COMMITTEE DRAFT **ISO/IEC 3rd CD 15408-1, revision**	Reference document: **SC 27 N19755** **REPLACES: SC 27 N19505**
Date: **2019-07-15**	Supersedes document N18803

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection Secretariat: Germany	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: **2019-09-09** Please submit your comments via the online balloting application by the due date indicated.

ISO/IEC 3rd CD 15408-1, revision

Title: IT Security techniques – Evaluation criteria for IT security — Part 1: Introduction and general model

Project: 1.27.16.01 (ISO/IEC 15408-1, revision)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
For details regarding previous development stages refer to 2nd page of this explanatory report.			

ISO/IEC 15408-1
1st WD
	54th WG 3 meeting, April 2017, Recommendations 5,10 11, 14 (N17041 = WG 3 N1413).	Results of call f. editor (N17276);
		SoV (N17025).
			PL NB endorsement of co-editor (N17549);
			Liaisons to:
			CCDB (WG 3 N1391);
			The Open Group (WG 3 N1394);
			ISO/TC 22/SC 32 (N17373);
			Text f. 1st WD (WG 3 N1435).

ISO/IEC 15408-1
2nd WD
	55th WG 3 meeting, October / November 2017, Recommendations 8, 10 (N17666 = WG 3 N1494).	SoCom (WG 3 N1461);
		Draft DoC (WG 3 N1501).
			Editor's report (WG 3 N1465);
			Liaisons to:
			CCDB (WG 3 N1455);
			ISO/TC 22/SC 32 (N18103);
			DoC (WG 3 N1462);
			Text f. 2nd WD (WG 3 N1463)

ISO/IEC 15408-1
1st CD
	56th WG 3 meeting, April 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30th SC 27 Plenary, April 2018, Resolution 6 (N18710).	SoCom (WG 3 N1526);
		Late Com (WG 3 N1562);
		Draft DoC (WG 3 N1501).
			Liaison to:
			CCDB (WG 3 N1521);
			DoC (WG 3 N1527);
			Text f. 1st CD (N18700).

ISO/IEC 15408-1
2nd CD
	57th WG 3 meeting / CRM, Sep / Oct 2018, Recommendations 8, 10 (N18471 = WG 3 N1557) / 30th SC 27 Plenary, April 2018, Resolution 6 (N18710)	SoV (N18851);
		Draft DoC (N18944).
			Liaison to:
			CCDB (WG 3 N1619);
			DoC (N18802);
			Text f. 2nd CD (N18803).

ISO/IEC 15408-1
3rd CD
	58th WG 3 meeting / CRM April 2019, Recommendations 12, 14, 17, 21 (N19523 = WG 3 N1676).	SoV (N19487);
		Draft DoC (N19537).
			Liaison to:
			CCDB (WG 3 N1680);
			DoC (N19504);
			Text f. 3rd CD (N19755).

3rd CD Consideration

In accordance with Recommendation 14 (see SC 27 N19523) of the 58th SC 27/WG 3 meeting / CRM held in Tel Aviv, Israel, 2019-04-01/05 the hereby attached document is re-circulated for a 8-week 3rd CD letter ballot closing by

2019-09-09

Medium: http://isotc.iso.org/livelink/livelink/open/jtc1sc27

No. of pages: 2 + 149

Explanatory Report, 2nd page			
Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
Study Period **IT security testing, evaluation and assurance standards and techniques**	51st WG 3 meeting, Oct. 2015, Recommendations 5, 6 (N15594 = WG 3 N1251).		Terms of Reference (WG 5 N1258); 1st /2nd call f. contr. (WG 3 N1259 /1317).
	52nd WG 3 meeting, April 2016, Recommendation 5, 7 (N16026 = WG 3 N1296).	Expert contr. (WG 3 N1299, 1301).	3rd call f. contr. (WG 3 N1377); Rapporteur's report (WG 3 N1320). Liaison to: CCDB (WG 3 N1266).

ISO/IEC NP 15408-1 (revision)
Evaluation criteria for IT security -- Part 1
NWIP
	53rd WG 3 meeting, Oct. 2016, Recommendations 5, 6, 15, 19 (N16607 = WG 3 N1364).	Expert contr. (WG 3 N1368, N1371, N1373).	SP report (WG 3 N1363);
			Call f. editor (WG 3 N1387 = N16886);
			Liaisons to:
			CCDB (WG 3 N1330);
			The Open Group (WG 3 N1332); Text f. NWIP (N16963 [replaces N16883]).

ISO/IEC JTC 1/SC 27/WG 3 N19755

Date: 2019-07-12

ISO/IEC 15408-1:####(EN)

ISO/IEC JTC 1/SC 27 IT Security techniques

Secretariat: DIN

IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

Techniques de sécurité IT — Critères d'évaluation pour a sécurité des technologies de l'information — Partie 1 : Introduction et modèle général

CD stage

Warning for WDs and CDs

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

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

Document type: International Standard
Document subtype:
Document stage: (30.20) Preparatory
Document language: E

READ ME FIRST

Editors general notes for this draft.

Red text in a box are the Editors' comments.

In this draft the editors highlighted the keywords relating to the ISO verbal forms, shall, should, may, can and must using green text in order to highlight these words. This convention will be removed before the FDIS level documents.

Text related to the multi-assurance concepts have been highlighted using blue text

Some editorial changes have also been introduced in order to comply with the ISO/IEC Directives part 2:2018

The editors are aware that the figures are of low quality. In the final documents high quality images will be used. The Editors hope that they are legible in this draft.

The Editors thank the WG 3 contributors for their contributions and support during the editing cycle.

Legal Notice:

The text for the legal notice agreed between ISO/IEC and the CCDB will be included here.

Contents

Table of Figures

Table 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

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

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

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

This fourth edition cancels and replaces the third edition (ISO/IEC 15408-1:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

- The document has been restructured
- Technical changes have been introduced:
    - Review of the terminology,
    - The introduction of the exact conformance type,
    - The removal of low assurance PPs and the introduction of Direct Rationale PPs,
    - The introduction of PP-Modules and PP-Configurations for modular evaluations
    - The introduction of multi-assurance evaluation.

Introduction

ISO/IEC 15408 (all parts) permits comparability between the results of independent security evaluations. ISO/IEC 15408 (all parts) does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 (all parts) is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 (all parts) is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 (all parts) in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, can result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties, and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 (all parts) addresses the protection of assets from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. ISO/IEC 15408 (all parts) may also be applicable to aspects of IT security outside of these three categories. ISO/IEC 15408 (all parts) is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. ISO/IEC 15408 (all parts) may be applied in other areas of IT but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408 (all parts). Some of these are identified below:

a) ISO/IEC 15408 (all parts) does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls.

b) ISO/IEC 15408 (all parts) does not address the evaluation methodology under which the criteria should be applied.

NOTE The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

c) ISO/IEC 15408 (all parts) does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 (all parts) will be used for evaluation purposes in the context of such a framework.

d) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408 (all parts). Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors must make separate provisions for those aspects.

e) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408 (all parts). In the case that independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 (all parts) is applied must make provision for such assessments.

ISO terminology, such as "can", "informative", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2.

In the application of ISO/IEC 15408 (all parts) a justification shall be provided whenever the recommended option is not chosen.

Editors' Note

During the meeting held in Tel-Aviv the editing group agreed to introduce specific limitation on STs, namely that an ST could claim conformance to only one PP-Configuration (which indirectly implies it cannot mix PPs and PP-Configurations).

While applying this change editors have concluded that this rule is relevant in the "exact conformance" and "multi-assurance" cases only, and does not apply to the traditional "strict/demonstrable single-assurance" CC model.

