ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"
Convenorship: **UNE**
Convenor: **Bañón Miguel Mr**

22216: Text for DTR ballot

Document type	Related content	Document date	Expected action
Project / Other	Project: ISO/IEC DTR 22216	2021-04-27	**INFO**

Description

WG 3 approved to publish 22216 at 2021 April meeting however 22216 was updated to remove requirements expressed with "shall" based on comments from ISO after the meeting. As changing the modal verbs could be seen as substantial change, DTR ballot will be launched again to approve these changes by SC27.

ISO/IEC JTC 1/SC 27/TR 22216:2021

Date: 2021-06-03

ISO/IEC TR 22216:2021(E)

ISO/IEC JTC 1/SC 27 IT Information Security

Secretariat: DIN

Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2021 and ISO/IEC 18045:2021

Sécurité de l'information, cybersécurité et protection de la vie privée — Nouveaux concepts et changements dans ISO/IEC 15408 : 2021 et ISO/IEC 18045 : 2021

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

Contents

List of tables

List of figures

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, *Information security, cybersecurity and privacy protection*.

This is the first edition of this document.

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 http://www.iso.org/members.html.

Introduction

The fourth edition of the ISO/IEC 15408 and ISO/IEC 18045 standards includes substantial changes from the third edition and subsequent Common Criteria and Common Evaluation Methodology Version 3.1 Revision 5 [14-17] (called CC 3.1 and CEM 3.1 in the following). This edition:

- extends the scope of the standard to cover complex product and communities' needs;
- offers compatibility with currently existing processes.

This document is meant to provide information and support to users of the fourth edition of the ISO/IEC 15408 series and ISO/IEC 18045 standards. The audience for this document includes:

- 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 evaluation authorities;
- consultants supporting ISO/IEC 15408 and ISO/IEC 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 document is familiar with the CC 3.1 and CEM 3.1.

The goal of the revision of the ISO/IEC 15408 series and ISO/IEC 18045 was manifold and intended to support and fluidify the work of all main groups with a general interest in the evaluation of the security properties of TOEs by restructuring the documents, introducing new concepts and updating the existing ones after rigorous consideration of commonly used approaches for the criteria. Specifically, the revision aimed to:

- take into consideration Common Criteria users, especially existing MRAs, and their stakeholders,

  NOTE CCRA and SOG-IS MRA are the only existing recognition arrangements.

- offer continued alignment with the supporting documents developed in the context of the existing MRAs;
- take into consideration commonly used approaches for the criteria and introduce technical changes to the standards accordingly.

New concepts and changes in ISO/IEC 15408:2021 and ISO/IEC 18045

1 Scope

This document:

— introduces the break down between ISO/IEC 15408 and ISO/IEC 18045 and new parts of the standard;

— presents the concepts that were newly introduced in the revised version as well as the rationale for their inclusion;

— proposes an evolution path and information on how to move from CC 3.1 and CEM 3.1 to the fourth edition;

— maps the evolutions between the CC 3.1 and CEM 3.1 revision 5 and the fourth edition ISO/IEC 15408:2021 and ISO/IEC 18045:2021.

2 Normative references

This document has no normative references.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 18045 apply.

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

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

3.1 Abbreviations

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 18045 and the following apply.

CC	Common Criteria
CEM	Common Evaluation Methodology

4 Overview

This document is meant to help users of the standard to understand how they can adapt the use of the standard to their needs by defining:

- supporting documents;
- refinements or application notes;
- extended requirements in an ST or PP;

and how they can use the concepts that were newly introduced or modified in the current version standard.

4.1 Structure of this document

This document has the following structure:

- the remainder of this section gives an overview of the new structure of the documents in the ISO/IEC 15408 series and the newly introduced technical concepts (in 4.2) and continues with usage information of this document for transitional information (in 4.3) and usage information of the ISO/IEC 15408 series for specific needs, respectively (in 4.4);
- in section 5, the major new concepts introduced in the standard are presented, classified and discussed;
- section 6 focuses on concrete guidelines for applying the ISO/IEC 15408 series and ISO/IEC 18045 for specific needs;
- finally, in section 7 the changes specific to each document in the ISO/IEC 15408 series and ISO/IEC 18045 introduced in the fourth edition are mapped and intuitively presented.

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

The fourth revision of the standard now includes 6 parts as shown in Figure 1 hereafter.

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

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. These derived evaluation methods and activities can potentially be included in PPs, PP-Modules, packages, STs and any documents supporting them.

ISO/IEC 15408-5 is a new part that provides pre-defined security requirements that have been identified as useful in support of common usage by stakeholders. It contains the text in regard to EALs (evaluation assurance levels) and CAPs (composed assurance packages) that was previously given in ISO/IEC 15408-3.

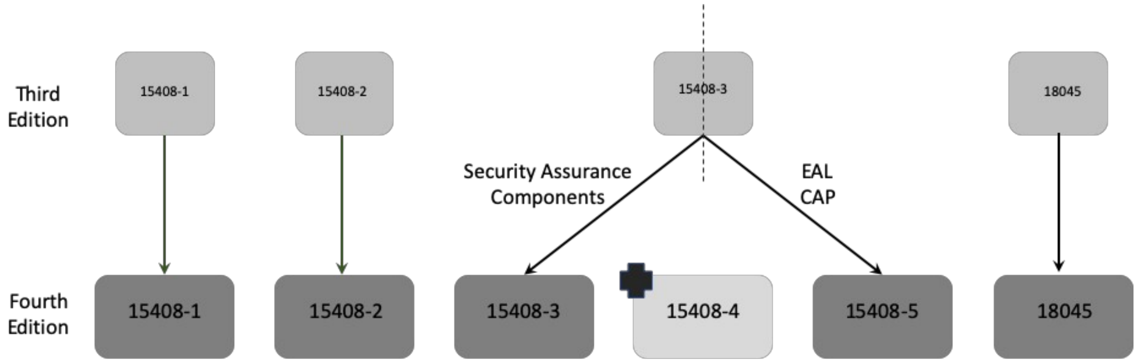


Figure 1 — Mapping between the third and fourth editions

Figure 1 illustrates the structure and partition of the ISO/IEC 15408 and ISO/IEC 18045 documents as well as their relationship in the third and fourth edition, respectively.

Table 1 presents the concepts that were newly introduced in the standard and provides a brief, descriptive overview for each.

Table 1 — Overview of newly introduced concepts

ISO/IEC 15408 Document	Newly introduced concept	Description	Impact
15408-1	Exact Conformance	A new hierarchical relationship between a PP or a PP-Configuration and an ST whereby all the requirements in the ST are drawn from the PP or the PP-Configuration, respectively. An ST is allowed to claim exact conformance to exactly one PP-Configuration; it is allowed to claim exact conformance to one or more PPs. If a PP states that exact conformance is required, the ST will conform to it in an exact manner, i.e. it will contain SPD and objectives identical to the ones in the PP, and the same set of SFRs as the PP with all the assignments and selections resolved.	ISO/IEC 15408-3 ISO/IEC 18045
	Direct Rationale	A construct allowing for an alternative method to derive the SFRs. The SFRs are specified by direct mapping from the SPD; security objectives for the TOE are not included, although security objectives for the operational environment can be specified. 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.	ISO/IEC 15408-3 ISO/IEC 18045
	PP-Modules	PP-Modules constitute internally consistent sets of SPD-elements, security objectives for the TOE and the operational environment, security functional requirements and security assurance requirements, defined in the context of one or more specific PPs and potentially of other PP-Modules. They are meant for addressing specific security features of a given TOE type that cannot be imposed uniformly for all products of that particular type. They are used only in conjunction with PP-Configurations.	ISO/IEC 15408-3 ISO/IEC 18045
	Multi-assurance Evaluation	A new evaluation paradigm which: • allows evaluating heterogeneous products or systems in a unique and coherent manner; • offers the possibility of adapting the assurance level for a product in terms of the different assurance levels of its parts.	ISO/IEC 15408-3 ISO/IEC 18045
	Composite evaluation	Real life products have complex supply chains and are most frequently built by composition. The composite evaluation method allows and facilitates the evaluation by each actor involved in the supply chain. In the absence of the composite evaluation method, the evaluation of such products would require developers to provide evidence that they are not in possession of.	ISO/IEC 15408-3 ISO/IEC 18045
15408-3	Complete Formal TSF model	Inadequacies in a TOE are frequently a consequence of misunderstanding the security requirements which, in turn leads to their flawed implementation. A complete formal TSF model is a formal security model encapsulating the important aspects of security and their relationship to the beha-	ISO/IEC 18045

ISO/IEC 15408 Document	Newly introduced concept	Description	Impact
		viour of the TOE. Specifically, it is a formal representation of the TSF as defined by the complete set of SFRs described in the ST and the set of its formal properties covers all the security objectives for the TOE. The formal TSF model can provide support and precise information throughout the design, implementation and review processes, thereby providing an increased level of assurance that the SFRs and the security objectives of the ST are satisfied by the TOE.	

4.3 Using this document for transitional information

Risk owners rely on PPs to express their specific security requirements in an unambiguous, implementation-independent manner. For new PPs, it is noted for risk owners that two evaluation approaches as well as new features such as composite evaluation and Direct Rationale PPs have been introduced. These have been briefly presented in Table 1 and are further discussed in section 5. For existing PPs, Figure 10 in section 7 illustrates the changes in mandatory content with respect to the third edition of the standard.

For developers it is noted that by default, requirements contained in existing STs are fully compatible. The transition to the fourth edition of the standard has no impact for developers unless new features of the ISO/IEC 15408 standard were used by the risk owners. In the latter case, the information and references provided for risk owners are to be consulted by developers as well.

Evaluators are not the main target of this document which provides only an introduction and cannot replace the reading of the ISO/IEC 15408 standard in its entirety. However, section 7 can serve as an overview for identifying relevant information. In particular, 7.3 provides tables identifying and illustrating work units that have been newly introduced in the fourth edition for the APE, ACE, ASE, ALC, ATE and AVA components.

4.4 Using the standard for specific needs

The details concerning evaluation methods and security components are described in later sections (see sections 5 and 6). From the point of view of risk owners, three main categories of needs are addressed:

- making sure that suppliers strictly adhere to a test plan defined or validated by the risk owner, instead of letting CBs and evaluators devise the test plan: this translates into exact conformance and specific evaluation methods;
- allowing the evaluation of more complex products: this translates into composite and multi-assurance evaluation;
- modular specification of security requirements: this translates into PP-Configurations and PP-Modules.

5 Major new concepts introduced in the standard

5.1 Approaches to security evaluation

The fourth revision of the standard now supports two different approaches to evaluation, as shown in Figure 2 hereafter: the attack-based approach and the specification-based approach.

The standard still supports the evaluation approach used in its previous versions, which is called hereafter the “attack-based approach”, which is an investigative approach. Notably, this approach:

- still mostly uses demonstrable or strict conformance;
- still uses EALs, the AVA_VAN components and the notions of refinement and extended component to define TOE-specific evaluation methodologies;
- still uses standard PPs and STs.

This approach is best used in contexts where state-of the-art and agility with regard to new attacks is demanded by certificate users or 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 or 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 and exploitability of these potential flaws.

A new approach, which is called hereafter the “specification-based approach”, consists in defining, at the PP level, the requirements, and the corresponding evaluation activities. This approach:

- uses exact conformance to PPs;
- often does not use EALs;
- can potentially use Direct Rationale PPs and STs.

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 that were not considered by the risk owner in the PP are not tested. It also aims to suppress the need to define a tailored test plan during the evaluation: the evaluator works exclusively based on a predefined list of tests instead of performing TOE-specific penetration testing.

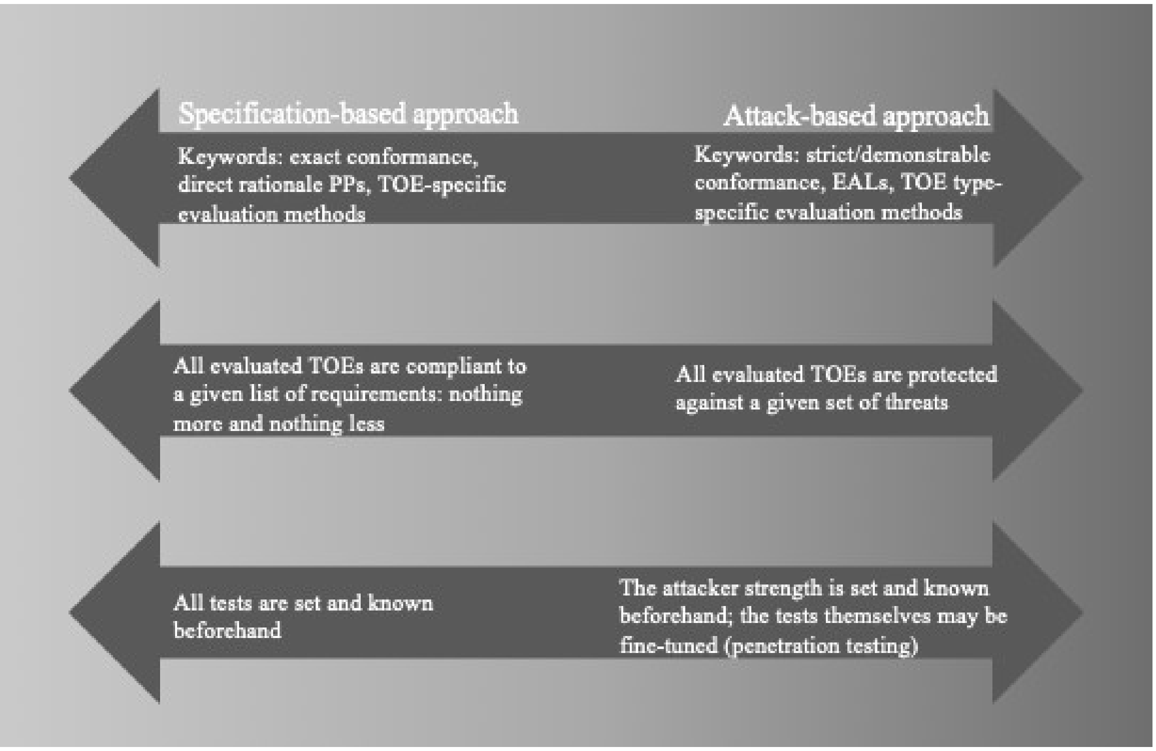

Specification-based approach
Attack-based approach
Keywords: exact conformance, direct rationale PPs, TOE-specific evaluation methods
Keywords: strict/demonstrable conformance, EALs, TOE type-specific evaluation methods
All evaluated TOEs are compliant to a given list of requirements: nothing more and nothing less
All evaluated TOEs are protected against a given set of threats
All tests are set and known beforehand
The attacker strength is set and known beforehand; the tests themselves may be fine-tuned (penetration testing)

Figure 2 — Specification-based and attack-based approaches

5.1.1 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 can vary, e.g. according to technology choices or IP constraints, provided they enforce the protection of the assets as expected. Such evaluations can be carried out without reference to a PP or can be based on PPs 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 can be accepted as conformant. The EALs 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 and 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.

