1936 2. Target of Evaluation, TOE
- 1937 3. Assurance
- 1938 4. Evaluation techniques
- 1939 5. Taxonomy

1940 Relevant terms, currently included in ISO/IEC 1stCD 15408-1, have been assigned to con-
1941 cepts by analysing respective definitions. As a result, several maps of relationships between
1942 terms are presented in following subchapters. It is not claimed the maps for respective con-
1943 cepts are complete. All presented maps are subject to modification and improvements.

1944 Other terms have not been assigned yet. It is expected to provide relevant maps in the next
1945 step of the development process.

1946 Finally, there are terms recommended to remove (still subject to further consideration).

1947 The complete list of terms, their definitions and current status with regards to the concept
1948 assignments are presented in the table located at the end of this Annex.

1949 It is worth to note some maps contain not defined terms. It is not necessary the fault nor
1950 proof of incompleteness. The term is not to be defined if used in common, dictionary mean-
1951 ing however it could be indispensable for completeness of the concept map. Such terms are
1952 indicated in red font. Finally, if we have any doubt with assigning particular terms, it ap-
1953 pears in a yellow box.

1954

1955

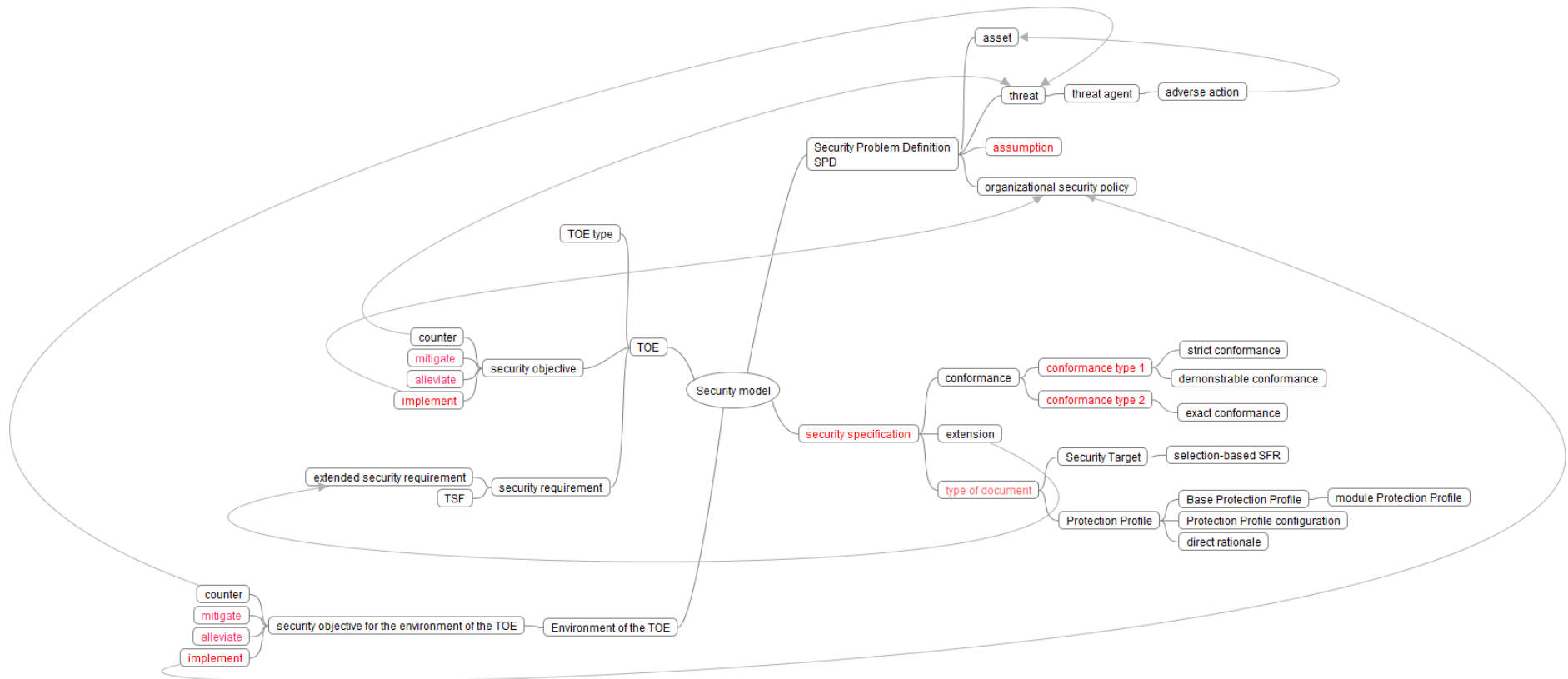
1956 **3.3 Concepts**1957 **3.3.1 Security Model**