In the "exact-conformance" approach, only specifications that mutually "allow" each other can be combined. Therefore PP-Configurations could not be combined, since they do not include an "allowed with" statement. By limiting conformance to only one PP-Configuration we avoid introducing changes in ASE in order to require checking "allowed with" statements of the inner PP-Configuration's components.

In the "multi-assurance" approach, special requirements are introduced in ACE to check the combination of assurance levels. Combining PP-Configurations would lead to the introduction of similar checks in ASE.

In the traditional "strict/demonstrable single-assurance" CC model, this limitation would be:

1) *unnecessary*: permitting a single-assurance ST to claim conformance with several strict/demonstrable PPs and PP-Configurations is in line with the traditional model and does not require any new special check. The rule for a ST claiming conformance with several PPs apply as well to several PP-Configurations and to combinations of PPs and PP-Configurations.

2) *costly and time-consuming*: requesting the developer and evaluator to write and then evaluate a PP-Configuration each time to check conformance with several PPs and PP-Configurations is time- and resource-consuming. Today this is not required in the case of several PPs and it does not seem to be appropriate that the standard puts unnecessary obligations for the use of PP-Configurations in the strict/demonstrable single-assurance model.

In consequence, CD3 document only constraints the conformance to a PP-Configuration in the exact conformance and multi-assurance cases. Unless experts raise an objection, no change will be made to the ISO/IEC 15408-1 in this aspect and this editor's note will be removed.

IT security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

1 Scope

This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of ISO/IEC 15408 (all parts). It describes the various parts of the standard; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

This document introduces:

- the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;
- a description of the organization of security components throughout the model;
- the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations;
- general information about the evaluation methods given in ISO/IEC 18045;
- guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;
- general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5; and
- information in regard to the scope of evaluation schemes.

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 15408-2:20XX, *IT security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

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

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

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

ISO/IEC 18045:20XX, *IT security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO/IEC/IEEE 24765:2017 and the following apply.

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

— ISO Online browsing platform, available at http://www.iso.org/obp

— IEC Electropedia, available at http://www.electropedia.org/

Editors' Note

The editors are aware that the terminology will evolve throughout the career of this revision.

The editors have removed the previous subdivisions in this draft and presented the terms in alphabetical order. In parallel, SC27/WG3 has decided to establish a separate Study Period on the hierarchy of concepts for terminology used in SC27/WG3 projects in particular focused on the ISO/IEC 15408 and ISO/IEC 18045 projects. The decision whether such grouping will be present in the next draft depends on the outcome from the Study Period.

Experts are asked to contribute to the concept-based order of terms to the Study Period . **See WG3 N1697**

Furthermore, the editing group has decided to take steps toward a dedicated Technical Specification to cover the terminology related to ADV_SPM subject therefore avoiding any impact to the schedule of the current CC revision.

Editors' note some general terminology issues:

a **sponsor** is the organization that is responsible for the production of a document. (For example the EALs guess the sponsor is the CCDB). Under the CCRA the term "sponsor" is used specifically, and this might be a confusing term to use in regard to identification of PPs, PP-Modules etc?

The **owner** of a document may be a different organization – For example an iTC

The **author** of a document is the entity writing the document. This can be different to the owner organization. e.g. consider a cPP that is sponsored by NIAP and Japan, the owner is the iTC, and the author is a subcontracted organization (that may change).

Editors request proposed definitions of these terms and appropriate use in the main text

3.1
acceptance procedure
procedure followed in order to accept newly created or modified configuration items as part of the TOE, or to move them to the next step of the life-cycle

Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance.

Note 2 to entry: There are several types of acceptance situations some of which may overlap:

a) acceptance of an item into the configuration management system for the first time, in particular as part of an integration process;

b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE;

EXAMPLE module, subsystem, quality control of the finished TOE.

c) subsequent to transport of configuration items

EXAMPLE parts of the TOE or preliminary products between different development sites;

d) subsequent to the delivery of the TOE to the consumer;

e) subsequent to the integration of the TOE

EXAMPLE inclusion of software, firmware and hardware components from other sources into the TOE.

3.2
action
evaluator action element of ISO/IEC 15408-3

Note 1 to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.3
activity
application of an assurance class of ISO/IEC 15408-3

3.4
administrator
entity that has a level of trust with respect to all policies implemented by the TSF

Note 1 to entry: Not all PPs or STs assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the TOE. Some of these policies may be related to the functionality of the TOE, others may be related to the operational environment.

3.5
adverse action
action performed by a threat agent on an asset

3.6
asset
entity that the owner of the TOE presumably places value upon

3.7
assignment
specification of an identified parameter in a functional element of a given functional or assurance component

Note 1 to entry: Such functional element is also called a requirement.

3.8
assurance
grounds for confidence that a TOE meets the SFRs

3.9
assurance package
named set of security assurance requirements

EXAMPLE "EAL 3".

3.10
attack potential
measure of the effort needed to exploit a vulnerability in a TOE

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (for example: Expertise, resources, and motivation) and properties related to the vulnerability itself (for example: Window of opportunity, time to exposure).

3.11
augmentation
addition of one or more requirements to a package

Note 1 to entry: in case of a functional package such an augmentation is considered only in the context of one package and is not considered in the context with other packages or PPs or STs.

Note 2 to entry: in case of an assurance package augmentation refers to one or more SAR(s).

3.12
authorized user
TOE user who may, in accordance with the SFRs, perform an operation

3.13
base component
independent entity in a multi-component product that provides services and resources to one or more dependent component(s)

Note 1 to entry: This applies in particular to 'composed TOEs' and 'composite products / composite TOEs'.

3.14

base component developer

entity developing the base component

3.15

base Protection Profile

base PP

Protection Profile specified in a PP-Module used as a basis to build a Protection Profile Configuration

3.16

base TOE

base component which is itself the subject of an evaluation

Note 1 to entry: This applies in particular to 'composed TOEs' and 'composite products / composite TOEs'.

3.17

base TOE developer

entity developing the base TOE

3.18

base TOE evaluator

entity performing the base TOE evaluation

3.19

base TOE evaluation authority

evaluation authority monitoring the evaluation of the base TOE

3.20

check

<evaluation verb> generate a verdict by a simple comparison

Note 1 to entry: Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

3.21

class

⟨taxonomy⟩ set of ISO/IEC 15408 families that share a common focus

3.22

coherent

logically ordered and having discernible meaning

Note 1 to entry: For documentation, this term addresses both the actual text and the structure of the document, in terms of whether it is understandable by its target audience.

3.23

compatible

⟨component⟩ property of a component able to provide the services required by another component, through the corresponding interfaces of each component, in consistent operational environments

3.24

component

⟨taxonomy⟩ smallest selectable set of elements on which requirements may be based

3.25

component TOE

(evaluated) TOE that is a component of another composed TOE

3.26

composed assurance package

CAP

assurance package consisting of components drawn predominately from the ACO class, representing a point on the pre-defined scale for composition assurance

3.27

composed TOE

TOE comprised solely of two or more component TOEs

3.28

composed evaluation

evaluation of a composed TOE using the specific evaluation technique applicable to composed TOEs

Note 1 to entry: This evaluation technique refers to the ACO assurance class that is defined in ISO/IEC 15408-3.

3.29

composite evaluation

evaluation of a composite TOE / product using the specific composite evaluation technique

Note 1 to entry: This evaluation technique refers to the COMP related assurance families that are specified in ISO/IEC 15408-3 for the ADV, ALC, ASE, ATE and AVA classes.

3.30

composite product

product comprised of two or more components which can be organized in two layers: a layer of one already evaluated base component (base TOE) and a layer of one dependent component

3.31

composite product evaluation authority

evaluation authority monitoring the evaluation of the composite product

3.32

composite product evaluator

entity performing the composite evaluation

3.33

composite product integrator

entity installing the dependent component on the base component for the composite product

3.34

composite TOE

TOE part of a composite product whereby the base TOE and the dependent component are part of the composite TOE

Note 1 to entry: A dependent component in a composite TOE may consist of one or more dependent components. For simplification, they are considered as ‘one dependent component’.