5.1.1.1 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 can be organized in a package). However, the approach does not forbid the use of the exact conformance concept whenever appropriate.

5.1.1.2 Edition of Protection Profiles and Security Targets

The “attack-based” approach uses standard or Direct Rationale PPs and STs. 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 can be of benefit to innovation by allowing vendors to complete their own requirements, as opposed to unified PPs;

  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;
- favours 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.

5.1.1.3 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 on one hand by ISO/IEC 18405 (which provides common notions such as the attack potential), and on the other hand 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 the type of technology considered. As a consequence, the evaluator has to consider the state-of-the-art of attacks for the selected AVA_VAN, regardless of the functional features described in the underlying PPs.
- 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 (e.g. 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 (e.g. if new attacks have been discovered in the field or in the academic literature).

5.1.2 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. Note that ISO/IEC 15408-3 and ISO/IEC 18045 are fundamental to the newly introduced framework for the specification of evaluation methods and activities.

5.1.2.1 Exact conformance

The “specification-based” approach uses exact conformance PPs, which ensures that the conformant ST does not change or even add anything to the PP’s 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.

It is noted that “optional features” are addressed by optional security functional requirements (SFRs).

A given type of TOE can provide a selection-based alternative for some of its SFRs. However, such selections can require the inclusion of different dependencies. For example, keys used in an IPSec tunnel can 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 can be described as optional requirements.

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 can be a set of suppliers for a given customer, a national certification scheme, an MRA, etc.) and are typically supplied in the form factor of a PP and some supporting documents. Note that a PP can directly contain evaluation methods and activities associated to its SFRs. Examples of this can be found in currently used collaborative PPs and their corresponding supporting documents (see documents [6] to [13]).

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 a derivation process is:

- to adapt ISO/IEC 18045 to a given technology;
- 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.

5.1.2.2 Edition of Protection Profiles and Security Targets

The “specification-based” approach can use standard or Direct Rationale PPs and STs. Direct Rationale PPs and STs do not use security objectives for the TOE; they include instead a direct mapping from threats and organizational security policies 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 usually 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.

5.1.2.3 Evaluation methodology — ISO/IEC 15408-4

The “specification-based” approach usually does not use EALs. Instead of relying on an assurance scale, the PP editor can define 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/IEC 18045 activities and use 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 considered by updating the PP or the supporting documents describing the requirements and the evaluation methodology.

5.2 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) Modularity of the evaluation process: splitting a product between different TOEs, resulting in several STs, and evaluating the complete product via a composition mechanism. This includes typically two main mechanisms:

   o composition of evaluated products using the ACO assurance class;

   o composite product evaluation using _COMP assurance components.

b) Modularity of requirements within a single TOE, through the following mechanisms:

- functional and assurance packages (notably EALs);
- modular PPs, 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 bundling[1], i.e. the structuring of functional and assurance requirements in dedicated subsections dependent on their purpose.

These newly introduced concepts and mechanisms providing modularity allow addressing various problems and facilitate their solution. For instance:

- products where the most critical assets are managed by a Secure Element can be suitable candidates for multi-assurance evaluation, whereas they could not be easily evaluated as a whole in previous versions of the standard;
- products where different vendors provide the software and hardware layers can be good candidates for composite evaluation;
- EALs ensure consistency, comparability and sufficiency of evidences when evaluating the robustness of a product against a given class of attackers. Other assurance packages might be created to answer specific procurement needs.

5.2.1 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.

ISO/IEC 15408-1 suggests several possible ways to break down a product into several parts, namely:

- layered;
- network or bi-directional;
- embedded.

The next sections provide some information on how and when to use each one of these models.

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

5.2.1.1 Composition models

Layered composition model

In the layered model the product is composed of a base component and a dependent component. The base component is independent of the dependent component. On the contrary, the dependent component relies on the base component and uses its functionality.

Network or bi-directional composition model

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.

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

Embedded composition model

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 can also be relevant for providers of building blocks to other developers.

5.2.1.2 Evaluation mechanisms for composition

This version of the standard supports two 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 originally defined in [14] and introduced in ISO/IEC 18405 for the _COMP assurance components.

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

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

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

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

- an Integrated Circuit (IC) and its dedicated embedded software, which is evaluated first;
- an execution environment, or platform, running on top of the IC and allowing the use of high-level programming languages for the applicative layer, which is evaluated using _COMP;
- some applications running on the platform, which are evaluated using _COMP.

5.2.2 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 (e.g. 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).

Packages are either:

- assurance packages, containing only assurance components or requirements; or
- functional packages, containing 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 can include a Security Problem Definition (SPD) and Security Objectives (for the TOE and the operational environment) derived from that SPD. Furthermore, functional packages can optionally declare a set of SFRs that are required in order for the package to be used or included by another requirements specification. If declared, this set of SFRs can be seen as a mandatory dependency at the package level.

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

Packages can also include optional evaluation methods and activities. These can be included in the package associated with the relevant security requirements. Alternatively, the evaluation methods and activities can be provided in a separate document.

EXAMPLE

- Alternative packages driven by a selection that is operated in an SFR.
- Using packages as a consistent set of assurance requirements: EALs are an example of widely used assurance packages.
- Using packages as a consistent set of functional requirements: a given community potentially wants 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-analyse which SFRs are needed.
- 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;
- STA (Security Target Assurance) provides assurance packages for ST evaluation.

5.2.3 Modular Protection Profiles

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

- packages can 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 can introduce changes to their TOE types. PP-Modules can use other PP-Modules as a base;
- PP-Modules can identify a set of selection-based SFRs provided that such SFRs do not introduce changes to the TOE and the TOE boundaries. Otherwise, it can be more suitable to define several PP-Modules;
- PP-Modules can carry a specific set of assurance components for the module (see multi-assurance evaluation in section 5.2.4).

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 in the evaluation of STs.

PP-Modules can be used for representing:

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

EXAMPLE An editor can potentially 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 can typically be used with alternative sets of base PPs, each corresponding to a given platform.

5.2.4 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 assurance components from ISO/IEC 15408-3, which allows claiming a global set of assurance requirements/assurance package for the entire TOE, and possibly multiple different sets of assurance requirements/assurance packages for different parts of the TSF, called the sub-TSFs.

The previous section already outlined the benefits of modular PPs. In addition, multi-assurance evaluation allows addressing heterogeneous products and evaluating modular TOEs that require different 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 three practical use cases for multi-assurance evaluations.

5.2.4.1 High-assurance selected functions

This use case 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 global assurance level, with one or more sub-TSFs that require a higher assurance level.

With the multi-assurance approach, a PP-Configuration author identifies the bigger TOE and the sub-TSFs including their boundaries and specifies each sub-TSF through a component PP or PP-Module carrying their specific sets of SFRs and SARs.

EXAMPLE A smartphone with a secure hardware-backed key store could be such a TOE. In this example, 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-TSF with SFRs for the key store at EAL4+ level. The sub-TSF's SFRs would encode the access control to the long-term keys as not allowing anyone to export them out of the sub-TSF and requiring authorization from the user via the bigger TOE to perform the cryptographic signature operation. This example is illustrated in Figure 3 hereafter.

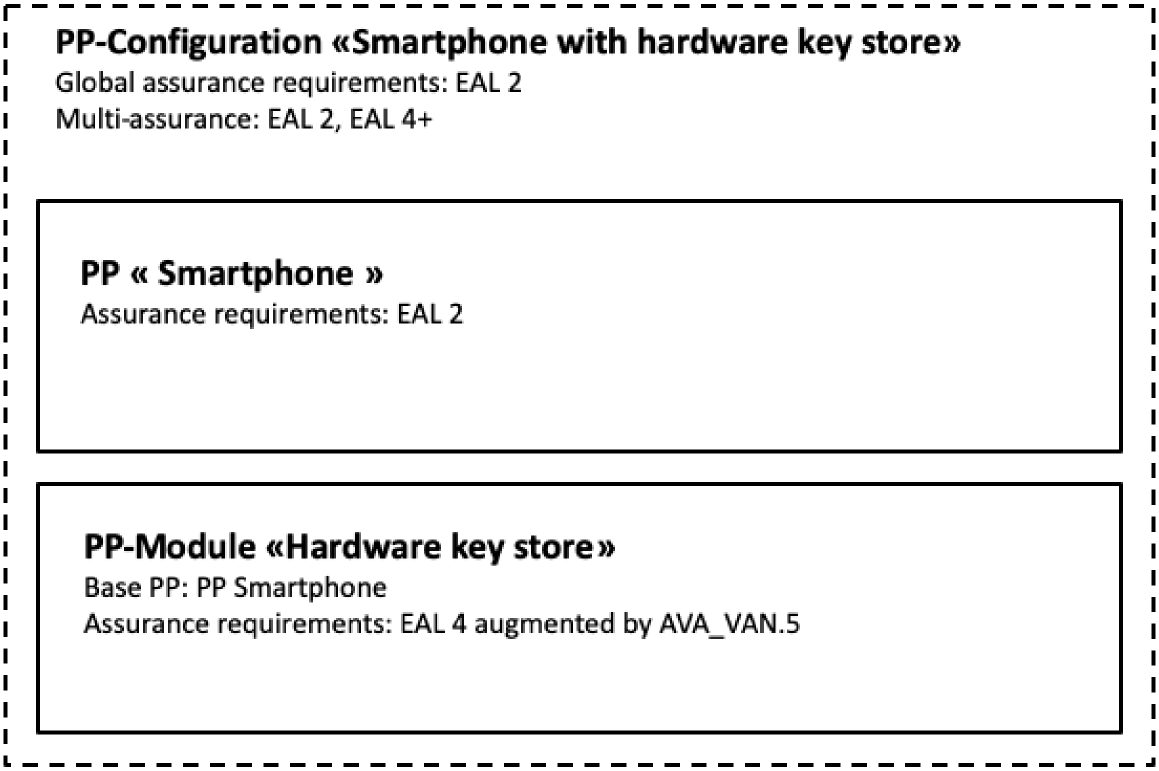

PP-Configuration «Smartphone with hardware key store»
Global assurance requirements: EAL 2
Multi-assurance: EAL 2, EAL 4+
PP « Smartphone »
Assurance requirements: EAL 2
PP-Module «Hardware key store»
Base PP: PP Smartphone
Assurance requirements: EAL 4 augmented by AVA_VAN.5

Figure 3 — Smartphone with hardware key store

5.2.4.2 Low assurance selected functions

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

We assume the existence of a TOE that is evaluated on a higher assurance level for most parts, with one or more sub-TSFs that allow a lower assurance level. With the multi-assurance approach, a PP-Configuration author identifies the bigger TOE and the sub-TSFs and specifies each sub-TSF through a component PP or PP-Module carrying their specific sets of SFRs and SARs.

EXAMPLE

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 4 hereafter.

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

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

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

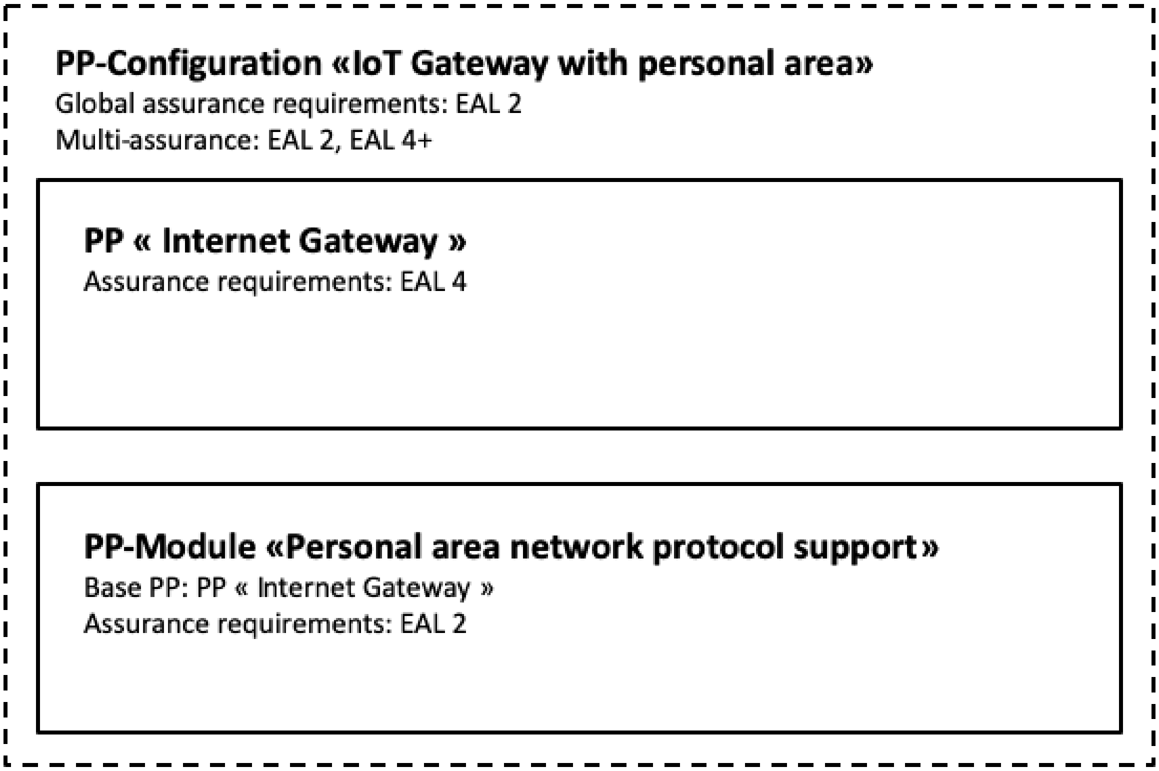

PP-Configuration «IoT Gateway with personal area»
Global assurance requirements: EAL 2
Multi-assurance: EAL 2, EAL 4+
PP « Internet Gateway »
Assurance requirements: EAL 4
PP-Module «Personal area network protocol support»
Base PP: PP « Internet Gateway »
Assurance requirements: EAL 2

Figure 4 — IoT gateway with personal area network

5.2.4.3 Point of Interaction use case

This use case consists of a payment terminal, called a Point of Interaction (POI), that manages assets with different sensitivity.