Fig. 3 Terms related to 'security model' concept

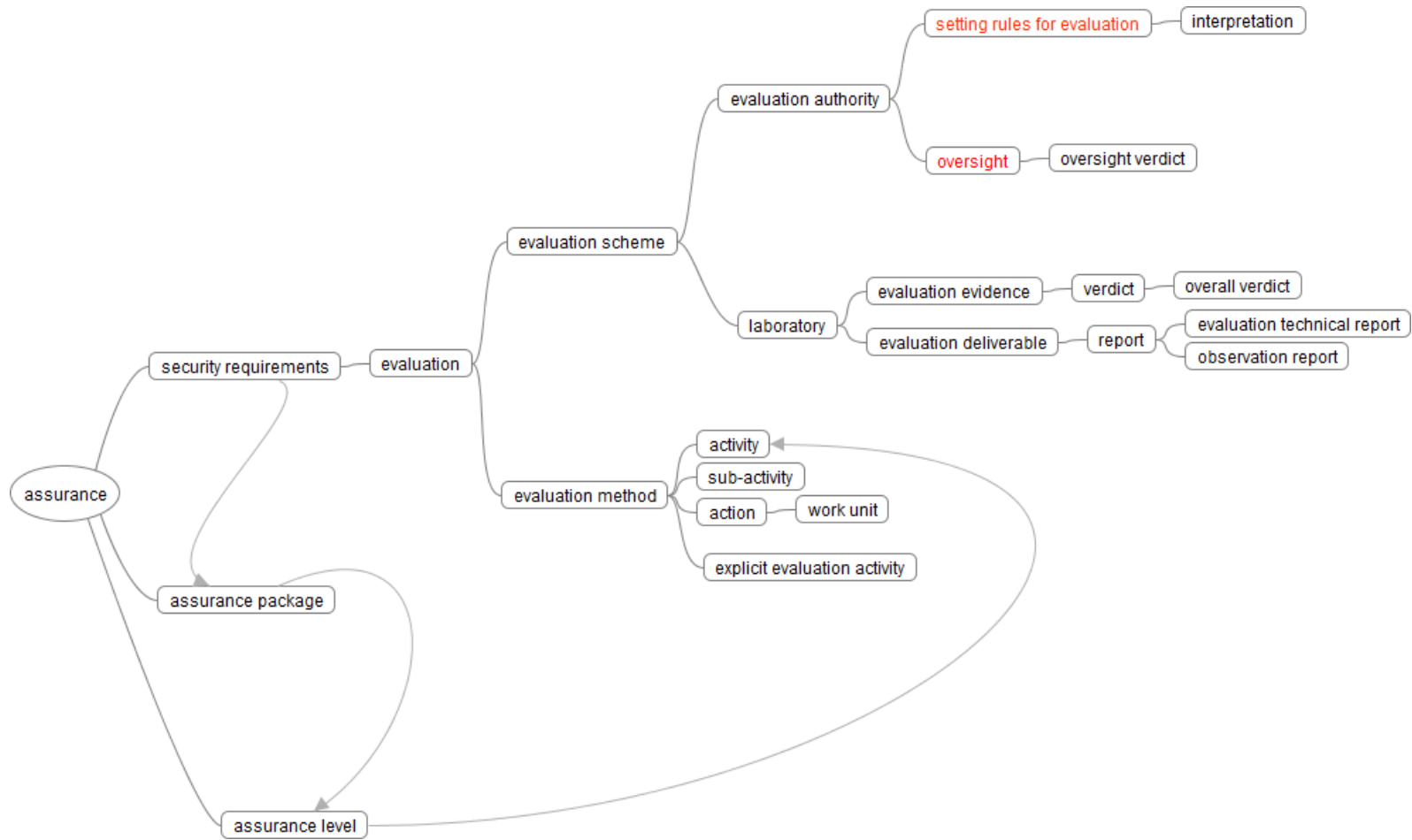
1960 **3.3.2 Assurance**

Fig. 1 Terms related to 'assurance' concept

1961
1962
1963

1964 3.3.3 Target of Evaluation, TOE

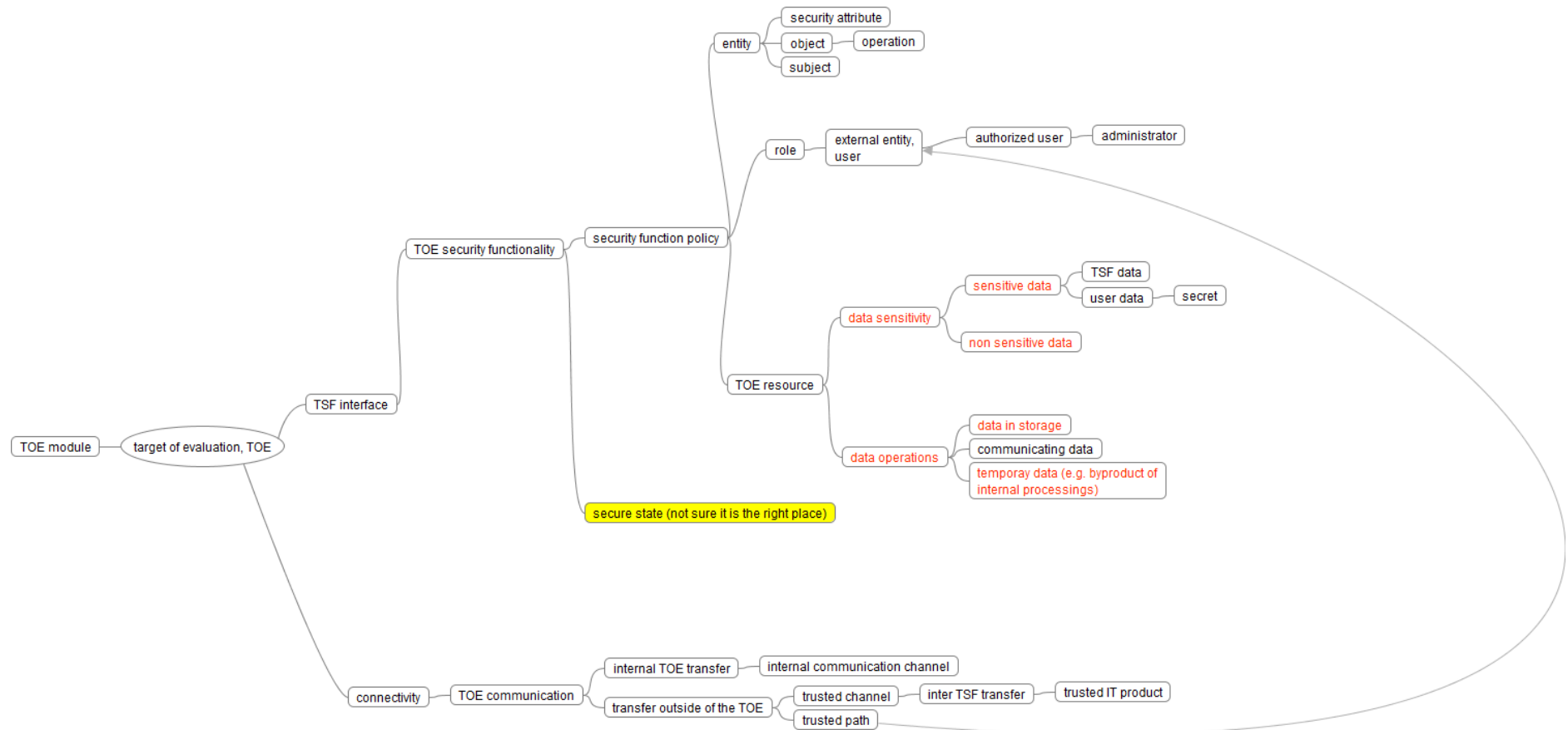


Fig. 5 Terms related to 'TOE' concept

1968 3.3.4 Evaluation techniques

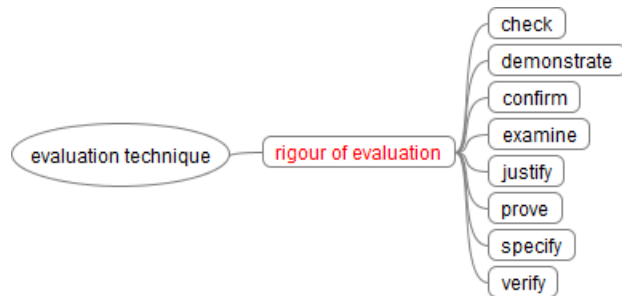


Fig. 6 Terms related to 'evaluation techniques' concept

1971 3.3.5 Taxonomy

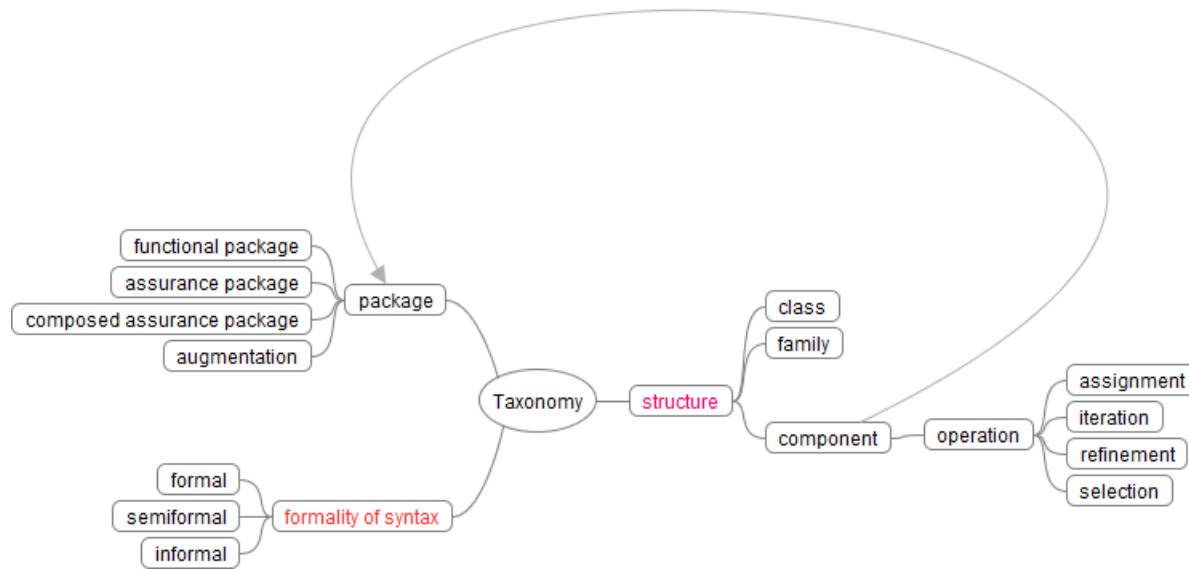


Fig. 7 Terms related to 'taxonomy' concept

1974 **4 Assignment of Terms**

1975 All terms are presented in Table 1.

1976 **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> <p>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”);</p> <p>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);</p> <p>c) subsequent to transports of configuration items (for example parts of the TOE or preliminary products) between different development sites;</p> <p>d) subsequent to the delivery of the TOE to the consumer;</p> <p>e) subsequent to the integration of the TOE.</p>	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 developmentNote 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	results, related to configuration management, produced or enforced by the configuration management system Note 1 to entry: These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviours during the product life-cycle.	not assigned yet
3.44	configuration management plan	description of how the configuration management system is used for the TOE Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.	not assigned yet