Note 2 to entry: A composite TOE may contain parts that are independent from the base component or base TOE respectively. For simplification, such parts are considered as belonging to the dependent component.

Note 3 to entry: The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach.

3.35

configuration item

item or aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process [during the TOE development]

Note 1 to entry: These may be either parts of the TOE or objects related to the development of the TOE like evaluation documents or development tools. Configuration management items may be stored in the configuration management system directly (for example, files) or by reference (for example, hardware parts) together with their version.

[SOURCE: ISO/IEC/IEEE 24765:2017 3.7771. modified, specification of TOE development requirement and note 1 to entry added]

3.36

configuration list

configuration management output document listing all configuration items for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product

Note 1 to entry: This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course, the list can be an electronic document inside of a configuration management tool. In that case, it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC.

3.37

configuration management

CM

discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

[SOURCE: ISO/IEC/IEEE 24765:2010 3.779 1.]

3.38

configuration management documentation

CM documentation

all configuration management documentation including configuration management output, configuration management list(s), configuration management system records, configuration management plan and configuration management usage documentation

3.39

configuration management evidence

everything that may be used to establish confidence in the correct operation of the configuration management system

EXAMPLE configuration management output, rationales provided by the developer, observations, experiments, or interviews made by the evaluator during a site visit

3.40

configuration management output

results, related to configuration management, produced, or enforced by the configuration management system

Note 1 to entry: These configuration management related results could occur as documents (for example filled paper forms, configuration management system records, logging data, hard-copies, and electronic output data) as well as actions (for example manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are configuration lists, configuration management plans and/or behaviors during the product life-cycle.

3.41

configuration management plan

description of how the configuration management system is used for the TOE

Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it may be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system may be used to a different extent for other products. That means the configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE development.

EXAMPLE The structure and content of a configuration management plan are presented in Annex A of ISO 10007:2017.

3.42

configuration management system

set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of his products during their life-cycles

Note 1 to entry: Configuration management systems may have varying degrees of rigour and function. At higher levels, configuration management systems may be automated, with flaw remediation, change controls, and other tracking mechanisms.

3.43

configuration management system record

output produced during the operation of the configuration management system documenting important configuration management activities

EXAMPLE Configuration management item change control forms and configuration management item access approval forms.

344

configuration management tool

manually operated or automated tool realizing or supporting a configuration management system

EXAMPLE Tools for the version management of the parts of the TOE.

3.45

configuration management usage documentation

part of the configuration management system, which describes, how the configuration management system is defined and applied by using for example handbooks, regulations and/or documentation of tools and procedures

3.46

confirm

<evaluation verb> declare that something has been reviewed in detail with an independent determination of sufficiency

Note 1 to entry: The level of rigour required depends on the nature of the subject matter.

3.47

connectivity

property of the TOE allowing interaction with IT entities external to the TOE

Note 1 to entry: This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

3.48

counter

act on or respond to a particular threat so that the threat is eradicated or mitigated

3.49

covert channel

enforced, illicit signaling channel that allows a user to surreptitiously contravene the multi-level separation policy and unobservability requirements of the TOE

3.50

delivery

transmission of the finished TOE from the production environment into the hands of the customer

Note 1 to entry: This product life-cycle phase may include packaging and storage at the development site, but does not include transportations of the unfinished TOE or parts of the TOE between different developers or different development sites.

3.51
demonstrable conformance
relation between a ST/PP and a PP, where the ST/PP provides an equivalent or more restrictive solution which solves the generic security problem in the PP

3.52
demonstrate
<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a "proof"

3.53
dependency
relationship between components such that a PP, ST functional package or assurance package including a component shall also include any other components that are identified as being depended upon or include a rationale as to why they are not

3.54
dependent component
dependent entity in a multi-component product that relies on the provision of services and resources by one or more base components

Note 1 to entry This applies in particular to 'composed TOEs' and 'composite products / composite TOEs'.

3.55
dependent component developer
entity developing the dependent component

3.56
dependent TOE
dependent component which is itself the subject of an evaluation

Note 1 to entry: This applies only to 'composed TOEs' and not to 'composite products / composite TOEs'.

3.57
dependent TOE developer
entity developing the dependent TOE

3.58
dependent TOE evaluation authority
evaluation authority monitoring the evaluation of the dependent TOE

3.59
dependent TOE evaluator
entity performing the dependent TOE evaluation

3.60
describe
<evaluation verb> provide specific details of an entity

3.61
determine
<evaluation verb> affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed.

3.62
developer
organization responsible for the development of the TOE

3.63

development

product life-cycle phase which is concerned with generating the implementation representation of the TOE

Note 1 to entry: Throughout the ALC: Life-cycle support requirements, development, and related terms (developer, develop) are meant in the more general sense to comprise development and production.

3.64

development environment

environment in which the TOE is developed

Note 1 to entry: The conditions include physical facilities, security controls, IT systems and development tools.

3.65

development tool

tools, including any applicable test software that support the development and production of the TOE

EXAMPLE for a software TOE, development tools are usually programming languages, compilers, linkers and generating tools.

3.66

direct rationale

type of Protection Profile or Security Target in which the SPD-elements of the SPD are mapped directly to the SFRs and possibly to the Security Objectives for the operational environment

Note 1 to entry: Direct rationale does not include security objectives for the TOE.

3.67

domain separation

security domain separation

security architecture property whereby the TSF defines separate security domains for each user and for the TSF and ensures that no user process can affect the contents of a security domain of another user or of the TSF

3.68

element

⟨taxonomy⟩ most detailed level of definition of a security need as defined in SFRs and SARs

3.69

encountered potential vulnerability

potential weakness in the TOE identified by the evaluator while performing Evaluation Activities that could be used to violate the SFRs

3.70

ensure

<evaluation verb> guarantee a strong causal relationship between an action and its consequences

Note 1 to entry: When this term is preceded by the word “help” it indicates that the consequence is not fully certain, on the basis of that action alone.

3.71

entity

identifiable item that is described by a set or collection of properties

Note 1 to entry: Entities include subjects, users (including external IT products), objects, information, sessions and/or resources.

3.72

evaluation

assessment of a PP, an ST, or a TOE, against defined criteria

3.73
evaluation activity
EA
activity derived from work units defined in ISO/IEC 18045

Note 1 to entry: The concept of evaluation activities, and the combination of evaluation activities into "evaluation methods", is described in ISO/IEC 15408-4.

3.74
evaluation assurance level
EAL
well-formed package of security assurance requirements defined ISO/IEC 15408-3 and drawn from ISO/IEC 15408-5, representing a point on the ISO/IEC 15408 pre-defined assurance scale

3.75
evaluation authority
body operating an evaluation scheme

Note 1 to entry: By applying the evaluation scheme evaluation authority sets the standards and monitors the quality of evaluations conducted by bodies within a specific community.

3.76
evaluation deliverable
resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities

3.77
evaluation evidence
item used as a basis for establishing the verdict of an evaluation activity

3.78
evaluation method
set of one or more evaluation activities that are derived from ISO/IEC 18045 work units for application in a specific context

3.79
evaluation scheme
rules, procedures, and management to carrying evaluations of IT products security implementing all parts of ISO/IEC 15408

Note 1 to entry: Administrative and regulatory framework is usually a part of an evaluation scheme. Such framework is out of the scope of ISO/IEC 15408.

Note 2 to entry: The objective of an evaluation scheme is to ensure that high standards of competence and impartiality are maintained and a consistency of evaluations is achieved.