EXAMPLE The POI is a paradigmatic example of a product composed of parts that respond to different security problems and assurance needs[2]. The POI PP defines several multi-assurance PP-Configurations, which could be expressed using the modular PP concepts.

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

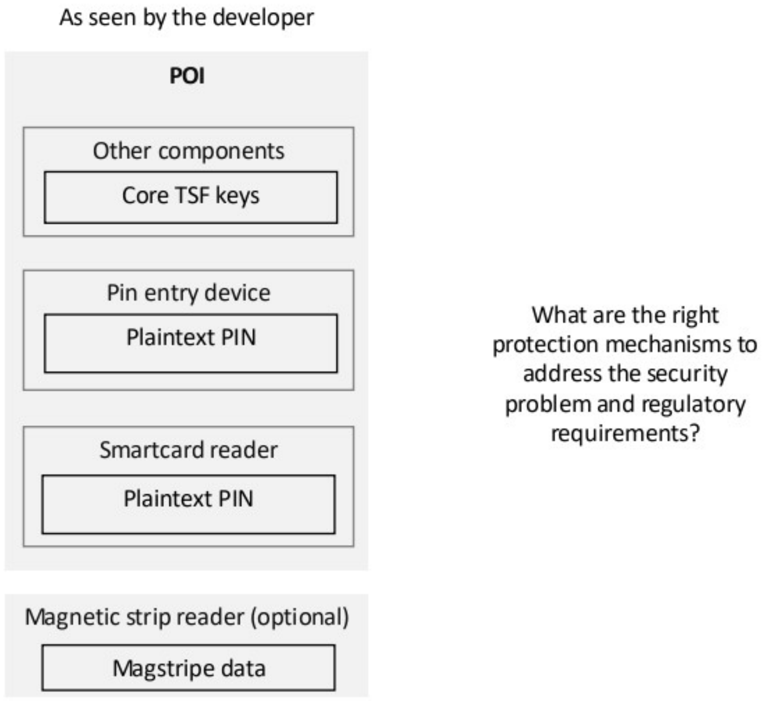

As seen by the developer
POI
Other components
Core TSF keys
Pin entry device
Plaintext PIN
Smartcard reader
Plaintext PIN
Magnetic strip reader (optional)
Magstripe data
What are the right protection mechanisms to address the security problem and regulatory requirements?

Figure 5 — POI developer

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

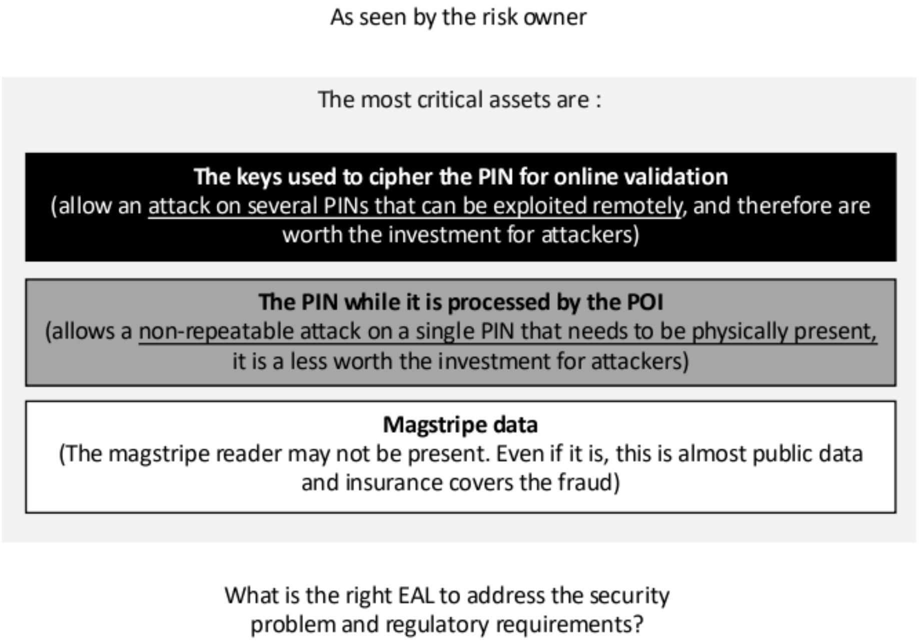

As seen by the risk owner
The most critical assets are :
The keys used to cipher the PIN for online validation
(allow an attack on several PINs that can be exploited remotely, and therefore are worth the investment for attackers)
The PIN while it is processed by the POI
(allows a non-repeatable attack on a single PIN that needs to be physically present, it is a less worth the investment for attackers)
Magstripe data
(The magstripe reader may not be present. Even if it is, this is almost public data and insurance covers the fraud)
What is the right EAL to address the security problem and regulatory requirements?

Figure 6 — POI risk owner

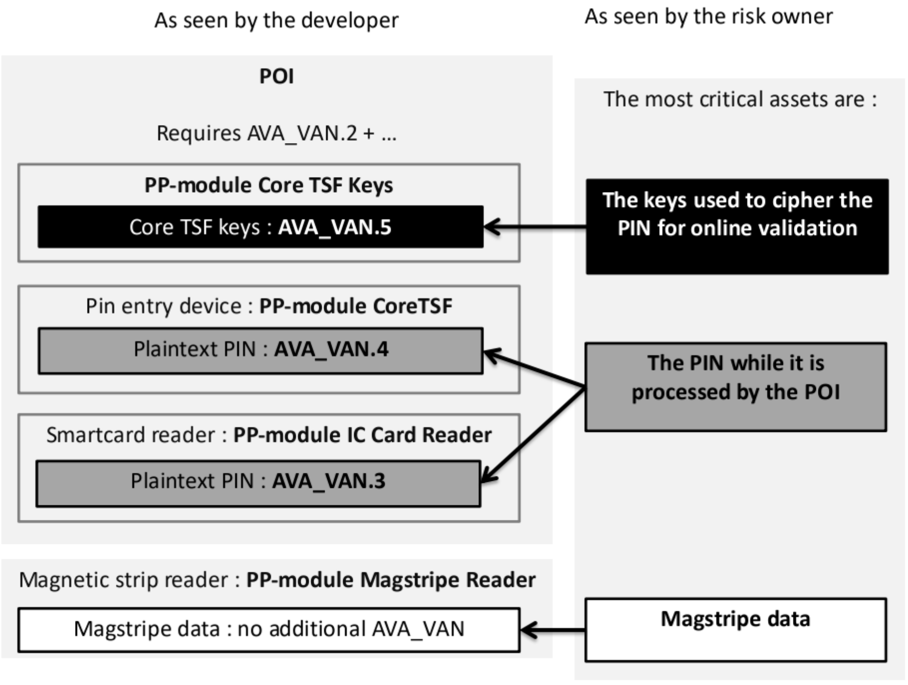
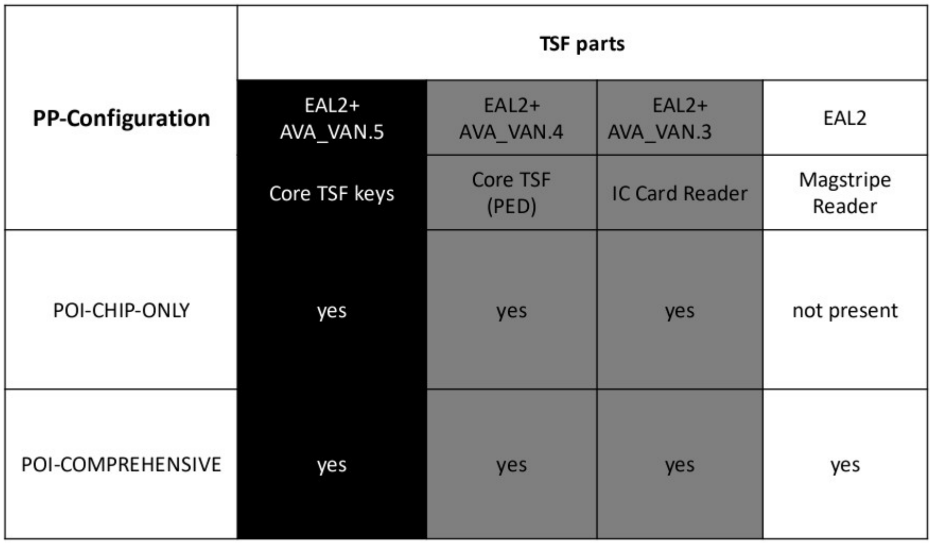

As seen by the developer
As seen by the risk owner
POI
Requires AVA_VAN.2 + ...
PP-module Core TSF Keys
Core TSF keys : AVA_VAN.5
Pin entry device : PP-module CoreTSF
Plaintext PIN : AVA_VAN.4
Smartcard reader : PP-module IC Card Reader
Plaintext PIN : AVA_VAN.3
Magnetic strip reader : PP-module Magstripe Reader
Magstripe data : no additional AVA_VAN
The most critical assets are :
The keys used to cipher the PIN for online validation
The PIN while it is processed by the POI
Magstripe data

Figure 7 — POI developer vs risk owner



PP-Configuration	TSF parts			
	EAL2+ AVA_VAN.5	EAL2+ AVA_VAN.4	EAL2+ AVA_VAN.3	EAL2
	Core TSF keys	Core TSF (PED)	IC Card Reader	Magstripe Reader
POI-CHIP-ONLY	yes	yes	yes	not present
POI-COMPREHENSIVE	yes	yes	yes	yes

Figure 8 — POI assurance requirements

5.2.5 Evaluation by composition and multi-assurance

The notions of composition and multi-assurance are aimed at solving different problems. In a nutshell, composed and composite evaluations refer to evaluation processes which are particularly suitable for multi-actor TOEs and allow reusing previous evaluation results, while multi-assurance refers to a property of some TOEs in the context of a particular security problem and operational environment.

- Evaluation by composition addresses TOEs with a supply and/or integration chain that can potentially involve multiple parties, each of which takes care of the evaluation of the security functionality it develops. Broadly speaking, the objective of composition is to assign a single, global assurance level for the junction of such TOEs. To this end, ISO/IEC 15408 standardizes the following two approaches for the reuse of evaluation results in an evaluation process:
  - o Composed evaluation allows to obtain a global assurance level (CAP) for a TOE from the individual assurance levels of its interacting sub-TOEs.
  - o Composite evaluation allows to obtain a global assurance level for a layered TOE, in an incremental way where the base layer is evaluated first, then the integrated dependent and base layers are evaluated by reusing the evaluation results of the base layer.
- Multi-assurance evaluation focuses on TOEs where different assurance needs apply to different parts of the security functionality (the sub-TSFs) while ensuring a global assurance level for the entire TOE. For instance, the sponsor assumes that some parts of a modular TOE require higher assurance (e.g. a higher EAL) than the rest. Before the introduction of multi-assurance, such needs would have forced a sponsor to undergo several evaluations of the same TOE for different STs. With this concept, ISO/IEC 15408 standardizes and optimizes this process, and allows to determine the

global assurance level for the TOE, which cannot be obtained by using the single-assurance approach.

From the point of view of the TOE/TSF, multi-assurance evaluation applies to any architecture, while evaluation by composition applies to specific architectures: composed evaluation applies to a TOE that consists of several interacting sub-TOEs, while composite evaluation applies to a TOE where a dependent layer relies on a base layer.

The rest of this section illustrates the relationship between composite, single-assurance and multi-assurance evaluation approaches.

Let the TOE be composed of sub-TSFs as shown in Figure 9, where EAL_A, EAL_B and EAL_C apply to the sub-TSFs and EAL_X is included in EAL_A, EAL_B and EAL_C.

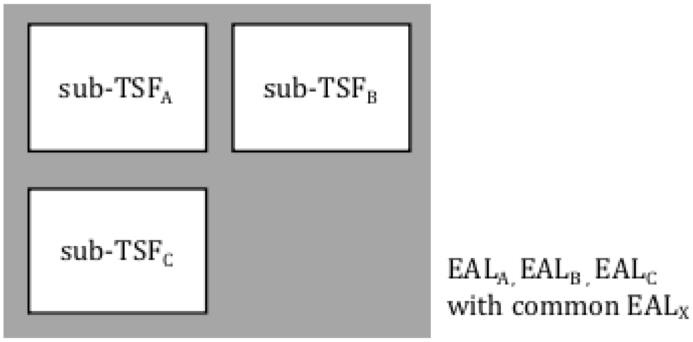


Figure 9 — Multi-assurance TOE

The way to achieve the common EAL_X for the entire TOE, and also the specific EAL_A, EAL_B and EAL_C for the sub-TSFs is either by using the multi-assurance evaluation approach, or by making as many single-assurance evaluations as sub-TSFs, as shown in Figure 10 (note that in each evaluation the entire TOE is evaluated against EAL_X).

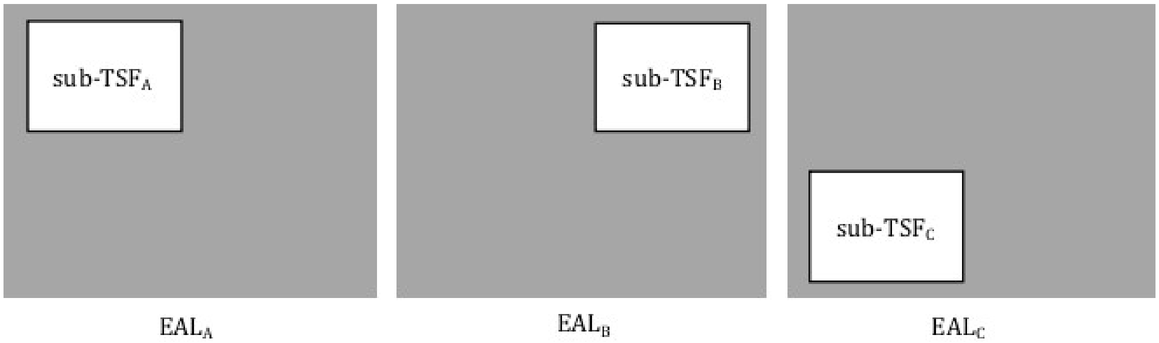


Figure 10 — Multiple single evaluations

Note that by construction and unlike a set of independent single-assurance evaluations, a multi-assurance evaluation allows determining the global assurance level of the TOE.

