TECHNICAL REPORT

ISO/IEC TR 22216

First edition
2022-05

Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

Sécurité de l'information, cybersécurité et protection de la vie privée — Nouveaux concepts et modifications dans l'ISO/IEC 15408:2022 et l'ISO/IEC 18045:2022

Reference number
ISO/IEC TR 22216:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

List of Figures

List of Tables

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

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

Introduction

The ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 include substantial changes compared to the former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 and subsequent Common Criteria and Common Evaluation Methodology Version 3.1 Revision 5 [14]-[17] (also called CC 3.1 and CEM 3.1 in the following). The edition:

— covers complex products and communities' needs;

— offers compatibility with currently existing processes.

The goal of the revision of the ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 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 Target of Evaluations (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 Mutual Recognition Agreements (MRAs), and their stakeholders,

NOTE The only existing recognition arrangements are the Common Criteria Recognition Arrangement[1] (CCRA) and Senior Officials Group — Information Systems Security Mutual Recognition Agreement[2] (SOG-IS MRA).

— offer continued alignment with the supporting documents developed in the context of the existing MRAs;

— take into consideration commonly used approaches for the criteria (including but not limited to CC 3.1 and CEM 3.1) and introduce technical changes accordingly.

This document is meant to provide information and support to users of the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022. 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, 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 CC 3.1 and CEM 3.1.

1) https://www.commoncriteriaportal.org/ccra/index.cfm

2) https://sogis.org

Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022

1 Scope

This document:

— introduces the break down between the former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008) and ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008 and the new parts introduced in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022;

— presents the concepts newly introduced 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 ISO/IEC 15408:2022 series and ISO/IEC 18045:2022, respectively;

— maps the evolutions between the CC 3.1 and CEM 3.1 and the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022, respectively.

2 Normative references

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

ISO/IEC 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, and ISO/IEC 18045:2022 apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp;

— IEC Electropedia: available at https://www.electropedia.org/.

3.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, and ISO/IEC 18045:2022 and the following apply.

CC Common Criteria

CEM Common Evaluation Methodology

4 Overview

4.1 General

This document is meant to help users of the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 to understand how they can adapt the use of the standards 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 newly introduced or modified in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022.

4.2 Structure of this document

This document has the following structure:

— subclauses 4.3 to 4.5 give an overview of the new structure of the documents in the ISO/IEC 15408:2022 series with the newly introduced technical concepts (in 4.3), usage information of this document for transitional information (in 4.4) and usage information of the ISO/IEC 15408:2022 series for specific needs, respectively (in 4.5);

— in Clause 5, the major new concepts introduced in the ISO/IEC 15408:2022 series are presented, classified and discussed;

— Clause 6 focuses on concrete guidelines for applying the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 for specific needs;

— finally, in Clause 7 the changes introduced and that are specific to each document in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 are mapped and intuitively presented.

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

The ISO/IEC 15408:2022 series now include five parts.

The ISO/IEC 15408:2022 series has been modified to include two additional parts, namely ISO/IEC 15408-4:2022 and ISO/IEC 15408-5:2022.

ISO/IEC 15408-4:2022 is a new part that defines a framework for deriving evaluation methods and activities from the evaluation methodology given in ISO/IEC 18045:2022. These derived evaluation methods and activities can potentially be included in PPs, PP-Modules, packages, STs and any documents supporting them.

ISO/IEC 15408-5:2022 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 15408-3:2008 and CC 3.1.

Figure 1 illustrates the structure and partition of the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 documents as well as their relationship to the previous editions.