Note 3 to entry: An evaluation scheme is usually established by an evaluation authority, which defines the evaluation environment, including criteria and methodology required to conduct IT security evaluations.

3.80
evaluation technical report
ETR
documentation of the overall verdict and its justification, produced by the evaluator, and submitted to an evaluation authority

3.81
evaluator
individual assigned to perform evaluations in accordance with a given evaluation standard and associated evaluation methodology

Note 1 to entry: An example of evaluation standards is the ISO/IEC 15408 series with the associated evaluation methodology given in ISO/IEC 18045.

[SOURCE: ISO/IEC 19896-1:2018]

3.82

exact conformance

EC

hierarchical relationship between a PP or PP Configuration and an ST where all the requirements in the ST are drawn only from the PP/PP Configuration

Note 1 to entry: An ST is allowed to claim exact conformance to one or more PPs but only to one PP configuration.

3.83

examine

<evaluation verb> generate a verdict by analysis using evaluator expertise

Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

3.84

exhaustive

<evaluation verb> characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan

Note 1 to entry: This term is used in ISO/IEC 15408 with respect to conducting an analysis or other activity. It is related to “systematic” but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to ensure that all possible avenues have been exercised.

3.85

explain

<evaluation verb> give argument accounting for the reason for taking a course of action

Note 1 to entry: This term differs from both “describe” and “demonstrate”. It is intended to answer the question “Why?” without actually attempting to argue that the course of action that was taken was necessarily optimal.

3.86

exploitable vulnerability

weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE

3.87

extended security requirement

security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408

Note 1 to entry: An extended security requirement may be either a SAR or a SFR.

Note 2 to entry: Extended security requirements are defined within extended component definitions.

3.88

external entity

user

human technical system or one of its components interacting with the TOE from outside of the TOE boundary

3.89

family

⟨taxonomy⟩ set of components that share a similar goal but differ in emphasis or rigour

3.90

formal

expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

3.91

functional interface

external interface providing a user with access to functionality of the TOE which is not directly involved in enforcing security functional requirements

Note 1 to entry: In a composed TOE these are the interfaces provided by the base component that are required by the dependent component to support the operation of the composed TOE.

3.92

functional package

named set of security functional requirements that may be accompanied by an SPD and Security Objectives derived from that SPD

3.93

general model

type of Protection Profile or Security Target in which the SPD-elements of the SPD are mapped to the Security Objectives for the TOE and to the Security Objectives for the operational environment.

Note 1 to entry: SFRs in the general model have to cover all security objectives for the TOE.

3.94

global assurance package

assurance package, i.e. a well-formed set of assurance requirements drawn from ISO/IEC 15408-3 or defined as a set of extended assurance components, that applies to the entire TOE in a multi-assurance evaluation

3.95

guidance documentation

documentation that describes the delivery, preparation, operation, management and/or use of the TOE

3.96

identity

representation uniquely identifying an entity within the context of the TOE

EXAMPLE An example of such a representation is a string.

Note 1 to entry: entities can be diverse such as a user, process, or disk. For a human user, the representation could be the full or abbreviated name or a unique pseudonym.

Note 2 to entry: An entity can have more than one identity.

3.97

implementation representation

least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement

Note 1 to entry: Source code that is then compiled or a hardware drawing that is used to build the actual hardware are examples of parts of an implementation representation.

3.98

informal

expressed in natural language

3.99

installation

procedure performed by a human user embedding the TOE in its operational environment and putting it into an operational state

Note 1 to entry: This operation is performed normally only once, after receipt and acceptance of the TOE. The TOE is expected to be progressed to a configuration allowed by the ST. If similar processes have to be performed by the developer they are denoted as “generation” throughout the class ALC: Life-cycle support. If the TOE requires an initial start-up that does not need to be repeated regularly, this process would be classified as installation.

3.100

inter TSF transfer

communication between the TOE and the security functionality of other trusted IT products

3.101

internal communication channel

communication channel between separated parts of the TOE

3.102

internal TOE transfer

communicating data between separated parts of the TOE

3.103

internally consistent

no apparent contradictions exist between any aspects of an entity

Note 1 to entry: In terms of documentation, this means that there can be no statements within the documentation that can be taken to contradict each other.

3.104

interpretation

clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045, or scheme requirement

3.105

iteration

use of the same component to express two or more distinct requirements

3.106

justify

<evaluation verb> provide a rationale providing sufficient reason

Note 1 to entry: The term 'justify' is more rigorous than a 'demonstrate'. This term requires significant rigour in terms of very carefully and thoroughly explaining every step of a logical analysis leading to a conclusion.

3.107

laboratory

organization with a management system providing evaluation and or testing work in accordance with a defined set of policies and procedures and utilizing a defined methodology for testing or evaluating the security functionality of IT products

Note 1 to entry: These organizations are often given alternative names by various approval authorities. For example, IT Security Evaluation Facility (ITSEF), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

[SOURCE: ISO/IEC 19896-1 ,3.7]

3.108

layering

design technique where separate groups of components are hierarchically organized to have separate responsibilities such that a group of components depends on groups of components below it in the hierarchy for services, and provides its services to the groups of components above it

3.109

life cycle model

framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a product, spanning the life of the system from the definition of its requirements to the termination of its use

Note 1 to entry: See also Figure 1.

[SOURCE: ISO/IEC/IEEE 24765:2017 2.2219 modified, note 1 to entry added]

3.110
module
TOE-module
small architectural unit that can be characterized in terms of the properties discussed in TSF internals (ADV_INT)

3.111
monitoring attack
generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the TOE by operating the TOE in the way that corresponds to the guidance documents

3.112
multi-assurance evaluation
evaluation using a PP-Configuration where the TOE is organized in parts, each part being associated with its own assurance package

3.113
non-bypassability
⟨of the TSF⟩ security architecture property whereby all SFR-related actions are mediated by the TSF

3.114
object
entity in the TOE, that contains or receives information, and upon which subjects perform operations

3.115
observation report
report written by the evaluator requesting a clarification or identifying a problem during the evaluation

3.116
operation
⟨on an ISO/IEC 15408 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection

3.117
operation
⟨on an object⟩ specific type of action performed by a subject on an object

3.118
operation
usage phase of the TOE including normal usage, administration, and maintenance of the TOE after delivery and preparation

3.119
operational environment
environment in which the TOE is operated, consisting of everything that is outside the TOE boundary

3.120
optional Security Functional Requirement
optional SFR
SFR in a Protection Profile or PP-Module that contributes to a stated aspect of the PP's security problem description but its inclusion in a conformant ST's list of SFRs is not mandatory.

Note 1 to entry: An optional SFR can address appropriate SPD elements threat(s) and/or OSPs.

3.121
organizational security policy
OSP
set of security rules, procedures, or guidelines for an organization

Note 1 to entry: A policy may pertain to a specific operational environment.

3.122
overall verdict
statement issued by an evaluator with respect to the result of an evaluation

Note 1 to entry: The statement can be expressed as “pass” or “fail”.

3.123
oversight verdict
statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities

3.124
potential vulnerability
suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.

3.125
preparation
activity in the life-cycle phase of a product, comprising the customer's acceptance of the delivered TOE and its installation

Note 1 to entry: preparation may include such things as booting, initialization, start-up and progressing the TOE to a state ready for operation.

3.126
production
life-cycle phase which consists of transforming the implementation representation into the implementation of the TOE, i.e. into a state acceptable for delivery to the customer

Note 1 to entry: This phase may comprise manufacturing, integration, generation, internal transports, storage, and labelling of the TOE.

3.127
Protection Profile
PP
implementation-independent statement of security needs for a TOE type

3.128
Protection Profile configuration
PP-Configuration
implementation-independent statement of security needs for a TOE type contained in base Protection Profile(s), Protection Profile Module(s), and Protection Profile(s) that are not base PPs for any PP-Module included.