In the following, let us consider the TOE shown in Figure 11, composed of a base and a dependent component, for which EAL$_X$ is the targeted assurance level.

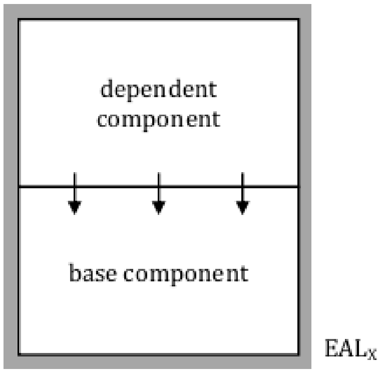


Figure 11 — Composite TOE

There are two ways of achieving EAL$_X$ for this TOE: either by applying the single-assurance evaluation model to the entire TOE (and TSF), or by using the composite evaluation approach in two evaluation steps as shown in Figure 12, where the base component is evaluated at EAL$_X$ level or higher and the results of the base component evaluation are reused in the composite evaluation at EAL$_X$.

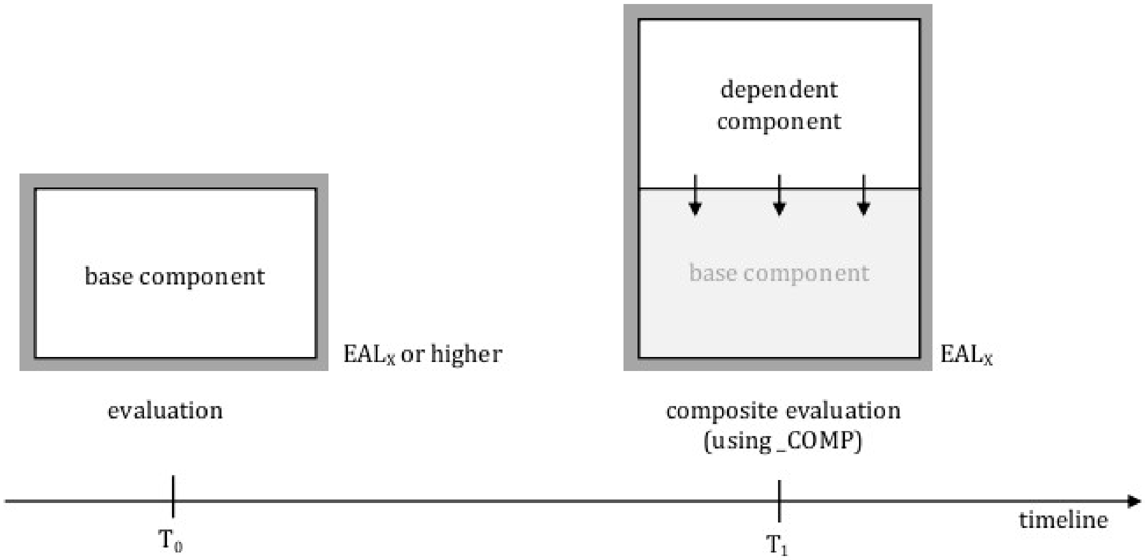


Figure 12 — Composite evaluation

The composite approach allows mapping the evaluation process to the development and integration life cycle and reusing the results of the base component evaluation in potentially many composite evaluations.

What does it mean to apply the multi-assurance approach to such a composite TOE? Figure 13 shows the composite TOE when using the concept of sub-TSF as in Figure 9, where EAL$_X$ is equal to EAL$_B$. Note that multi-assurance makes sense when EAL$_A$ is higher than EAL$_B$.

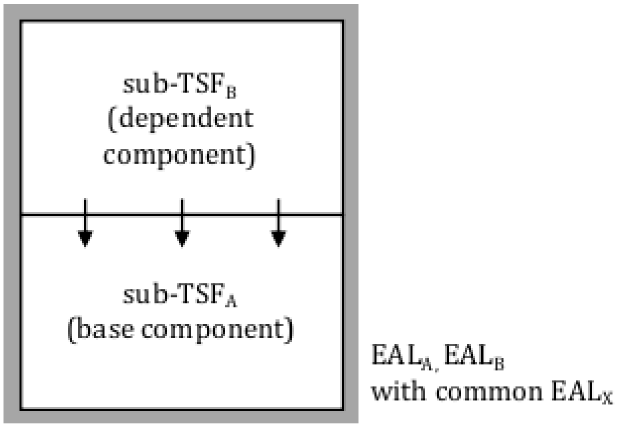


Figure 13 — Multi-assurance evaluation of a composite TOE

The multi-assurance approach allows to associate the base and dependent sub-TSFs to their own assurance levels at the same evaluation. Figure 14 shows a combined multi-assurance/composite evaluation.

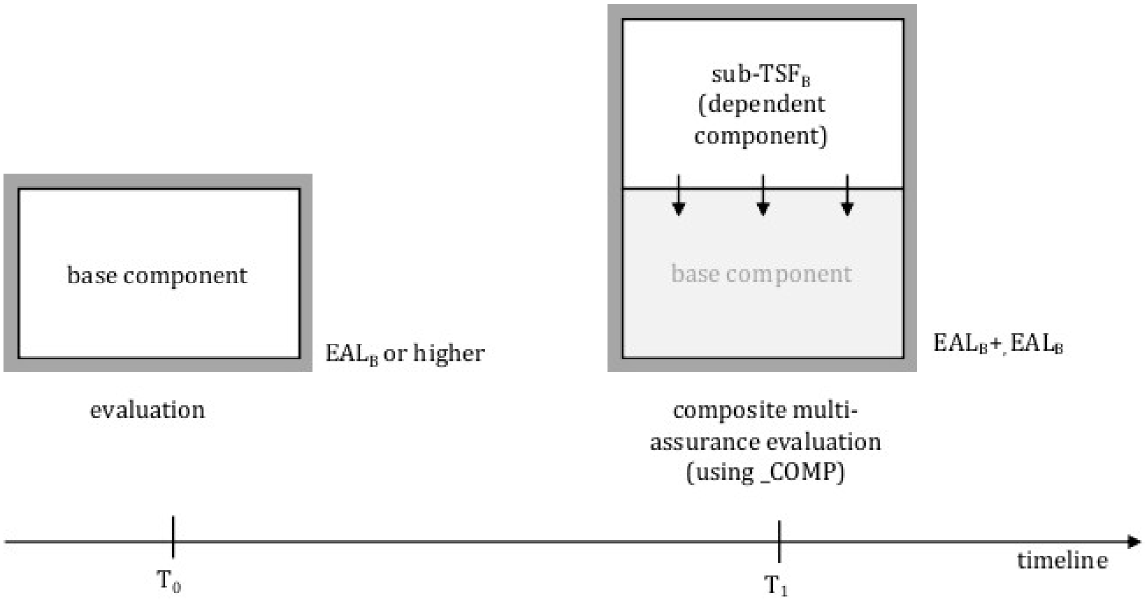


Figure 14 — Multi-assurance composite evaluation

As the previous examples illustrate, multi-assurance and evaluation by composition target different main objectives and are compatible notions that can be used together.

6 Applying the standard to specific needs

6.1 Refining and deriving requirements

As in previous versions, the standard supports the definition of tailored functional and assurance security requirements by means of three constructs, namely refinement, application note and extended components.

6.1.1 Refinements

The refinement operation allows to strengthen an existing requirement, e.g. by narrowing the scope or adding obligations. As usual a TSF that satisfies the refined requirement is meant to satisfy the original requirement.

6.1.2 Application Notes

Application notes are also used to supplement the specification of requirements. Although the meaning of the requirement is not changed, the application note provides contextual information and helps interpreting the CC requirement in a specific domain. For instance, an application can be used to give meaning to abstract CC terms such as “user”, “role”, etc.

6.1.3 Extended requirements

Extended components are defined when the TSF cannot be characterized using the standard catalogue of SFRs or SARs defined in ISO/IEC 15408. This construct allows to address a missing class, family or component. The definition has to follow the same syntactic rules as the standard requirements and rationale for their definition must be provided: the author of the extended requirement has to explain why the standard catalogue was not appropriate to solve their problem.

The new standard introduces several SFRs that had been defined using the extended components mechanism in PPs, e.g. FCS_RNG.1 and FPT_INI.1.

6.2 Refining and deriving evaluation methods

The notion of derived evaluation methods in ISO/IEC 15408-4 addresses concerns related to the standard’s capabilities to address more technology areas. 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.

6.2.1 Attack-based approach

Currently, evaluation methods defined using SAR and ISO/IEC 18045 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], [4] and [5]. Similar efforts have been made for the evaluation of payment terminals and Hardware Devices with Security Boxes (see document [3]).

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 methods.

6.2.2 Specification-based approach

Currently, the definition of evaluation methods in cPPs is performed either in the PP itself, linked to specific SFRs or SARs, or given in separate supporting documents.

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 methods.

6.3 Practical aspects of supporting documents

The use of supporting documents to tailor the assurance requirements and provide the definition of specific evaluation methods constitute a wide-spread practice. Although the concept of supporting document is out of the standard, these documents are defined, validated, used and maintained within well-established expert communities. The new version of the standard aims to offer additional tools without affecting the operation of such communities or the validity of the produced supporting documents.

7 Evolutions in the fourth edition of ISO/IEC 15408 and ISO/IEC 18045

7.1 Changes in ISO/IEC 15408-1

Table 2 — Changes in ISO/IEC 15408-1

ISO/IEC 15408-1 fourth edition	
Structure	This part of ISO/IEC 15408 has been restructured to allow the grouping of related topics appropriately. Figure 9 illustrates the clause structure and the differences between CC v3.1 revision 5 [14] and the fourth edition of the standard.
Terminology	Changes as a result of the JTC 1 directives. Changes and new terms as a result of other changes in the standards, e.g. exact conformance, multi-assurance, composite evaluation. Consolidation of terms given in ISO/IEC 18045 into ISO/IEC 15408-1.
Packages	Text discussing the mandatory contents of packages has been added to the sub-clause 9.2 Package types. A new sub-clause has been added to discuss the inclusion of optional evaluation methods and activities in packages.
Protection Profiles	Figure 10 illustrates the mandatory content of PPs and underlines the differences between CC v3.1 revision 5 [14] and the fourth edition.
Modularity	STs cannot directly claim conformance to PP-Modules, only to exactly one PP-Configuration. PP-Modules can claim specific sets of assurance requirements. Figure 11 illustrates the mandatory content of STs and underlines the differences between CC v3.1 revision 5 [14] and the fourth edition. Figure 12 illustrates the mandatory content of PP-Modules and underlines the differences between CC v3.1 revision 5 [14] and the fourth edition. Figure 13 illustrates the mandatory content of PP-Configurations and underlines the differences between CC v3.1 revision 5 [14] and the fourth edition.
Multi-assurance	Text that describes the multi-assurance evaluation paradigm has been

	provided.
PP-Configurations	Text has been added for allowing PP-Modules that require exact conformance to specify (and allow for use) optional requirements. PP-Configurations can be of either single- or multi-assurance type.
Composition of assurance	The clause related to composition has been restructured and updated. The composite evaluation paradigm has been described.
New Annex numbering and structure	The annexes were re-numbered in order to mirror the order of the main clauses. The previous Annex E — Guidance for Operations – has been removed and replaced by PP/PP-Configuration Conformance. Currently, the document includes the following normative annexes: Annex A) Specification of Packages Annex B) Specification of Protection Profiles Annex C) Specification of PP-Modules and PP-Configurations Annex D) Specification of Security Targets and Direct Rationale STs Annex E) PP/PP-Configuration Conformance

The following diagram illustrates the differences between the clause structure of CC v3.1 revision 5 (Part 1) [14] and the fourth edition of the standard.