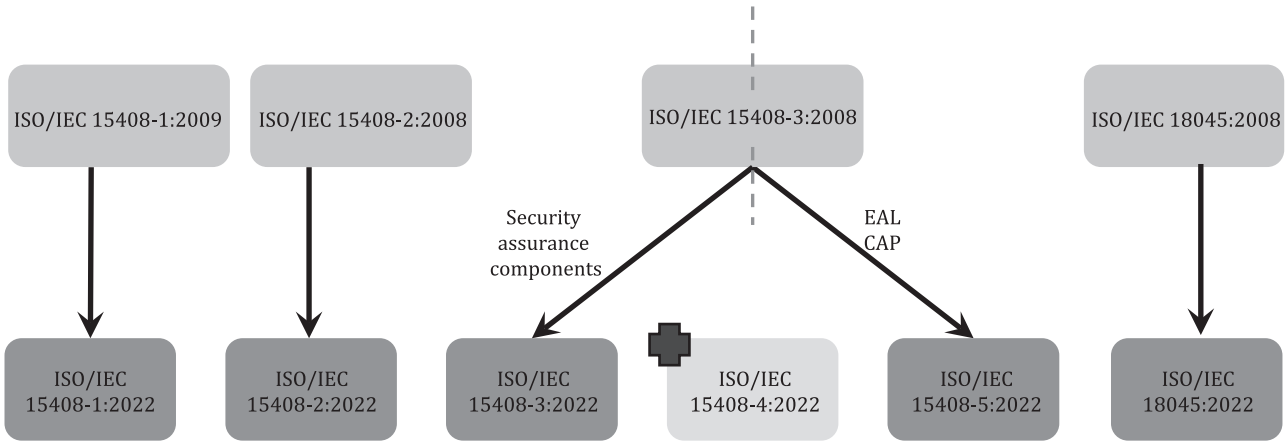

Figure 1 — ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 structure and mapping to former ISO/IEC 15408 series (ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008, ISO/IEC 15408-3:2008) and ISO/IEC 18045:2008

Table 1 presents the concepts newly introduced in the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 and provides a brief, descriptive overview for each.

Table 1 — Overview of newly introduced concepts

ISO/IEC 15408 Document	Newly introduced concept	Description	Impact
ISO/IEC 15408-1:2022	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 15408-3:2022 ISO/IEC 18045:2022
	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 15408-3:2022 ISO/IEC 18045:2022
	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 15408-3:2022 ISO/IEC 18045:2022
	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 15408-3:2022 ISO/IEC 18045:2022

Table 1 *(continued)*

ISO/IEC 15408 Document	Newly introduced concept	Description	Impact
ISO/IEC 15408-1:2022	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 15408-3:2022 ISO/IEC 18045:2022
	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 15408-3:2022 ISO/IEC 18045:2022
ISO/IEC 15408-3:2022	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 behaviour 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.	ISO/IEC 18045:2022

4.4 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 Clause 5. For existing PPs, Figure 16 in Clause 7 illustrates the changes in mandatory content with respect to CC 3.1.

For developers it is noted that by default, requirements contained in existing STs are fully compatible. The transition to the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 has no impact for developers unless new features of the ISO/IEC 15408:2022 series 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 15408:2022 series and ISO/IEC 18045:2022 in their entirety. However, Clause 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 ISO/IEC 15408:2022 series for the APE, ACE, ASE, ALC, ATE and AVA components.

4.5 Using the ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 for specific needs

The details concerning evaluation methods and security components are described in Clause 5 and Clause 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 Certification Bodies (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 ISO/IEC 15408:2022 series and ISO/IEC 18045:2022

5.1 Approaches to security evaluation

5.1.1 General

The ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 now support two different approaches to evaluation, as shown in Figure 2: the attack-based approach and the specification-based approach.

The ISO/IEC 15408:2022 series and ISO/IEC 18045:2022 still support the evaluation approach used in 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.