3.129
Protection Profile module
PP-Module
implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles

3.130
prove
<evaluation verb> show correspondence by formal analysis in its mathematical sense

Note 1 to entry: It is completely rigorous in all ways. Typically, the term prove is used when there is a desire to show correspondence between two TSF representations at a high level of rigour.

3.131
record
<evaluation verb> retain a written description of procedures, events, observations, insights, and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time

3.132

refinement

addition of details to a security component

3.133

report

<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report

3.134

residual vulnerability

weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE

3.135

role

pre-defined set of rules establishing the allowed interactions between a user and the TOE

3.136

secret

information that shall be known only to authorized users and/or the TSF in order to enforce a specific SFP

3.137

secure state

state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs

3.138

security assurance requirement

SAR

security requirement, that refers to the conditions and processes for the development and delivery of the TOE, and the actions required of evaluators with respect to evidence produced from these conditions and processes

3.139

security attribute

property of subjects, users, objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs

Note 1 to entry: Users can include external IT products.

3.140

security domain

environment provided by the TSF for the use by untrusted entities in such a way that the environment is isolated and protected from other environments

3.141

security function policy

SFP

set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs

3.142

security functional requirement

SFR

security requirement, which contributes to fulfil the TOE's Security Problem Definition (SPD) as defined in a specific ST or in a PP

Note 1 to entry: A security functional requirement can be addressed directly as in the direct rationale model, or indirectly, through the Security Objectives for the TOE, as in the general model.

3.143
security objective
statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

3.144
security problem
security problem definition
SPD
statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address

Note 1 to entry: This statement consists of a combination of: threats to be countered by the TOE and its operational environment, the OSPs enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.

Note 2 to entry: SPD-elements include threats, OSPs, and assumption.

3.145
security requirement
requirement, stated in 15408 standardized language, which is part of a TOE security specification as defined in a specific ST or in a PP

3.146
Security Target
ST
implementation-dependent statement of security requirements for a TOE based on a security problem definition

3.147
selection
specification of one or more items from a list in a component

3.148
selection-based Security Functional Requirement
selection-based SFR
SFR in a Protection Profile/PP-Module that contributes to a stated aspect of the PP's//PP-Module's security problem definition that is to be included in a conformant ST if a selection choice identified in the PP/PP-Module indicates that it has an associated selection-based SFR

3.149
semiformal
expressed in a restricted syntax language with defined semantics

3.150
single-assurance evaluation
evaluation using a single set of assurance requirements

3.151
specify
<evaluation verb> provide specific details about an entity in a rigorous and precise manner

3.152
strict conformance
hierarchical relationship between a PP and a ST/PP where all the requirements in the PP also exist in the ST/PP

Note 1 to entry: This relation can be paraphrased as "the ST shall contain all statements that are in the PP but may contain more". Strict conformance is expected to be used for stringent requirements that are to be adhered to in a single manner.

3.153

sub-activity

application of an assurance component of ISO/IEC 15408-3

Note 1 to entry: Assurance families are not explicitly addressed in ISO/IEC 15408 (all parts) because evaluations are conducted on a single assurance component from an assurance family.

3.154

sub-TSF

combined functionality of all hardware, software, and firmware of a TOE that is relied upon for the correct enforcement of the SFRs defined in one PP-Configuration component

Note 1 to entry: This set of SFRs is closed by dependencies, objectives, and SPD elements in the PP-Configuration component.

Note 2 to entry: The notion of sub-TSF is applied in relationship with the specification and evaluation of PP-Configurations and conformant STs. It can be used in the single-assurance approach but it must be used in the multi-assurance approach: sub-TSFs must be defined in a multi-assurance PP-Configuration and in conformant STs.

Note 3 to entry: each sub-TSF is associated with its own set of SARs in a multi-assurance PP-Configuration. In the rest of the document, a set of SARs may be an assurance package.

Note 4 to entry: a sub-TSF has the characteristics of a TSF.

3.155

subject

entity in the TOE that performs operations on objects

3.156

tailoring

addition of one or more functional requirements to a functional package, and/or the addition of one or more selections to an SFR in a functional package

Note 1 to entry: such tailoring is considered only in the context of one package and is not considered in the context with other packages, PPs, or PP-Modules.

Note 2 to entry: the selections in the SFR may be replaced by the additional selections.

Note 3 to entry: selections can only be added for packages claimed by PPs or PP-Modules. STs cannot claim package-name tailored conformance to the package.

3.157

target of evaluation

TOE

set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

3.158

threat agent

entity that can exercise adverse actions on assets protected by the TOE

3.159

time period to exposure

time interval when an element is participating in an IT system and could be attacked

3.160

TOE resource

anything usable or consumable in the TOE

3.161

TOE security functionality

TSF

combined functionality of all hardware, software, and firmware of a TOE that is relied upon for the correct enforcement of the SFRs

3.162
TOE type
set of TOEs that have common characteristics

Note 1 to entry: The TOE type may be more explicitly defined in a PP.

3.163
trace
<evaluation verb> identity relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second

3.164
transfer outside of the TOE
TSF-mediated communication of data to entities not under the control of the TSF

3.165
translation
describes the process of describing security requirements in a standardized language.

Note 1 to entry: Use of the term translation in this context is not literal and does not imply that every SFR expressed in standardized language can also be translated back to the Security Objectives.

3.166
trusted channel
means by which a TSF and another trusted IT product can communicate with necessary confidence

3.167
trusted IT product
IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly

3.168
trusted path
means by which a user and a TSF can communicate with the necessary confidence

Note 1 to entry: Communication typically implies the establishment of identification and authentication of both parties, as well as the concept of a user specific session which is integrity-protected.

Note 2 to entry: When the external entity is a trusted IT product, the notion of trusted channel is used instead of trusted path.

Note 3 to entry: Both physical and logical aspects of secure communication can be considered as mechanisms for gaining confidence.

3.169
TSF data
data for the operation of the TOE upon which the enforcement of the SFR relies

3.170
TSF interface
TSFI
means by which either external entities or subjects within the TOE but outside of the TSF interact with or supply data to the TSF

3.171
TSF self-protection
security architecture property whereby the TSF cannot be corrupted by non-TSF code or entities

3.172
user data
data received or produced by the TOE, which is meaningful to some external entity but which do not affect the operation of the TSF

Note 1 to entry: Depending of the concept, this definition assumes that the same data created by users that has an actual impact on the operation of the TSF can be regarded as the TSF data.

3.173
verdict
statement issued by an evaluator with respect to evaluator action element, assurance component, or class

Note 1 to entry: The statement can be presented as: pass, fail or inconclusive.

Note 2 to entry: Also see overall verdict.

3.174
verify
<evaluation verb> rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see “confirm”. This term has more rigorous connotations. The term “verify” is used in the context of evaluator actions where an independent effort is required of the evaluator.

3.175
vulnerability
weakness in the TOE that can be used to violate the SFRs in some environment

3.176
window of opportunity
period of time that an attacker has access to the TOE

3.177
work unit
most granular level of evaluation work

Note 1 to entry: ISO/IEC 18405 defines the evaluation work units for a subset of ISO/IEC 15408-3 security assurance requirements.