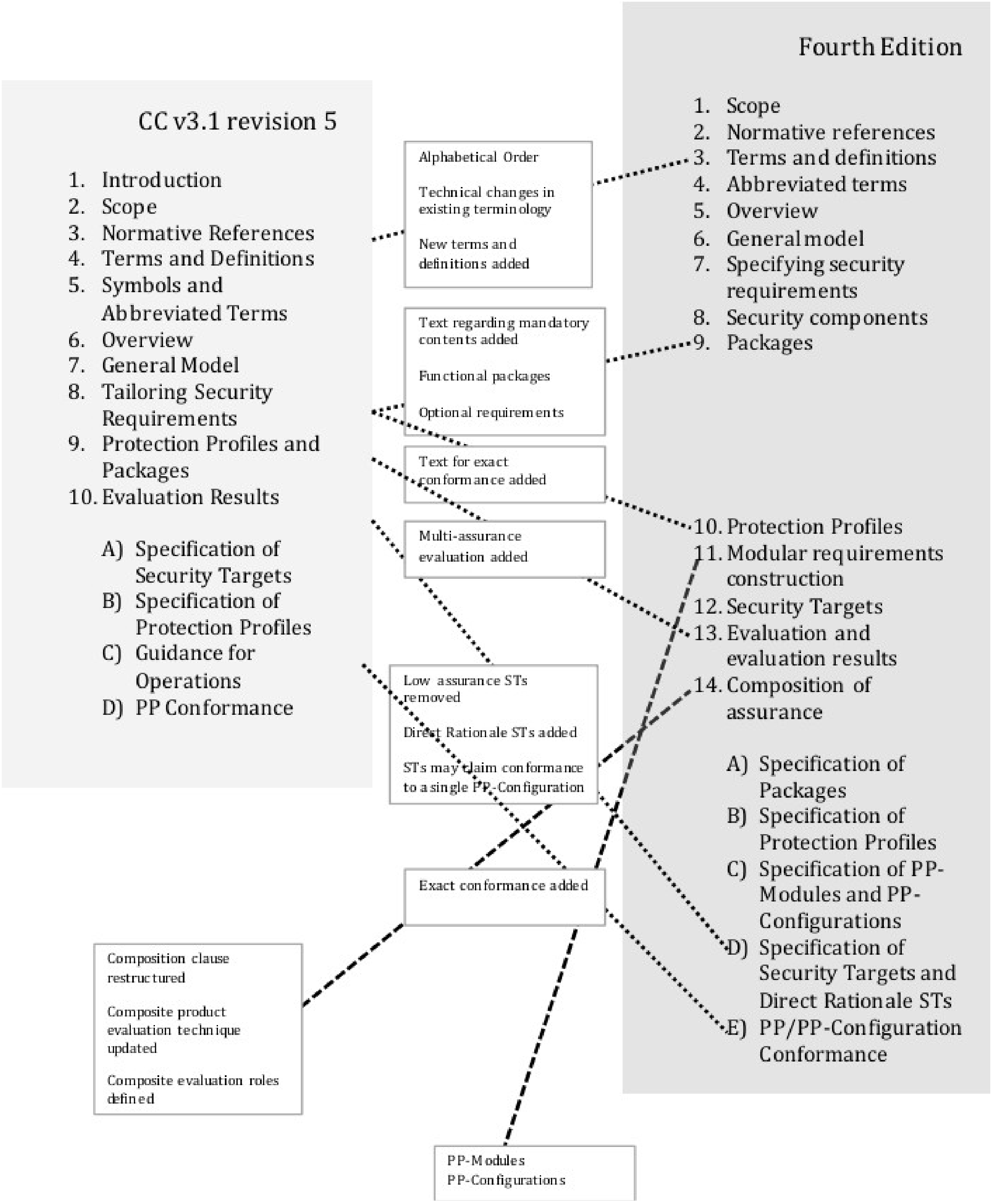

CC v3.1 revision 5
1. Introduction
2. Scope
3. Normative References
4. Terms and Definitions
5. Symbols and Abbreviated Terms
6. Overview
7. General Model
8. Tailoring Security Requirements
9. Protection Profiles and Packages
10. Evaluation Results
A) Specification of Security Targets
B) Specification of Protection Profiles
C) Guidance for Operations
D) PP Conformance
Fourth Edition
1. Scope
2. Normative references
3. Terms and definitions
4. Abbreviated terms
5. Overview
6. General model
7. Specifying security requirements
8. Security components
9. Packages
10. Protection Profiles
11. Modular requirements construction
12. Security Targets
13. Evaluation and evaluation results
14. Composition of assurance
A) Specification of Packages
B) Specification of Protection Profiles
C) Specification of PP-Modules and PP-Configurations
D) Specification of Security Targets and Direct Rationale STs
E) PP/PP-Configuration Conformance
Alphabetical Order
Technical changes in existing terminology
New terms and definitions added
Text regarding mandatory contents added
Functional packages
Optional requirements
Text for exact conformance added
Multi-assurance evaluation added
Low assurance STs removed
Direct Rationale STs added
STs may claim conformance to a single PP-Configuration
Exact conformance added
Composition clause restructured
Composite product evaluation technique updated
Composite evaluation roles defined
PP-Modules
PP-Configurations

Figure 15 — Clause structure — fourth edition vs. CC version 3.1 revision 5

The following diagrams illustrate the differences between the mandatory contents of PPs, STs, PP-Modules and PP-Configurations in CC version 3.1 revision 5 [14] and the fourth edition of the standard. Bold text indicates content that has been introduced in the new edition. Text in italics indicates concepts that have been modified.

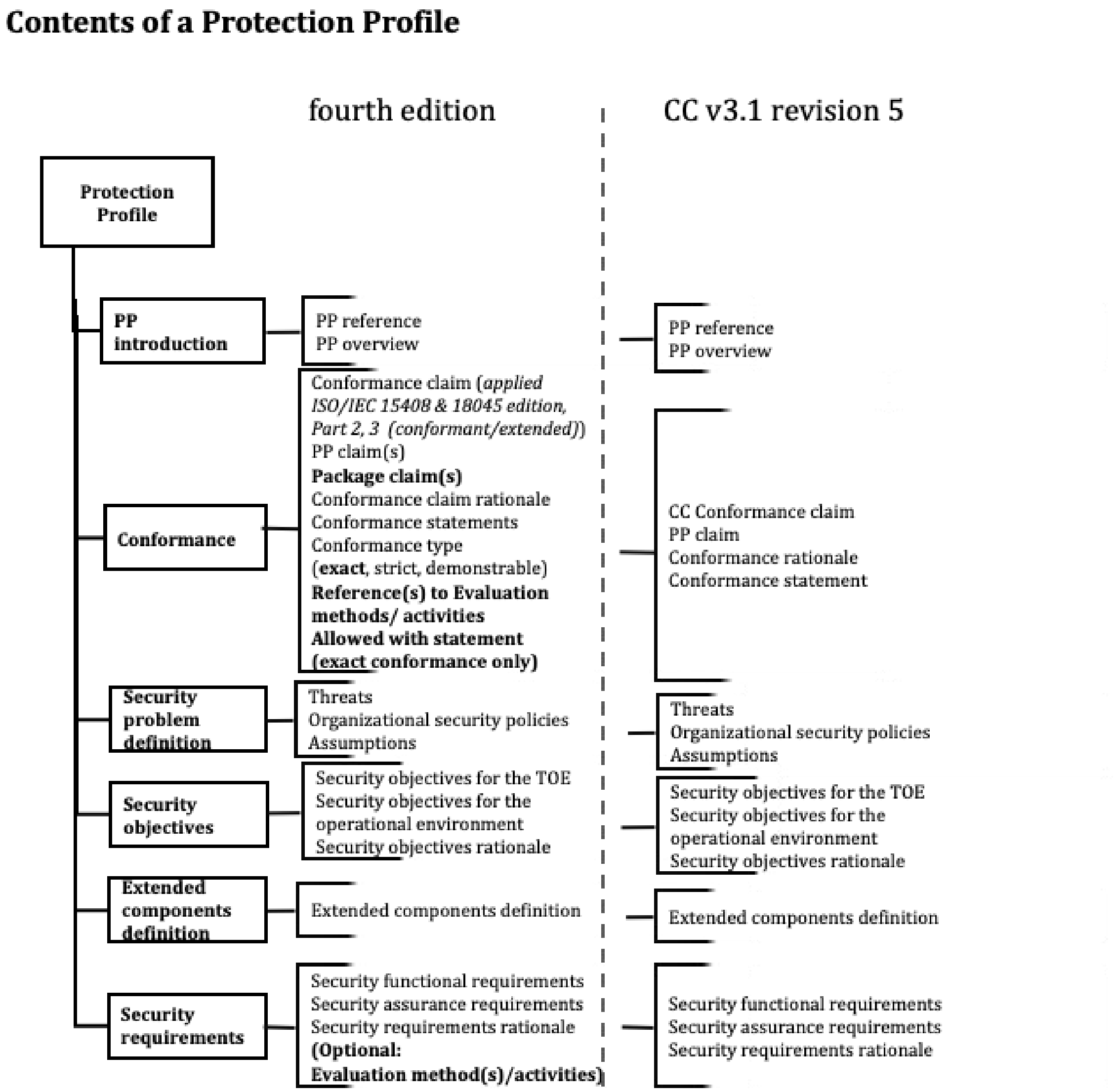

Contents of a Protection Profile
fourth edition
CC v3.1 revision 5
Protection Profile
PP introduction
PP reference
PP overview
PP reference
PP overview
Conformance
Conformance claim (applied ISO/IEC 15408 & 18045 edition, Part 2, 3 (conformant/extended))
PP claim(s)
Package claim(s)
Conformance claim rationale
Conformance statements
Conformance type
(exact, strict, demonstrable)
Reference(s) to Evaluation methods/ activities
Allowed with statement
(exact conformance only)
CC Conformance claim
PP claim
Conformance rationale
Conformance statement
Security problem definition
Threats
Organizational security policies
Assumptions
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
(Optional:
Evaluation method(s)/activities)
Security functional requirements
Security assurance requirements
Security requirements rationale

Figure 16 — Contents of a PP — fourth edition vs CC version 3.1 revision 5

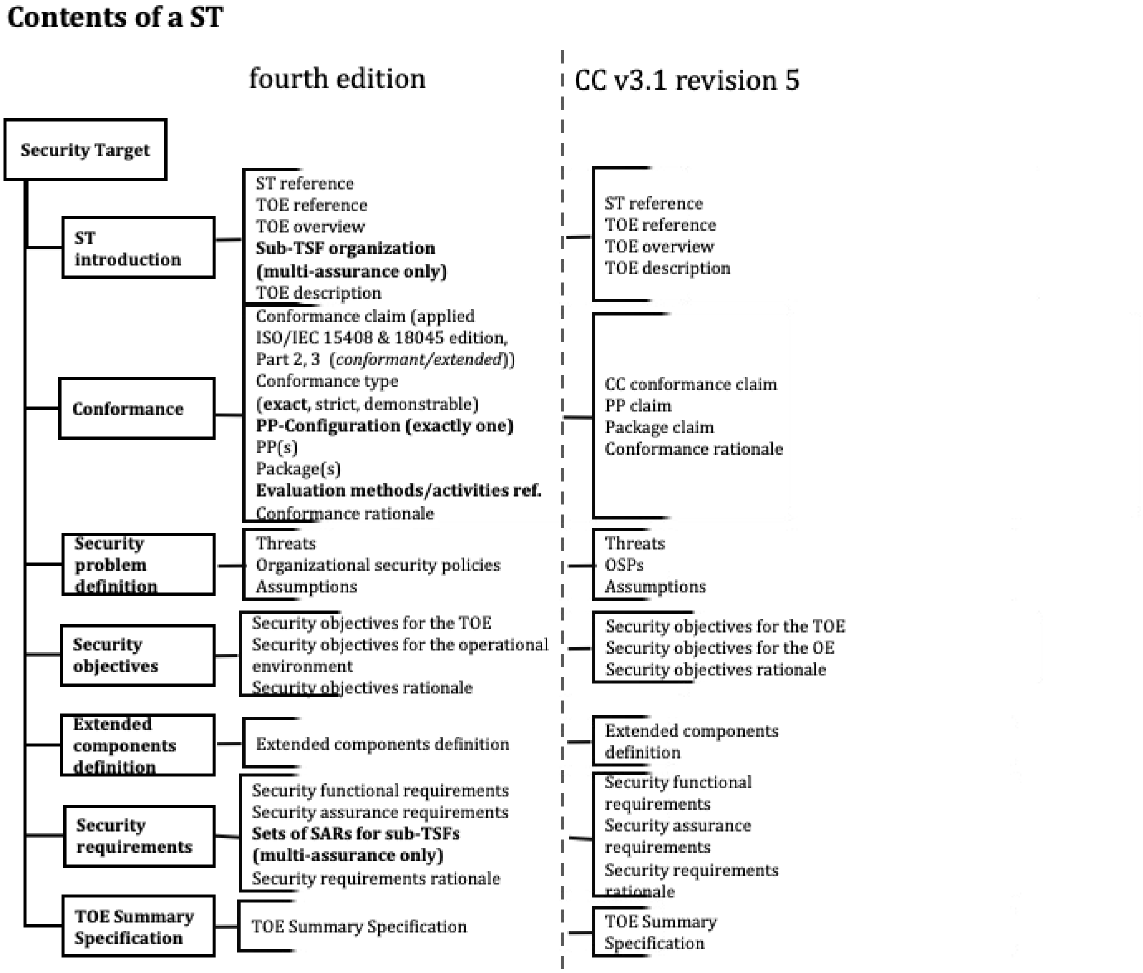

Contents of a ST
fourth edition
CC v3.1 revision 5
Security Target
ST introduction
ST reference
TOE reference
TOE overview
Sub-TSF organization (multi-assurance only)
TOE description
Conformance
Conformance claim (applied ISO/IEC 15408 & 18045 edition, Part 2, 3 (conformant/extended))
Conformance type (exact, strict, demonstrable)
PP-Configuration (exactly one)
PP(s)
Package(s)
Evaluation methods/activities ref.
Conformance rationale
Security problem definition
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Sets of SARs for sub-TSFs (multi-assurance only)
Security requirements rationale
TOE Summary Specification
TOE Summary Specification
ST reference
TOE reference
TOE overview
TOE description
CC conformance claim
PP claim
Package claim
Conformance rationale
Threats
OSPs
Assumptions
Security objectives for the TOE
Security objectives for the OE
Security objectives rationale
Extended components definition
Security functional requirements
Security assurance requirements
Security requirements rationale
TOE Summary Specification