3.45	configuration management system	set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles Note 1 to entry: Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms.	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	not assigned yet
		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	
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	<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
3.85	explain	<evaluation verb> give argument accounting for the reason for taking a course of action Note 1 to entry: This term differs from both “describe” and “demonstrate”. It is intended to answer the question “Why?” without actually attempting to argue that the course of action that was taken was necessarily optimal.	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	security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408 Note 1 to entry: An extended security requirement may be either an SAR or an SFR. Note 2 to entry: Extended security requirements are defined within extended component definitions.	security model
3.88	Extended TOE	Text	not assigned yet
3.89	Extended TSF	Text	not assigned yet
3.90	external entity user	human or IT entity possibly interacting with the TOE from outside of the TOE boundary Note 1 to entry: An external entity can also be referred to as a user.	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	external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements Note 1 to entry: In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.	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	
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.	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	TOE
		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.	
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 classNote 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

1977

1978

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

1979

1980

Bibliography

- 1981 This bibliography contains references to further material and standards that the reader of
 1982 this document may find useful. For undated references the reader is recommended to refer
 1983 to the latest edition of the referenced document.
- 1984 [1] JIL - The Application of CC to Integrated Circuits - Version 3.0 - February 2009
- 1985 [2] JIL - Application of Attack Potential to Smartcards - Version 2.9 - January 2013
- 1986 [3] JIL - CEM Refinements for POI Evaluation - Version 1.0 (for trial use) - 27th May 2011
- 1987 [4] JIL - Application of Attack Potential to POIs - Version 1.0 (for trial use) - 9th June 2011
- 1988 [5] JIL - Application of Attack Potential to Hardware Devices with Security Boxes - Version
 1989 2.0 (for trial use) - December 2015
- 1990 [6] JIL - Security Architecture requirements (ADV_ARC) - for smart cards and similar devices
 1991 - Version 2.0 - January 2012
- 1992 [7] JIL - Minimum Site Security Requirements - Version 2.1 (for trial use) – December 2017
- 1993 [8] Supporting Document - Mandatory Technical Document - Full Drive Encryption:
 1994 Authorization Acquisition - January 2015 - Version 1.0 - CCDB - 2015-01-003
- 1995 [9] Supporting Document - Mandatory Technical Document - Full Drive Encryption:
 1996 Encryption Engine - January 2015 - Version 1.0 - CCDB-2015-01-004