4 Abbreviated terms

The following abbreviations are used in ISO/IEC 15408 (all parts):

AP	Assurance Package
API	Application Programming Interface
CAP	Composition Assurance Package
CD	Compact Disk
CM	Configuration Management
COMP	Composite Product Assurance Package
DAC	Discretionary Access Control
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator
EA	Evaluation Activity
EAL	Evaluation Assurance Level
EM	Evaluation Method
EMS	Electromagnetic spectrum
ETR	Evaluation Technical Report
GAP	Global assurance package
GB	Gigabyte

GHz	Gigahertz
GUI	Graphical User Interface
HSM	Hardware Security Module
HTTPS	Hypertext transfer protocol secure
IC	Integrated Circuit
IOCTL	Input Output Control
IP	Internet Protocol
IPsec	IP security (protocol)
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory access control
MB	Megabyte
MBps	Megabytes per second
OR	Observation Report
OS	Operating System
OSP	Organizational Security Policy
OTP	One-time programmable
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
PP	Protection Profile
PPA	Protection Profile Assurance Package
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFP	Security Function Policies
SFR	Security Functional Requirement
SPA	Simple Power Analysis
SPD	Security Problem Definition
SSH	Secure shell
ST	Security Target
STA	Security Target Assurance Package
TCP	Transmission Control Protocol
TLS	Transport layer security
TOE	Target of Evaluation
TSF	TOE Security Functionality

TSFI	TSF Interface
USB	Universal serial bus
VPN	Virtual Private Network

5 Overview

5.1 General

This Clause 5 introduces the main concepts of ISO/IEC 15408 (all parts). It identifies the concept of the Target of Evaluation (TOE), the target audience of ISO/IEC 15408 (all parts), and the approach taken to present the material in ISO/IEC 15408 (all parts).

5.2 The different parts of ISO/IEC 15408

ISO/IEC 15408 (all parts) is presented as a set of distinct but related parts as identified below. Terms used in the description of the parts are explained in 3.

a) **ISO/IEC 15408-1, Introduction, and general model** is the introduction to ISO/IEC 15408 (all parts). It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.

b) **ISO/IEC 15408-2, Security functional components** establishes a set of functional components that serve as standard templates upon which security functional requirements for TOEs are based. ISO/IEC 15408-2 catalogues the set of security functional components and organizes them in families and classes.

c) **ISO/IEC 15408-3, Security assurance components** establishes a set of assurance components that serve as standard templates upon which security assurance requirements for TOEs are based. ISO/IEC 15408-3 catalogues the set of security assurance components and organizes them into families and classes. ISO/IEC 15408-3 also defines evaluation criteria for PPs, STs and TOEs.

d) **ISO/IEC 15408-4, Framework for the specification of evaluation methods and activities** provides a standardized framework for the specification of evaluation methods and activities that may be included in PPs, STs and any documents supporting them, to be used by evaluators in support of evaluations using the model described in the other parts of ISO/IEC 15408. ISO/IEC 18045 is fundamental to ISO/IEC 15408 (part 4).

e) **ISO/IEC 15408-5, Pre-defined packages of security requirements** provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders. Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

In support of ISO/IEC 15408 (all parts), other documents have been published. The bibliography provides a list of supportive documents and it is anticipated that other documents will be published, including technical rationale material and guidance documents.

NOTE ISO/IEC 18045 provides the baseline methodology for IT security evaluations performed in accordance with ISO/IEC 15408 (all parts). Target audience of ISO/IEC 15408 (all parts)

5.2.1 General

There are five main groups with a general interest in evaluation of the security properties of TOEs: consumers (risk owners), developers, technical working groups, evaluators and others. The information presented in ISO/IEC 15408 (all parts) has been structured to support the needs of all of these groups which are considered to be the principal users of ISO/IEC 15408 (all parts). The groups can benefit from the criteria as explained in 5.2.2 through 5.2.6 .

5.2.2 Consumers (Risk owners)

ISO/IEC 15408 (all parts) is written to ensure that evaluation fulfils the needs of risk owners as this is the fundamental purpose and justification for the evaluation process.

Risk owners can use the results of evaluations to help decide whether a TOE fulfils their security needs. These security needs are typically identified as a result of both risk analysis and policy direction. Risk owners can also use the evaluation results to compare different TOEs.

ISO/IEC 15408 (all parts) gives risk owners, especially those in consumer groups and communities of interest, an implementation- independent structure, termed the PP, in which to express their security requirements in an unambiguous manner.

5.2.3 Developers

ISO/IEC 15408 (all parts) is intended to support IT product developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are contained in an implementation-dependent construct termed the Security Target (ST). This ST may conform to one or more PPs to show that the TOE meets the security requirements from consumers as laid down in those PPs.

ISO/IEC 15408 (all parts) can then be used to determine the responsibilities and actions to provide evidence that is necessary to support the evaluation of the TOE against these requirements. It also defines the content and presentation of that evidence.

5.2.4 Technical working groups

ISO/IEC 15408 (all parts) is intended to support technical working groups in preparing and developing PPs, PP-Modules, PP-Configurations, packages and supporting documents or guidance. Technical working groups can be composed of stakeholders including consumers (risk owners), developers, evaluators, and academics.

5.2.5 Evaluators

ISO/IEC 15408 (all parts) contains criteria to be used by evaluators when forming judgements about the conformance of TOEs, STs, PPs and PP-Configurations to their security requirements. ISO/IEC 15408 (all parts) describes the general set of actions the evaluator is to carry out.

NOTE ISO/IEC 15408 (all parts) does not specify procedures to be followed in carrying out those actions. More information on these procedures may be found in 13.

5.2.6 Others

While ISO/IEC 15408 (all parts) is oriented towards specification and evaluation of the IT security properties of TOEs, it can also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that can benefit from information contained in ISO/IEC 15408 (all parts) are:

a) system custodians and system security officers responsible for determining and meeting organizational IT security policies and requirements;

b) auditors, both internal and external, responsible for assessing the adequacy of the security of an IT solution (which may consist of or contain a TOE);

c) security architects and designers responsible for the specification of security properties of IT products;

d) accreditors responsible for accepting an IT solution for use within a particular environment;

e) sponsors of evaluation responsible for requesting and supporting an evaluation;

f) evaluation authorities responsible for the management and oversight of IT security evaluation programs; and

g) academia who perform research on the topic of IT security.

Table 1 presents, for each of the audience groupings, how the parts of ISO/IEC 15408 are of interest.

Table 1 — Road map to the "Evaluation criteria for IT security"

	Consumers (Risk owners)	**Developers**	**Technical working groups**	**Evaluators**	**Others**
Part 1	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications and security problem definitions for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for packages, PPs, PP-Modules and PP-Configurations.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use when evaluating PPs, PP-Configurations and STs.	May use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition.
Part 2	Shall use for guidance and reference when formulating statements of security functional components for their risk-environment.	Shall use for reference when interpreting statements of security functional components in packages, PPs and PP-Modules. Shall use when developing STs. May use when formulating security functionality for IT products.	Shall use for reference when formulating statements of security functional components in packages, PPs and PP-Modules.	Shall use for reference when evaluating security functional components given in packages, PPs and PPP-modules or security functional requirements in STs.	May use for reference when reviewing security functional components given in packages, PPs and PP-Modules or security functional requirements in STs.

	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 3	Shall use for guidance and reference when determining the security assurance required for their risk-environment.	Shall use for reference when interpreting statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations. Shall use when developing STs May use when formulating or improving development processes.	Shall use for reference when formulating statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations.	Shall use for reference when evaluating security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.	May use for reference when reviewing security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.
Part 4	Should use for reference and background information in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities. Should use when formulating specific evaluation methods and activities.	May use for reference purposes and for guidance in the structure of evaluation methods and activities.

	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 5	Should use for reference in determining the contents of any claimed pre-defined packages of security requirements.	Shall use when developing STs claiming conformance to pre-defined packages of security requirements. Shall use for reference when preparing a TOE for evaluation conformant to pre-defined packages of security requirements.	Shall use when developing PPs, PP-Modules and PP-Configurations claiming conformance to pre-defined packages of security requirements.	Shall use for reference when evaluating PPs, PP-Modules and PP-Configurations or STs claiming conformance to pre-defined packages of security requirements.	May use for reference in determining the contents of any claimed pre-defined packages of security requirements.