Figure 17 — Contents of an ST — fourth edition vs CC version 3.1 revision 5

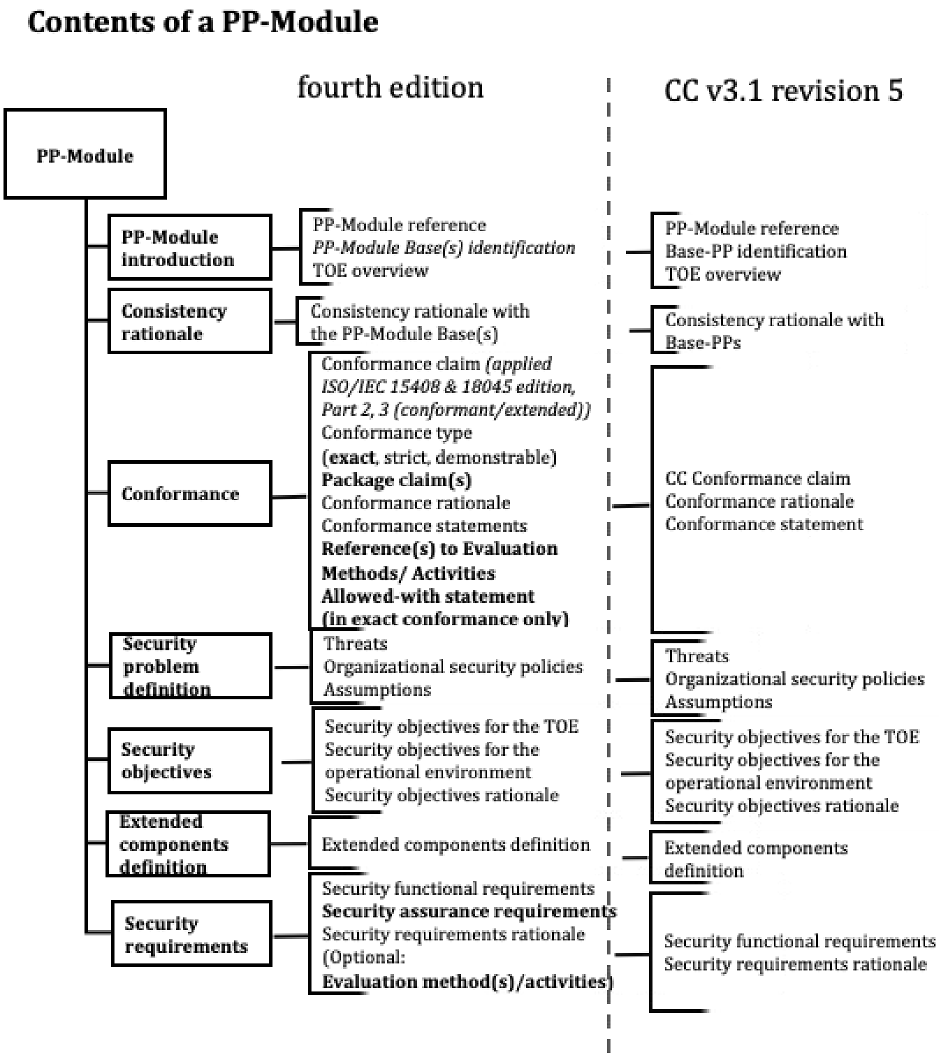

Contents of a PP-Module
fourth edition
CC v3.1 revision 5
PP-Module
PP-Module introduction
PP-Module reference
PP-Module Base(s) identification
TOE overview
Consistency rationale
Consistency rationale with the PP-Module Base(s)
Conformance
Conformance claim (applied ISO/IEC 15408 & 18045 edition, Part 2, 3 (conformant/extended))
Conformance type (exact, strict, demonstrable)
Package claim(s)
Conformance rationale
Conformance statements
Reference(s) to Evaluation Methods/ Activities
Allowed-with statement (in exact conformance only)
Security problem definition
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
(Optional: Evaluation method(s)/activities)
PP-Module reference
Base-PP identification
TOE overview
Consistency rationale with Base-PPs
CC Conformance claim
Conformance rationale
Conformance statement
Threats
Organizational security policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security objectives rationale
Extended components definition
Security functional requirements
Security requirements rationale

Figure 18 — Contents of a PP-Module — fourth edition vs CC version 3.1 revision 5

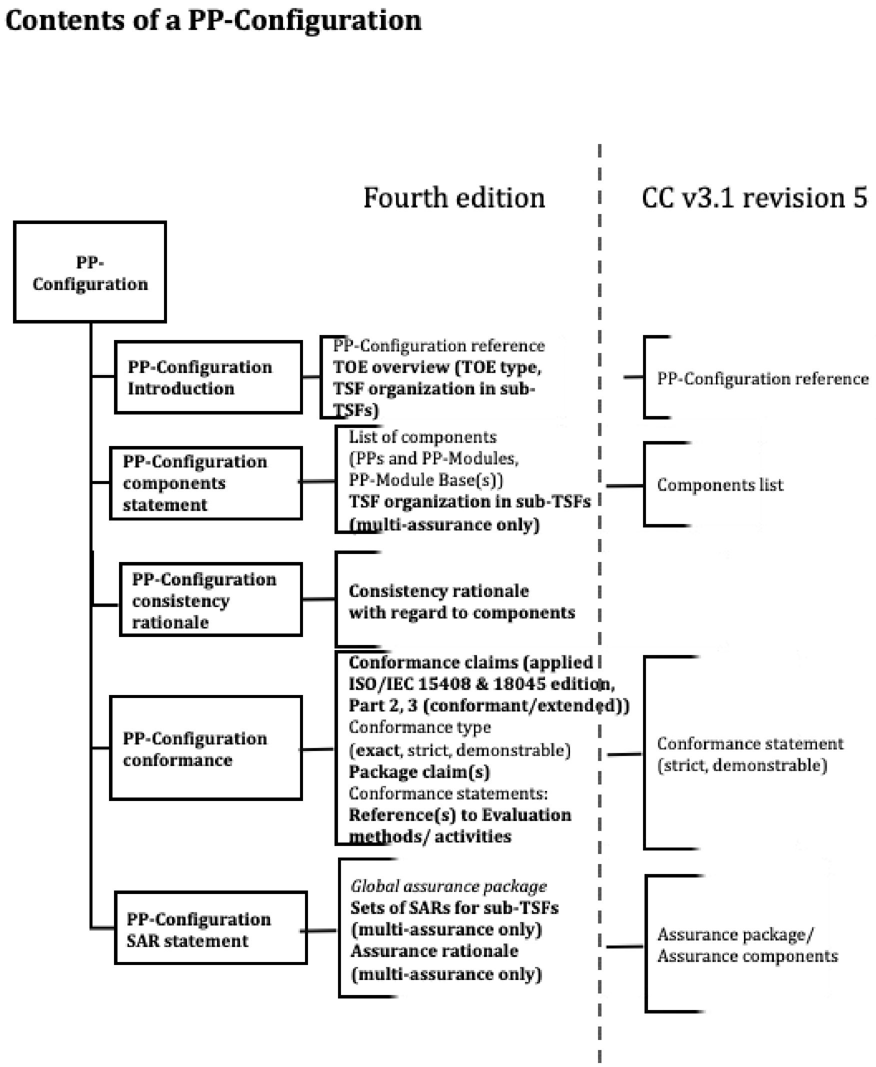

Contents of a PP-Configuration
Fourth edition
CC v3.1 revision 5
PP-Configuration
PP-Configuration Introduction
PP-Configuration reference
TOE overview (TOE type, TSF organization in sub-TSFs)
PP-Configuration reference
PP-Configuration components statement
List of components (PPs and PP-Modules, PP-Module Base(s))
TSF organization in sub-TSFs (multi-assurance only)
Components list
PP-Configuration consistency rationale
Consistency rationale with regard to components
PP-Configuration conformance
Conformance claims (applied ISO/IEC 15408 & 18045 edition, Part 2, 3 (conformant/extended))
Conformance type
(exact, strict, demonstrable)
Package claim(s)
Conformance statements:
Reference(s) to Evaluation methods/ activities
Conformance statement (strict, demonstrable)
PP-Configuration SAR statement
Global assurance package
Sets of SARs for sub-TSFs (multi-assurance only)
Assurance rationale (multi-assurance only)
Assurance package/ Assurance components

Figure 19 — Contents of a PP-Configuration — fourth edition vs CC version 3.1 revision 5

7.2 Changes in ISO/IEC 15408-2

SFRs that are used *de facto* in PPs have been introduced in the standard, while other SFRs are refactored to better reflect the state-of-the-art.

Table 3 illustrates the changes to the SFRs. The newly introduced families are indicated in **bold** text. The modified families are shown in *italics* and they are preceded by the * symbol.

For the comparison and the differences illustrated in the table below, CC v3.1 revision 5 (Part 2) [15] and the fourth edition of the ISO/IEC 15408-2 standard are used.

Table 3 — Changes in ISO/IEC 15408-2

Class	CC v3.1 revision 5	Fourth edition
FAU: Security Audit	FAU_ARP: Security audit automatic response	FAU_ARP: Security audit automatic response
	FAU_GEN: Security audit data generation	**FAU_GEN: Security audit generation*
	FAU_SAA: Security audit analysis	FAU_SAA: Security audit analysis
	FAU_SAR: Security audit review	FAU_SAR: Security audit review
	FAU_SEL: Security audit event selection	FAU_SEL: Security audit event selection
	FAU_STG: Security audit event storage	**FAU_STG: Security audit event storage*
FCO: Communication	FCO_NRO: Non-repudiation of origin	FCO_NRO: Non-repudiation of origin
	FCO_NRR: Non-repudiation of receipt	FCO_NRR: Non-repudiation of receipt
FCS: Cryptographic Support	FCS_CKM: Cryptographic key management	**FCS_CKM: Cryptographic key management*
	FCS_COP: Cryptographic operation	FCS_COP: Cryptographic operation
		FCS_RBG: Random bit generation
		FCS_RNG: Random number generation
FDP: User Data Protection	FDP_ACC: Access control policy	FDP_ACC: Access control policy
	FDP_ACF: Access control functions	FDP_ACF: Access control functions
	FDP_DAU: Data authentication	FDP_DAU: Data authentication
	FDP_ETC: Export from the TOE	**FDP_ETC: Export from the TOE*
	FDP_IFC: Information flow control policy	FDP_IFC: Information flow control policy
	FDP_IFF: Information flow control functions	FDP_IFF: Information flow control functions
		FDP_IRC: Information retention control
	FDP_ITC: Import from outside of the TOE	FDP_ITC: Import from outside of the TOE
	FDP_ITT: Internal TOE transfer	FDP_ITT: Internal TOE transfer
	FDP_RIP: Residual information protection	FDP_RIP: Residual information protection
	FDP_ROL: Rollback	FDP_ROL: Rollback

Class	CC v3.1 revision 5	Fourth edition
		FDP_SDC: Stored data confidentiality
	FDP_SDI: Stored data integrity	FDP_SDI: Stored data integrity
	FDP_UCT: Inter-TSF user data confidentiality transfer protection	FDP_UCT: Inter-TSF user data confidentiality transfer protection
	FDP_UIT: Inter-TSF user data integrity transfer protection	FDP_UIT: Inter-TSF user data integrity transfer protection
FIA: Identification and authentication	FIA_AFL: Authentication failures	FIA_AFL: Authentication failure~~s~~
		FIA_API: Authentication proof of identity
	FIA_ATD: User attribute definition	FIA_ATD: User attribute definition
	FIA_SOS: Specification of secrets	FIA_SOS: Specification of secrets
	FIA_UAU: User authentication	FIA_UAU: User authentication
	FIA_UID: User identification	FIA_UID: User identification
	FIA_USB: User-subject binding	FIA_USB: User-subject binding
FMT: Security Management		**FMT_LIM: Limited capabilities and availability**
	FMT_MOF: Management of functions in TSF	FMT_MOF: Management of functions in TSF
	FMT_MSA: Management of security attributes	FMT_MSA: Management of security attributes
	FMT_MTD: Management of TSF data	FMT_MTD: Management of TSF data
	FMT_REV: Revocation	FMT_REV: Revocation
	FMT_SAE: Security attribute expiration	FMT_SAE: Security attribute expiration
	FMT_SMF: Specification of management functions	FMT_SMF: Specification of management functions
	FMT_SMR: Security management roles	FMT_SMR: Security management roles
FPR: Privacy	FPR_ANO: Anonymity	FPR_ANO: Anonymity
	FPR_PSE: Pseudonymity	FPR_PSE: Pseudonymity
	FPR_UNL: Unlinkability	FPR_UNL: Unlinkability
	FPR_UNO : Unobservability	FPR_UNO : Unobservability
FPT: Protection of the TSF		**FPT_EMS: TOE Emanation**
	FPT_FLS: Fail secure	FPT_FLS: Fail secure

Class	CC v3.1 revision 5	Fourth edition
		FPT_INI: TSF initialization
	FPT_ITA: Availability of exported TSF data	FPT_ITA: Availability of exported TSF data
	FPT_ITC: Confidentiality of exported TSF data	FPT_ITC: Confidentiality of exported ~~TSF~~ data
	FPT_ITI: Integrity of exported TSF data	FPT_ITI: Integrity of exported TSF data
	FPT_ITT: Internal TOE TSF data transfer	FPT_ITT: Internal TOE TSF data transfer
	FPT_PHP: TSF physical protection	FPT_PHP: TSF physical protection
	FPT_RCV: Trusted recovery	FPT_RCV: Trusted recovery
	FPT_RPL: Replay detection	FPT_RPL: Replay detection
	FPT_SSP: State synchrony protocol	FPT_SSP: State synchrony protocol
	FPT_STM: Time stamps	**FPT_STM: Time stamps*
	FPT_TDC: Inter-TSF TSF data consistency	FPT_TDC: Inter-TSF TSF data consistency
	FPT_TEE: Testing of external entities	FPT_TEE: Testing of external entities
	FPT_TRC: Internal TOE TSF data replication consistency	FPT_TRC: Internal TOE TSF data replication consistency
	FPT_TST: TSF self-test	FPT_TST: TSF self-test
FRU: Resource utilization	FRU_FLT: Fault tolerance	FRU_FLT: Fault tolerance
	FRU_PRS: Priority of service	FRU_PRS: Priority of service
	FRU_RSA: Resource allocation	FRU_RSA: Resource allocation
FTA: TOE Access	FTA_LSA: Limitation on scope of selectable attributes	FTA_LSA: Limitation on scope of selectable attributes
	FTA_MCS: Limitation on multiple concurrent session	FTA_MCS: Limitation on multiple concurrent session
	FTA_SSL: Session locking and termination	FTA_SSL: Session locking and termination
	FTA_TAB: TOE access banners	**FTA_TAB: TOE access banners*
	FTA_TAH: TOE access history	FTA_TAH: TOE access history
	FTA_TSE: TOE session establishment	FTA_TSE: TOE session establishment
FTP: Trusted path/channels	FTP_ITC: Inter-TSF trusted channel	FTP_ITC: Inter-TSF trusted channel
		FTP_PRO: Trusted channel proto-

Class	**CC v3.1 revision 5**	**Fourth edition**
		col
	FTP_TRP: Trusted path	FTP_TRP: Trusted path

7.3 Changes in ISO/IEC 15408-3

Table 4 — Changes in ISO/IEC 15408-3

ISO/IEC 15408-3 fourth edition	
General	Text related to assurance packages (i.e. EALs and CAPs) has been moved to ISO/IEC 15408-5.
Summary	Changes already introduced in CC 3.1 revision 5 have been included. Several assurance classes and families were updated: - ACE: updated to cover the new or modified concepts such as exact conformance and allowed-with statements, and multi-assurance PP-Configurations; - ADV_SPM: redefined to focus on the formal model of the complete TSF and the proof of a set of properties that covers the complete set of security objectives; - ALC_TDA: new class concerned with the generation of certain artefacts for assessing the trustworthiness of the development process; - APE: updated to cover the new or modified concepts such as exact conformance and allowed-with statements; Direct Rationale PPs, specification of evaluation methods/activities using ISO/IEC 15408-4; - ASE: updated to cover the new or modified concepts such as exact conformance, Direct Rationale STs, specification of evaluation methods/activities using ISO/IEC 15408-4; - _COMP: new classes applicable to the composite evaluations.