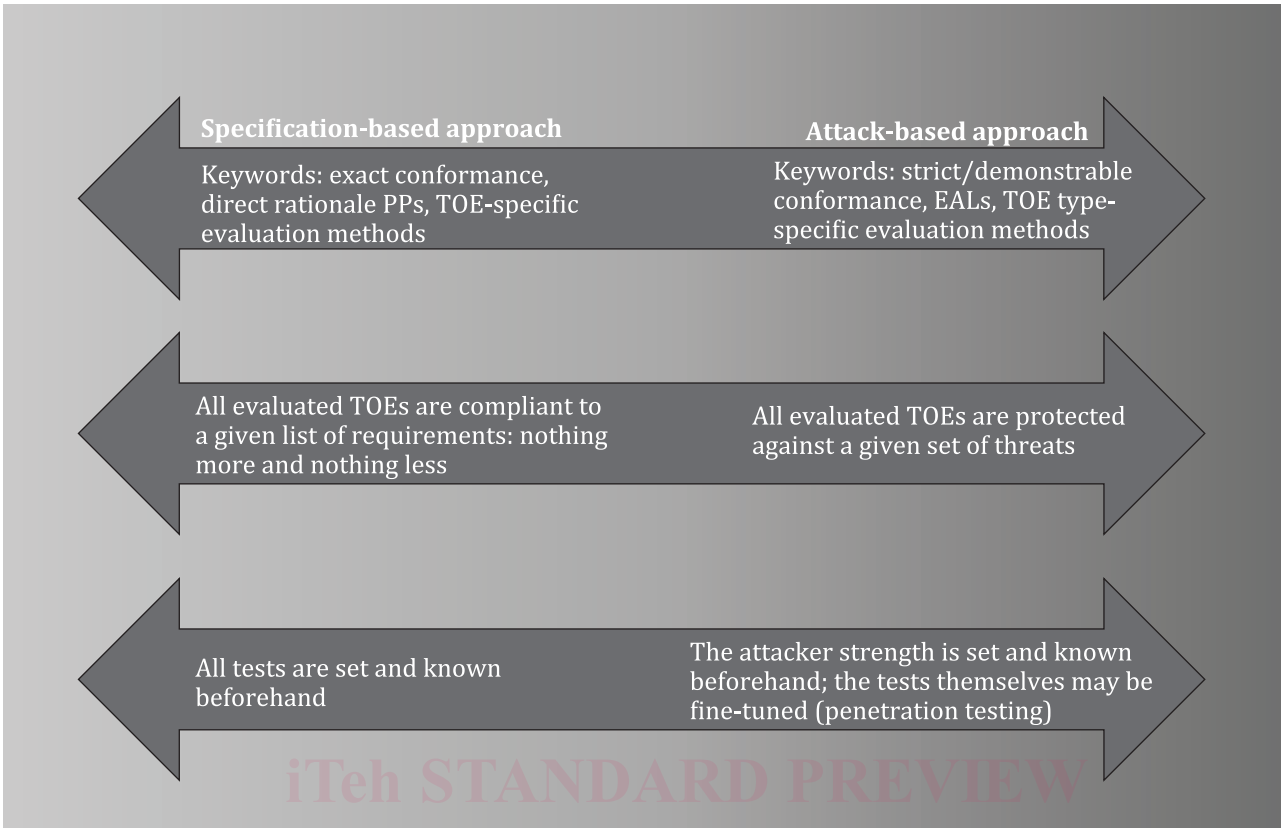

Figure 2 — Specification-based and attack-based approaches

5.1.2 The attack-based approach

5.1.2.1 General

As in previous versions, the ISO/IEC 15408:2022 series supports the evaluation methodology defined in ISO/IEC 18405:2022.

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 18045:2022, 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.

5.1.2.2 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.

5.1.2.3 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 18045:2022 activities; whenever a technical domain is mature enough, ISO/IEC 15408-4:2022 or refinement and extended components techniques can also be used to derive dedicated evaluation methods.

5.1.2.4 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 18405:2022 (which provides common notions such as the attack potential), and on the other hand by the evaluation schemes that use the ISO/IEC 15408:2022 series and ISO/IEC 18405:2022 (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).

5.1.3 The specification-based approach

5.1.3.1 General

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 15408-3:2022. The details added to SFRs and SARs are meaningful in particular contexts, for a particular TOE type, or in a given industry sector.