5.3 The Target of Evaluation (TOE)

5.3.1 General

ISO/IEC 15408 (all parts) is flexible in what to evaluate and is therefore not tied to the boundaries of IT products as commonly understood. Therefore, in the context of evaluation ISO/IEC 15408 (all parts) uses the term “TOE” (Target of Evaluation).

While there are cases where a TOE consists of a complete IT product, this need not be the case. The TOE may be an IT product, a part of an IT product, a set of IT products, a unique technology that may never be made into a product, or a combination of these.

As far as ISO/IEC 15408 (all parts) is concerned, the precise relation between the TOE and any IT products is only important in one aspect: the evaluation of a TOE containing only part of an IT product should not be misrepresented as the evaluation of the entire IT product.

EXAMPLE

Examples of TOEs include devices characterized by few interfaces, reduced attack surface, and a well-known supply chain:

- A network device;
- A software application;
- An operating system;
- A virtualization system;
- An integrated circuit;
- The cryptographic co-processor of an integrated circuit;
- An application for a mobile device;
- A database application excluding the remote client software normally associated with that database application.

TOEs can also be more complex, characterized by a large interface/large interfaces and/or number of components, multiple manufacturing/integration phases, field upgradeable products such as:

- A Local Area Network (LAN) including all terminals, servers, network equipment and software;

- A mobile device;
- Gateways and hubs;
- A software application in combination with an operating system;
- A multi-function device, such as a multi-function printer;
- A Hardware Security Module (HSM).

5.3.2 TOE Boundaries

The concept of a TOE boundary is fundamental to the specification of the ST.

A TOE may be a complete IT product (or products), a part of an IT product, or made up of various components. The ST shall clearly outline the physical and logical scope of the TOE as it is delivered to the customer.

Any parts of an IT product that are not within the TOE boundary are outside the scope of the evaluation and are called *non-TOE parts of the IT product*.

5.3.3 Different representations of the TOE

In ISO/IEC 15408 (all parts), a TOE can occur in several representations in relationship with the assurance criteria:

NOTE These assurance criteria include testing (ATE) and vulnerability analysis (AVA), which require TOE samples, some design (ADV_IMP), which require an implementation representation, for instance source code, and lifecycle (ALC), which requires the TOE’s configuration list.

EXAMPLE

TOE representations for a software TOE:

- a list of files in a configuration management system;
- a single master copy, that has just been compiled;
- the source code for a specific version of an open-source distribution;
- a box containing physical media and a manual, ready to be shipped to a customer;
- a binary file available for secure download;
- an installed and operational version.

TOE representations for a hardware TOE:

- Integrated circuit layout;
- Memory mappings;
- Wafers;
- Modules.

All of these are considered to be a TOE and wherever the term “TOE” is used in ISO/IEC 15408 (all parts), the context determines the representation that is meant.

5.3.4 Different configurations of the TOE

In general, IT products can be configured in many ways with different options enabled or disabled. During an evaluation performed in accordance with ISO/IEC 15408 (all parts), it will be determined whether a TOE meets certain requirements. The flexibility in configuration can lead to problems since all possible configurations of the TOE must meet the requirements. For these reasons, it is often the case that the guidance part of the TOE constrains the possible configurations of the TOE. That is, the guidance for the TOE can be different from the general guidance of the IT product.

EXAMPLE 1

An operating system IT product: This product can be configured in many ways including the types of users, number of users, types of external connections allowed/disallowed, options enabled/disabled etc.

In general, if an IT product contains or is a TOE then the configuration of the product will need to be much more tightly controlled, since some configuration options can lead to a TOE not meeting the requirements.

EXAMPLE 2

- allow all types of external connections,
- the system administrator does not need to be authenticated.

For this reason, there would be an expected difference between the guidance documentation for the general IT product, that can allow many configurations; and the guidance documentation for the TOE, that may allow only one or only a set of configurations that do not differ in security-relevant ways.

NOTE If the guidance documentation for the TOE allows more than one configuration, these configurations are collectively called "the TOE" and each configuration must meet the requirements levied on the TOE.

5.3.5 Operational environment of the TOE

Everything outside the TOE boundary belongs to the TOE operational environment. In the case where the TOE is part of an IT product the IT product can have non-TOE parts. Such non-TOE parts are also part of the operational environment of the TOE.

The ST shall describe assumptions and define security objectives for the operational environment which together with the security functionality provided by the TOE itself are necessary to mitigate the threats, and to enforce organizational security policies.

The security objectives for the operational environment may support the TOE security functionality.

The ST shall formulate clear requirements for the TOE environment in order to provide the user sufficient information to use the evaluated TOE properly.

EXAMPLE

Secure key generation and injection premises and processes is an example of a security objective for the operational environment which supports the TOE cryptographic services specified using FCS components from ISO/IEC15408-2.

5.4 Presentation of material in this document

The general model is presented in 6 which explains the concepts relating to the evaluation of the security functionality of IT products, the definition of the security problem and the specification of security requirements addressing the security problem. Concepts relating to the specification of security requirements, packages, PPs, PP-Modules and PP-Configurations, that relate to the needs of risk-owners with similar security problems are introduced.

The means of specifying security requirements and the completion of security components provided in ISO/IEC 15408-2 and ISO/IEC 15408-3 is explained in 7 and 8.

The requirements and recommendations for the core constructs of packages, PPs, PP-Modules, PP-Configurations and ST s, are explained in Clauses 9, 10, 11 and 11.3.3.

The requirements and recommendations for evaluation and evaluation results for TOEs, STs, PPs and PP-Configurations are found in 13.

Finally, the topic of composing assurance is found in 14.

6 General model

6.1 Background

This Clause 6 presents the general concepts used throughout ISO/IEC 15408 (all parts), including the context in which the concepts are to be used and the approach for applying the concepts. ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4, and ISO/IEC 15408-5 expand on the use of these concepts, and assume that the approach described here is used. Further, for users of ISO/IEC 15408 (all parts) who intend to perform evaluation activities, ISO/IEC 18045 is applicable.

ISO/IEC 15408 (all parts) discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of ISO/IEC 15408 (all parts). However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which ISO/IEC 15408 (all parts) is applicable. Clause 6 assumes that the reader has knowledge of IT security and it is not intended to act as a tutorial in this area.

6.2 Assets and security controls

Security is concerned with the protection of assets within the operational environment.

EXAMPLE 1

An example of an asset is the contents of a file or a server.

Examples of operational environments are:

- a data center;
- a computer network connected to the Internet;
- a LAN;
- the every-day environment of a user;
- a general office environment.

Many assets are in the form of information that is stored, processed, and transmitted by IT products to meet requirements laid down by owners of the information. Information owners may require that availability, dissemination, and modification of any such information are strictly controlled and that the assets are protected from threats by security controls implemented in the operational environment. Figure 1 illustrates these high-level concepts and relationships.

NOTE ISO/IEC 27001 provides requirements for establishing, implementing, maintaining and continually improving an information security management system including the specification of controls.