In the following tables the important changes and additions to each class are illustrated. The newly introduced elements and families are indicated in **bold** text and they are accompanied by a brief description. The modified elements and families are shown in *italics* and they are accompanied by a brief description. For increased visibility, families that have been introduced or modified are highlighted in grey.

For the comparison and the differences illustrated in the tables below, CC v3.1 revision 5 (Part 3) [16] and the fourth edition of the ISO/IEC 15408-3 standard are used.

Table 5 — Class APE — fourth edition vs CC version 3.1 revision 5

Class APE: Protection Profile evaluation		
CC v3.1 revision 5	*Fourth Edition*	
PP Introduction APE_INT.1	PP Introduction APE_INT.1	
Conformance claims APE_CCL.1	Conformance claims *APE_CCL.1*	
Developer action elements	Developer action elements	
APE_CCL.1.1D	APE_CCL.1.1D	
APE_CCL.1.2D	APE_CCL.1.2D	
APE_CCL.1.3D	APE_CCL.1.3D	
Content and presentation elements	Content and presentation elements	
APE_CCL.1.1C	*APE_CCL.1.1C*	Slight changes for ISO/IEC 15408 identification
APE_CCL.1.2C	*APE_CCL.1.2C*	
APE_CCL.1.3C	*APE_CCL.1.3C*	
APE_CCL.1.4C	APE_CCL.1.4C	
APE_CCL.1.5C	APE_CCL.1.5C	
APE_CCL.1.6C	**APE_CCL.1.6C**	Correspond to former APE_CCL.1.6C split in 2 for functional and assurance packages, respectively
	APE_CCL.1.7C	
	APE_CCL.1.8C	New element for conformance to PP description as PP Conformant
APE_CCL.1.7C	APE_CCL.1.9C	
APE_CCL.1.8C	*APE_CCL.1.10C*	Extended to include functional packages
APE_CCL.1.9C	*APE_CCL.1.11C*	
APE_CCL.1.10C	*APE_CCL.1.12C*	
APE_CCL.1.11C	*APE_CCL.1.13C*	Extended to include exact conformance
	APE_CCL.1.14C	New elements for allowed-with statements for the exact conformance case
	APE_CCL.1.15C	
	APE_CCL.1.16C	New element for evaluation methods and evaluation activities identification
Evaluator action elements	Evaluator action elements	

Class APE: Protection Profile evaluation	
CC v3.1 revision 5	*Fourth Edition*
APE_CCL.1.1E	APE_CCL.1.1E
Security problem definition APE_SPD .1	Security problem definition APE_SPD.1
Security objectives APE_OBJ.1	Security objectives *APE_OBJ.1*
Developer action elements APE_OBJ.1.1D	Developer action elements APE_OBJ.1.1D **APE_OBJ.1.2D** New element requiring a security objective rationale
Content and presentation elements APE_OBJ.1.1C	Content and presentation elements APE_OBJ.1.1C **APE_OBJ.1.2C** **APE_OBJ.1.3C** New elements for the security objective rationale
Evaluator action elements APE_OBJ.1.1E	Evaluator action elements APE_OBJ.1.1E
APE_OBJ.2	APE_OBJ.2
Extended components definition APE_ECD.1	Extended components definition APE_ECD.1
Security requirements APE_REQ.1	Security requirements *APE_REQ.1*
Developer action elements APE_REQ.1.1D APE_REQ.1.2D	Developer action elements APE_REQ.1.1D APE_REQ.1.2D
Content and presentation elements APE_REQ.1.1C APE_REQ.1.2C APE_REQ.1.3C APE_REQ.1.4C APE_REQ.1.5C	Content and presentation elements APE_REQ.1.1C APE_REQ.1.2C APE_REQ.1.3C APE_REQ.1.4C APE_REQ.1.5C **APE_REQ.1.6C**

New elements related to the security requirements rationale

Class APE: Protection Profile evaluation	
CC v3.1 revision 5	*Fourth Edition*
	APE_REQ.1.7C
	APE_REQ.1.8C
	APE_REQ.1.9C
APE_REQ.1.6C	APE_REQ.1.10C
Evaluator action elements	Evaluator action elements
APE_REQ.1.1E	APE_REQ.1.1E
APE_REQ.2	APE_REQ.2

Table 6 — Class ACE — fourth edition vs CC version 3.1 revision 5

Class ACE: Protection Profile Configuration evaluation	
CC v3.1 revision 5	*Fourth Edition*
PP-Module Introduction	PP-Module Introduction
ACE_INT.1	*ACE_INT.1*
Developer action elements	Developer action elements
ACE_INT.1.1D	ACE_INT.1.1D
Content and presentation elements	Content and presentation elements
ACE_INT.1.1C	**ACE_INT.1.1C**
ACE_INT.1.2C	**ACE_INT.1.2C**
	ACE_INT.1.3C
	ACE_INT.1.4C
	ACE_INT.1.5C
	ACE_INT.1.6C
	ACE_INT.1.7C
	ACE_INT.1.8C
	ACE_INT.1.9C
Evaluator action elements	Evaluator action elements
ACE_INT.1.1E	ACE_INT.1.1E
PP-Module conformance claims	PP-Module conformance claims
ACE_CCL.1	*ACE_CCL.1*
Developer action elements	Developer action elements
ACE_CCL.1.1D	ACE_CCL.1.1D

All elements have been newly added in order to cover the identification of PP-Module Base(s), the dependency structure of PP-Module Base(s), TOE overview(s), etc.

Element requiring a conformance statement

Class ACE: Protection Profile Configuration evaluation	
CC v3.1 revision 5	*Fourth Edition*
	ACE_CCL.1.2D
Content and presentation elements	Content and presentation elements
ACE_CCL.1.1C	*ACE_CCL.1.1C* Slight changes for ISO/IEC 15408 identification
ACE_CCL.1.2C	*ACE_CCL.1.2C*
	ACE_CCL.1.3C New element for description of conformance type
	ACE_CCL.1.4C New element for description of conformance to ISO/IEC 15408-3
	ACE_CCL.1.5C
ACE_CCL.1.4C	ACE_CCL.1.6C
ACE_CCL.1.3C	
	ACE_CCL.1.7C New element for description of conformance to functional packages
	ACE_CCL.1.8C New elements for identification
	ACE_CCL.1.9C
	ACE_CCL.1.10C New element for allowed-with statements for the exact conformance case
	ACE_CCL.1.11C New element for evaluation methods and evaluation activities
Evaluator action elements	Evaluator action elements
ACE_CCL.1.1E	ACE_CCL.1.1E
PP-Module SPD	PP-Module Security problem definition
ACE_SPD.1	ACE_SPD.1
PP-Module Security objectives	PP-Module Security objectives
	ACE_OBJ.1- PP-Module security objectives for the operational environment
ACE_OBJ.1	ACE_OBJ.2

Class ACE: Protection Profile Configuration evaluation	
CC v3.1 revision 5	*Fourth Edition*
PP-Module extended components definition	PP-Module extended components definition
ACE_ECD.1	*ACE_ECD.1* Developer and content and presentation elements were slightly changed.
PP-Module security requirements	PP-Module security requirements
ACE_REQ.1	*ACE_REQ.1*
Dev. action elements	Developer action elements
ACE_REQ.1.1D	*ACE_REQ.1.1D extended to SFRs and SARs*
ACE_REQ.1.2D	ACE_REQ.1.2D
Content and presentation elements	Content and presentation elements
ACE_REQ.1.1C	
ACE_REQ.1.2C	*ACE_REQ.1.1C extended to SFRs and SARs*
	ACE_REQ.1.2C extended to SFRs and SARs
ACE_REQ.1.3C	
ACE_REQ.1.4C	ACE_REQ.1.3C
ACE_REQ.1.5C	ACE_REQ.1.4C
ACE_REQ.1.6C	*ACE_REQ.1.5C extended to SFRs and SARs*
ACE_REQ.1.7C	*ACE_REQ.1.6C*
	ACE_REQ.1.7C
	ACE_REQ.1.8C demonstrate that SFRs enforce all OSPs
	ACE_REQ.1.9C explain why SARs were chosen
	ACE_REQ.1.10C internal consistency for the rationale
Evaluator action elements	Evaluator action elements
ACE_REQ.1.1E	ACE_REQ.1.1E
	ACE_REQ.2 PP-Module derived security requirements Component added for the case in which the SFRs are derived from the security objectives for the TOE
PP-Module consist.	PP-Module consistency
ACE_MCO.1	*ACE_MCO.1*
Dev. action elements	Developer action elements
ACE_MCO.1.1D	*ACE_MCO.1.1D*

Class ACE: Protection Profile Configuration evaluation	
CC v3.1 revision 5	*Fourth Edition*
	ACE_MCO.1.2D new element requiring an assurance rationale
Content and presentation elements	Content and presentation elements
ACE_MCO.1.1C	*ACE_MCO.1.1C*
	ACE_MCO.1.2C
ACE_MCO.1.2C	*ACE_MCO.1.3C* extended
ACE_MCO.1.3C	*ACE_MCO.1.4C* extended
ACE_MCO.1.4C	*ACE_MCO.1.5C* extended
	ACE_MCO.1.6C **ACE_MCO.1.7C** New elements for the assurance rationale
Evaluator action elements	Evaluator action elements
ACE_MCO.1.1E	ACE_MCO.1.1E
PP-Configuration consistency	PP-Configuration consistency
ACE_CCO.1	*ACE_CCO.1*
Developer action elements	Developer action elements
ACE_CCO.1.1D	ACE_CCO.1.1D
ACE_CCO.1.2D	ACE_CCO.1.2D
	ACE_CCO.1.3D element for TOE overview
ACE_CCO.1.3D	*ACE_CCO.1.4D* element for conformance claim
	ACE_CCO.1.5D conformance statement within claim
ACE_CCO.1.4D	**ACE_CCO.1.6D** element for consistency rationale
	ACE_CCO.1.7D
	ACE_CCO.1.8D element for evaluation methods and activities
Content and presentation elements	Content and presentation elements
ACE_CCO.1.1C	ACE_CCO.1.1C
ACE_CCO.1.2C	ACE_CCO.1.2C
ACE_CCO.1.3C	
ACE_CCO.1.4C	
ACE_CCO.1.5C	
	ACE_CCO.1.3C-ACE_CCO.1.21C new elements
Evaluator action elements	Evaluator action elements

Class ACE: Protection Profile Configuration evaluation	
CC v3.1 revision 5	*Fourth Edition*
ACE_CCO.1.1E	ACE_CCO.1.1E
ACE_CCO.1.2E	ACE_CCO.1.2E

Table 7 — Class ASE — fourth edition vs CC version 3.1 revision 5

Class ASE: Security Target evaluation	
CC v3.1 revision 5	*Fourth Edition*
ST Introduction	ST Introduction
ASE_INT.1	*ASE_INT.1*
Developer action elements	Developer action elements
ASE_INT.1.1D	ASE_INT.1.1D
Content and presentation elements	Content and presentation elements
ASE_INT.1.1C	ASE_INT.1.1C
ASE_INT.1.2C	ASE_INT.1.2C
ASE_INT.1.3C	ASE_INT.1.3C
ASE_INT.1.4C	ASE_INT.1.4C
ASE_INT.1.5C	ASE_INT.1.5C
ASE_INT.1.6C	ASE_INT.1.6C
	ASE_INT.1.7C element for multi-assurance ST
ASE_INT.1.7C	ASE_INT.1.8C
ASE_INT.1.8C	ASE_INT.1.9C
Evaluator action elements	Evaluator action elements
ASE_INT.1.1E	ASE_INT.1.1E
ASE_INT.1.2E	ASE_INT.1.2E
Conformance claims	Conformance claims
ASE_CCL.1	*ASE_CCL.1*
Developer action elements	Developer action elements
ASE_CCL.1.1D	APE_CCL.1.1D
ASE_CCL.1.2D	APE_CCL.1.2D

Class ASE: Security Target evaluation		
CC v3.1 revision 5	*Fourth Edition*	
Content and presentation elements	Content and presentation elements	
ASE_CCL.1.1C	*ASE_CCL.1.1C*	Slight changes for ISO/IEC 15408 identification
ASE_CCL.1.2C	*ASE_CCL.1.2C*	
ASE_CCL.1.3C	*ASE_CCL.1.3C*	
ASE_CCL.1.4C	ASE_CCL.1.4C	
ASE_CCL.1.5C	*ASE_CCL.1.5C*	
ASE_CCL.1.6C	ASE_CCL.1.6C	
	ASE_CCL.1.7C	Conformance to PP descrip-
ASE_CCL.1.7C	*ASE_CCL.1.8C*	
ASE_CCL.1.8C	*ASE_CCL.1.9C*	
ASE_CCL.1.9C	*ASE_CCL.1.10C*	
ASE_CCL.1.10C	*ASE_CCL.1.11C*	
	ASE_CCL.1.12C	New element for conformance
	ASE_CCL.1.13C	New element for evaluation methods and activities identification
Evaluator action elements	Evaluator action elements	
ASE_CCL.1.1E	ASE_CCL.1.1E	
Security problem definition	Security problem definition	
ASE_SPD .1	ASE_SPD.1	
Security objectives	Security objectives	
ASE_OBJ.1	*ASE_OBJ.1*	
Developer action elements	Developer action elements	
ASE_OBJ.1.1D	ASE_OBJ.1.1D	New element requiring a security objective rationale
	ASE_OBJ.1.2D	
Content and presentation elements	Content and presentation elements	
ASE_OBJ.1.1C	ASE_OBJ.1.1C	
	ASE_OBJ.1.2C	New elements for the security objective rationale
	ASE_OBJ.1.3C	
Evaluator action elements	Evaluator action elements	
ASE_OBJ.1.1E	ASE_OBJ.1.1E	

Class ASE: Security Target evaluation	
CC v3.1 revision 5	*Fourth Edition*
ASE_OBJ.2	ASE_OBJ.2
Extended components definition	Extended components definition
ASE_ECD.1	ASE_ECD.1
Security requirements	Security requirements
ASE_REQ.1	*ASE_REQ.1*
Developer action elements	Developer action elements
ASE_REQ.1.1D	ASE_REQ.1.1D
ASE_REQ.1.2D	ASE_REQ.1.2D
Content and presentation elements	Content and presentation elements
ASE_REQ.1.1C	ASE_REQ.1.1C
	ASE_REQ.1.2C New elements for single and multi-assurance STs
	ASE_REQ.1.3C
ASE_REQ.1.2C	ASE_REQ.1.4C
	ASE_REQ.1.5C natural language description
ASE_REQ.1.3C	ASE_REQ.1.6C
ASE_REQ.1.4C	ASE_REQ.1.7C
ASE_REQ.1.5C	ASE_REQ.1.8C
	ASE_REQ.1.9C
	ASE_REQ.1.10C New elements for the security rationale
	ASE_REQ.1.11C
ASE_REQ.1.6C	ASE_REQ.1.12C
	ASE_REQ.1.13C new element for evaluation methods and activities
Evaluator action elements	Evaluator action elements
ASE_REQ.1.1E	ASE_REQ.1.1E
ASE_REQ.2	*ASE_REQ.2* In the content and presentation elements, two new elements **ASE_REQ.2.2C** and **ASE_REQ.2.3C** Concerning the statement of security requirements in the single-/multi-assurance case were added.
TOE summary specification	TOE summary specification
ASE_TSS.1	ASE_TSS.1

Class ASE: Security Target evaluation	
CC v3.1 revision 5	*Fourth Edition*
ASE_TSS.2	ASE_TSS.2
	Consistency of composite product ST **ASE_COMP** New family added for determining whether the ST of the composite product does not contradict the ST of the related base component.