- 1997 [10] Supporting Document - Mandatory Technical Document - Evaluation Activities for
 1998 Stateful Traffic Filter Firewalls cPP - February 2015 - Version 1.0 - CCDB-2015-01-002
- 1999 [11] Supporting Document - Mandatory Technical Document - Evaluation Activities for
 2000 Network Device cPP - February 2015 - Version 1.0 - CCDB-2015-01-001
- 2001 [12] collaborative Protection Profile for Network Devices - Version 1.0 - 27-Feb-2015
- 2002 [13] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition -
 2003 Version 1.0 - January 26, 2015
- 2004 [14] collaborative Protection Profile for Full Drive Encryption - Encryption Engine - Version
 2005 1.0 - January 26, 2015
- 2006 [15] collaborative Protection Profile for Stateful Traffic Filter Firewalls - Version 1.0 - 27-
 2007 Feb-2015
- 2008 [16] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction
 2009 and general model, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-001)
- 2010 [17] Common Criteria for Information Technology Security Evaluation. Part 2: Security
 2011 functional components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-002)
- 2012 [18] Common Criteria for Information Technology Security Evaluation. Part 3: Security
 2013 assurance components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-003)

2014	[19] Common Methodology for Information Technology Security Evaluation. Evaluation methodology, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-004)
2015	
2016	[20] CC and CEM addenda. Selection-based SFRs, Optional SFRs, May 2017, Version 0.5 (CCDB-2017-05-XXX)
2017	
2018	
2019	Bibliography to be updated
2020	
2021	