Table 8 — Class ADV — fourth edition vs CC version 3.1 revision 5

Class ADV: Development	
CC v3.1 revision 5	*Fourth Edition*
Security Architecture ADV_ARC.1	Security Architecture ADV_ARC.1
Functional specification ADV_FSP.1 ADV_FSP.2 ADV_FSP.3 ADV_FSP.4 ADV_FSP.5 ADV_FSP.6	Functional specification ADV_FSP.1 ADV_FSP.2 ADV_FSP.3 ADV_FSP.4 ADV_FSP.5 ADV_FSP.6
Implementation representation ADV_IMP.1 ADV_IMP.2	Implementation representation ADV_IMP.1 ADV_IMP.2
TSF internals ADV_INT.1 ADV_INT.2 ADV_INT.3	TSF internals ADV_INT.1 ADV_INT.2 ADV_INT.3
Security policy modelling ADV_SPM.1	**Formal TSF model** **ADV_SPM.1** All the developer action elements, content and presentation elements, and evaluator action elements have been modified and supplemented to correspond to a complete formal TSF model.

Class ADV: Development	
CC v3.1 revision 5	*Fourth Edition*
TOE design	TOE design
ADV_TDS.1	ADV_TDS.1
ADV_TDS.2	ADV_TDS.2
ADV_TDS.3	ADV_TDS.3
ADV_TDS.4	ADV_TDS.4
ADV_TDS.5	ADV_TDS.5
ADV_TDS.6	ADV_TDS.6
	Composite design compliance
	ADV_COMP.1
	Newly introduced family for determining whether the requirements on the dependent component, imposed by the related base component, are fulfilled in the composite product.

Table 9 — Class AGD — fourth edition vs CC version 3.1 revision 5

Class AGD: Guidance documents	
CC v3.1 revision 5	*Fourth Edition*
Operational user guidance	Operational user guidance
AGD_OPE.1	AGD_OPE.1
Preparative procedures	Preparative procedures
AGD_PRE.1	AGD_PRE.1

Table 10 — Class ALC — fourth edition vs CC version 3.1 revision 5

Class ALC: Life-cycle support	
CC v3.1 revision 5	*Fourth Edition*
CM capabilities	CM capabilities
ALC_CMC.1	ALC_CMC.1
ALC_CMC.2	ALC_CMC.2
ALC_CMC.3	ALC_CMC.3

Class ALC: Life-cycle support	
CC v3.1 revision 5	*Fourth Edition*
ALC_CMC.4 ALC_CMC.5	ALC_CMC.4 ALC_CMC.5
CM scope ALC_CMS.1 ALC_CMS.2 ALC_CMS.3 ALC_CMS.4 ALC_CMS.5	CM scope ALC_CMS.1 ALC_CMS.2 ALC_CMS.3 ALC_CMS.4 ALC_CMS.5
Delivery ALC_DEL.1	Delivery ALC_DEL.1
Development security ALC_DVS.1 ALC_DVS.2	Development security ALC_DVS.1 ALC_DVS.2
Flaw remediation ALC_FLR.1 ALC_FLR.2 ALC_FLR.3	Flaw remediation ALC_FLR.1 ALC_FLR.2 ALC_FLR.3
Life-cycle definition ALC_LCD.1 ALC_LCD.2	Life-cycle definition ALC_LCD.1 *ALC_LCD.2* A new evaluator action element **ALC_LCD.2.2E** was added.
	TOE Development Artefact **ALC_TDA.1** Uniquely identifying implementation representation **ALC_TDA.2** Matching CMS scope of implementation representation **ALC_TDA.3** Regenerate TOE with well-defined development tools Newly introduced family aiming to add trust to the development process or development.

Class ALC: Life-cycle support	
CC v3.1 revision 5	*Fourth Edition*
Tools and techniques	Tools and techniques
ALC_TAT.1	ALC_TAT.1
ALC_TAT.2	ALC_TAT.2
ALC_TAT.3	ALC_TAT.3
	Integration of composition parts and consistency check of delivery procedures
	ALC_COMP.1
	Newly introduced family for integration of composition parts and consistency check of delivery procedures.

Table 11 — Class ATE — fourth edition vs CC version 3.1 revision 5

Class ATE: Tests	
CC v3.1 revision 5	*Fourth Edition*
Coverage	Coverage
ATE_COV.1	ATE_COV.1
ATE_COV.2	ATE_COV.2
ATE_COV.3	ATE_COV.3
Depth	Depth
ATE_DPT.1	ATE_DPT.1
ATE_DPT.2	ATE_DPT.2
ATE_DPT.3	ATE_DPT.3
ATE_DPT.4	ATE_DPT.4
Functional tests	Functional tests
ATE_FUN.1	ATE_FUN.1
ATE_FUN.2	ATE_FUN.2
Independent testing	Independent testing
ATE_IND.1	ATE_IND.1
ATE_IND.2	ATE_IND.2
ATE_IND.3	ATE_IND.3

Class ATE: Tests	
CC v3.1 revision 5	*Fourth Edition*
	Composite functional testing **ATE_COMP.1** Newly introduced family aiming to determine whether a composite product exhibits the properties necessary to satisfy the functional re-

Table 12 — Class AVA — fourth edition vs CC version 3.1 revision 5

Class AVA: Vulnerability assessment	
CC v3.1 revision 5	*Fourth Edition*
Vulnerability assessment AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5	Vulnerability assessment AVA_VAN.1 *AVA_VAN.2* *AVA_VAN.3* *AVA_VAN.4* *AVA_VAN.5* New elements (***.2D and *.2C**) have been added and **.2E* has been modified. * stands for AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, and AVA_VAN.5
	Composite product vulnerability assessment **AVA_COMP.1** Newly introduced family aiming to determine the exploitability of flaws or weaknesses in the composite product in the intended environment.

Table 13 — Class ACO — fourth edition vs CC version 3.1 revision 5

Class ACO: Composition	
CC v3.1 revision 5	*Fourth Edition*
Composition rationale	Composition rationale

ACO_COR.1	ACO_COR.1
Development evidence	Development evidence
ACO_DEV.1	ACO_DEV
ACO_DEV.2	ACO_DEV.2
ACO_DEV.3	ACO_DEV.3
Reliance of dependent component	Reliance of dependent component
ACO_REL.1	ACO_REL.1
ACO_REL.2	ACO_REL.2
Composed TOE testing	Composed TOE testing
ACO_CTT.1	ACO_CTT.1
ACO_CTT.2	ACO_CTT.2
Composition vulnerability analysis	Composition vulnerability analysis
ACO_VUL.1	ACO_VUL.1
ACO_VUL.2	ACO_VUL.2
ACO_VUL.3	ACO_VUL.3

7.4 Addition of ISO/IEC 15408-4

Table 14 — ISO/IEC 15408-4

ISO/IEC 15408-4 fourth edition	
General	This is a new part of ISO/IEC 15408. This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.
General model of evaluation methods and evaluation activities	Clause 4 describes the concepts and the model and explains the derivation of evaluation methods and evaluation activities relying on ISO/IEC 15408-3 and ISO/IEC 18045.
Structure of evaluation methods	Clause 5 describes the structure of an evaluation method as follows: 5.1 Overview 5.2 Specification of an Evaluation Method 5.2.1 Overview

ISO/IEC 15408-4 fourth edition	
	5.2.2 Identification of evaluation methods 5.2.3 Entity responsible for the evaluation method 5.2.4 Scope of the evaluation method 5.2.5 Dependencies 5.2.6 Required input from the developer or other entities 5.2.7 Required tool types 5.2.8 Required evaluator competences 5.2.9 Requirements for reporting 5.2.10 Rationale for the evaluation method 5.2.11 Additional verb definitions 5.2.12 Set of evaluation activities
Structure of evaluation activities	Clause 6 describes the structure of evaluation activities as follows: 6.1 Overview 6.2 Specification of an evaluation activity 6.2.1 Unique Identification of the evaluation activity 6.2.2 Objective of the evaluation activity 6.2.3 Evaluation activity links to SFRs, SARs, and other evaluation activities 6.2.4 Required input from the developer or other entities 6.2.5 Required tool types 6.2.6 Required evaluator competences 6.2.7 Assessment strategy 6.2.8 Pass/fail criteria 6.2.9 Requirements for reporting 6.2.10 Rationale for the evaluation activity

7.5 Addition of ISO/IEC 15408-5

Table 15 — ISO/IEC 15408-5

ISO/IEC 15408-5 fourth edition	
Summary	The text in regard to assurance packages (EAL and CAP) from CC v3.1 revision

ISO/IEC 15408-5 fourth edition	
	5 [16] has been incorporated into ISO/IEC 15408-5. New assurance packages have been proposed to facilitate the evaluation of composition and Direct Rationale PPs and STs: — COMP (Composite Product); — PPA (Protection Profile Assurance); — STA (Security Target Assurance).

7.6 Changes in ISO/IEC 18045

Table 16 — Changes in ISO/IEC 18045

ISO/IEC 18045 fourth edition	
Structure	This part of the standard has been restructured to allow the grouping of like topics appropriately.
Terms and definitions	Consolidation of terms given in ISO/IEC 18045 into ISO/IEC 15408-1.
Summary	Every change introduced in the ISO/IEC 15408 series is reflected in the new edition of ISO/IEC 18045. An exhaustive list of the introduced changes exceeds the scope of this document, but below a subset of the modifications and additions is indicated: — work units corresponding to ASE_COMP, ALC_COMP, ADV_COMP, ATE_COMP, and AVA_COMP defined in Appendix 1.1 of JIL *Composite product evaluation for Smart Cards and similar devices* have been included; — work units for the new APE, ACE, ASE components describing how evaluation methods and activities are to be presented and evaluated have been defined; — work units related to exact conformance for the new APE, ACE, ASE components have been defined; — work units for ADV_SPM have been defined; — work units related to multi-assurance for the new APE, ACE, ASE components have been defined; — work units for ALC_TAD have been defined.

Bibliography

This bibliography contains references to further material and standards useful to the readers of this document. For the referenced ISO/IEC 15408 and ISO/IEC 18045 documents, the cited edition applies. For the rest of the references, the reader is recommended to refer to the latest edition of the referenced document.

[1] JIL — The Application of CC to Integrated Circuits — Version 3.0 — February 2009

[2] JIL — Application of Attack Potential to Smartcards — Version 3.1 — June 2020

[3] JIL — Application of Attack Potential to Hardware Devices with Security Boxes — Version 3.0 — June 2020

[4] JIL — Security Architecture requirements (ADV_ARC) — for smart cards and similar devices — Version 2.0 — January 2012

[5] JIL — Minimum Site Security Requirements — Version 3.0 — February 2020

[6] Supporting Document — Mandatory Technical Document — Full Drive Encryption: Authorization Acquisition — January 2015 — Version 1.0 — CCDB — 2015-01-003

[7] Supporting Document — Mandatory Technical Document — Full Drive Encryption: Encryption Engine — January 2015 — Version 1.0 — CCDB-2015-01-004

[8] Supporting Document — Mandatory Technical Document — Evaluation Activities for Stateful Traffic Filter Firewalls cPP — February 2015 — Version 1.0 — CCDB-2015-01-002

[9] Supporting Document — Mandatory Technical Document — Evaluation Activities for Network Device cPP — February 2015 — Version 1.0 — CCDB-2015-01-001

[10] collaborative Protection Profile for Network Devices — Version 2.2E — 27-03-2020

[11] collaborative Protection Profile for Full Drive Encryption — Authorization Acquisition — Version 2.0E — 01-02- 2019

[12] collaborative Protection Profile for Full Drive Encryption — Encryption Engine — Version 2.0E — 01-02- 2019

[13] collaborative Protection Profile for Stateful Traffic Filter Firewalls — Version 1.4 — 01-07-2020

[14] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-001)

[15] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-002)

[16] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, April 2017, Version 3.1 Revision 5 (CCMB-2017-04-003)

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

[18] CC and CEM addenda. Exact Conformance, Selection-based SFRs, Optional SFRs, May 2017, Version 0.5 (CCDB-2017-05-XXX)

[19] ISO/IEC 15408-1:2009, Information technology — IT security techniques — Evaluation criteria for IT security — Part 1: Vocabulary, introduction and general requirements

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

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

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

[23] ISO/IEC 15408-1:2021, Information technology — IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general requirements

[24] ISO/IEC 15408-2: 2021, Information technology — IT Security techniques — Evaluation criteria for IT security — Part 2: Security functional components

[25] ISO/IEC 15408-3: 2021 Information technology — IT Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[26] ISO/IEC 15408-4: 2021, Information technology — IT Security techniques — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities

[27] ISO/IEC 15408-5: 2021, Information technology — IT Security techniques — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

[28] ISO/IEC 18045: 2021, Information technology — IT Security techniques — Methodology for IT security evaluation