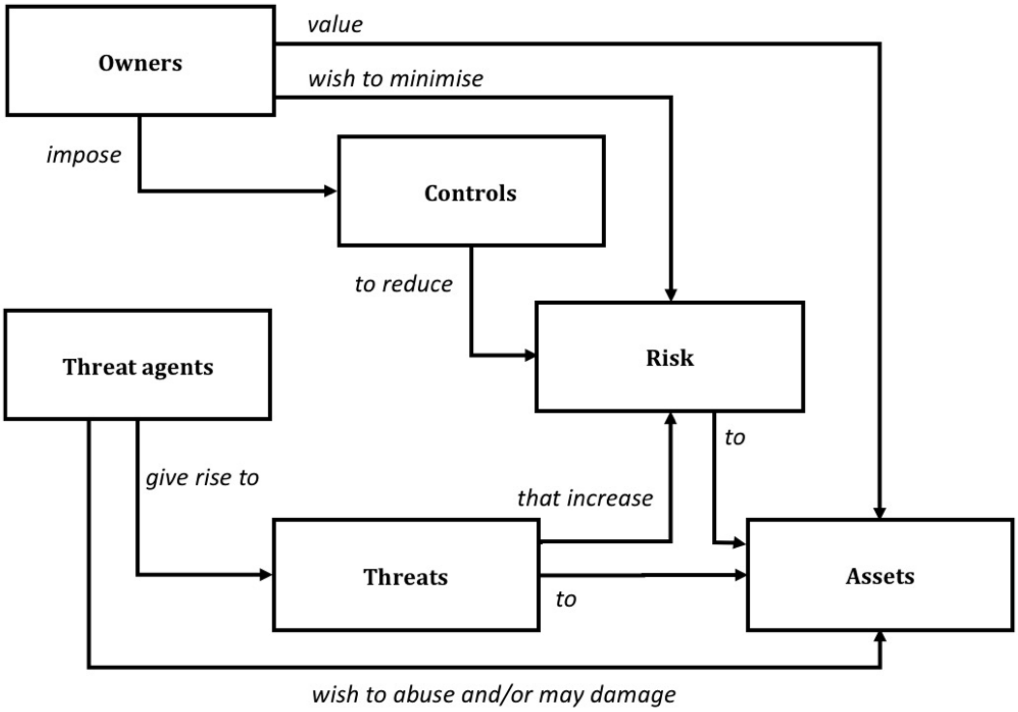


Figure 1 — Evaluation concepts and relationships

Safeguarding assets of interest is the responsibility of owners who place value on those assets. Actual or presumed threat agents can also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner.

EXAMPLE 2

Examples of threat agents include hackers, malicious users, non-malicious users, who sometimes make errors, computer processes and accidents.

The owners of the assets will perceive such threats as a potential source of impairment of the assets, leading to a decrease of their value. Security-specific impairment commonly includes but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realized and the impact on the assets when that threat is realized. Subsequently controls are imposed to reduce the risks to assets. These controls can consist of IT-related controls (such as firewalls and smart cards) and non-IT controls (such as guards and procedures). See also ISO/IEC 27001 and ISO/IEC 27002 for a more general discussion on security controls and how to implement and manage them.

Owners of assets can be held responsible for those assets and therefore should be able to defend the decision to accept the risks of exposing the assets to the threats.

Two important elements in defending this decision are being able to demonstrate that:

- the controls are sufficient: if the applied controls do what they claim to do, the threats to the assets are countered;
- the controls are correct: That is, the applied controls do what they claim to do.

Many owners of assets lack the knowledge, expertise, or resources necessary to judge sufficiency and correctness of the security controls, and they may not wish to rely solely on the assertions of the developers of the security controls. These consumers can therefore choose to increase their confidence in the sufficiency and correctness of some or all of their security controls by ordering an evaluation of these security controls.

Figure 2 describes the evaluation concepts and relationships discussed in this Clause 6.

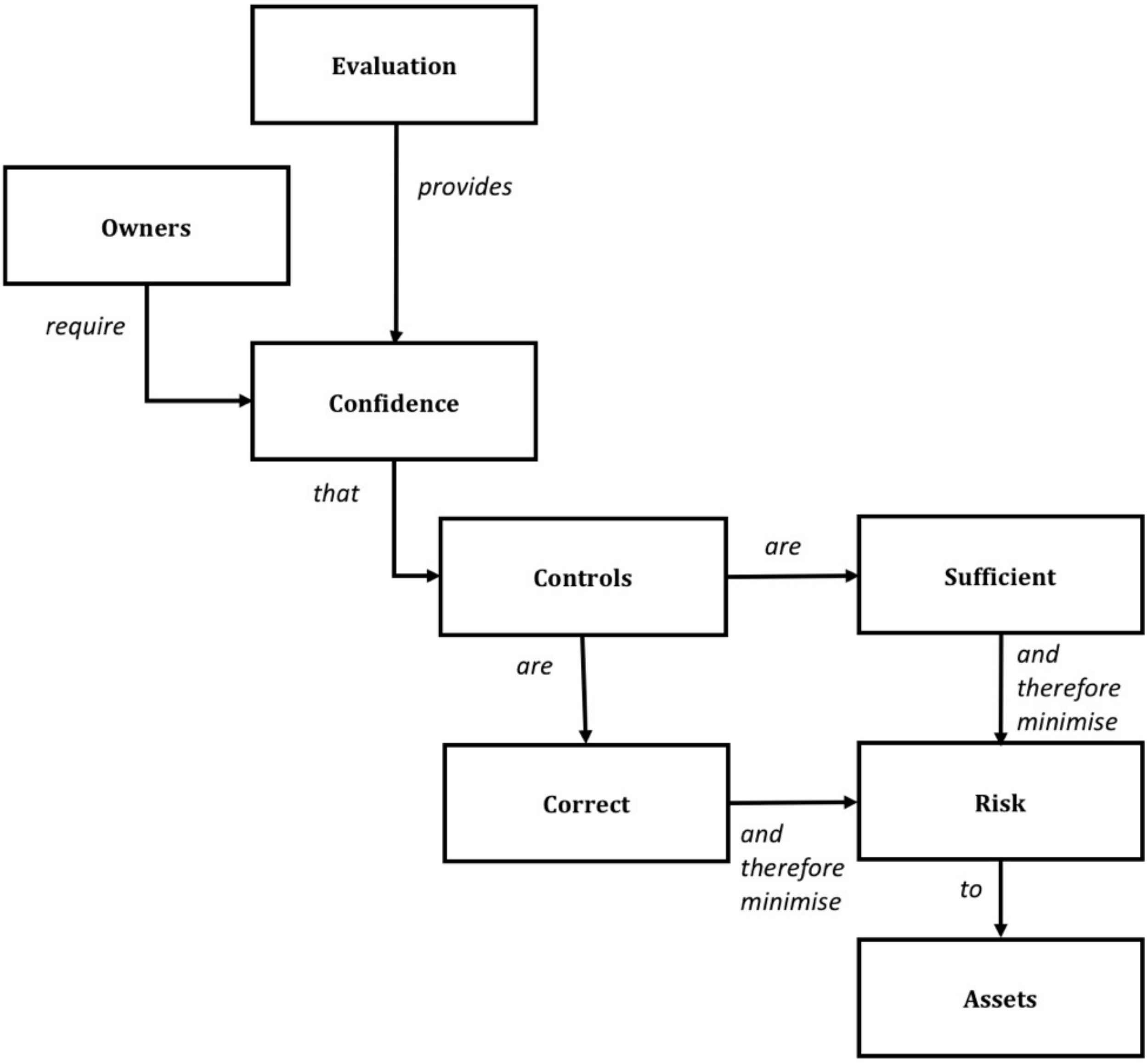


Figure 2 — Evaluation concepts and relationships

In an evaluation, the sufficiency of the security controls is analysed through a construct called the Security Target (ST).

6.3 Core constructs of the ISO/IEC 15408 (all parts) paradigm

6.3.1 General

The ISO/IEC 15408 series defines a flexible framework for the evaluation of IT products.

To allow consumer groups and technical communities to express their security needs, and to facilitate authoring appropriate documents that express these needs, five constructs: STs, packages, PPs, PP-Modules and PP-Configurations are provided in the paradigm.

STs, PP-Modules, PPs and PP-Configurations shall specify a conformance type. This document specifies three conformance types; demonstrable, strict, and exact. Conformance types and associated requirements shall be described in detail in Annex E.

As this evaluation may need to meet varying assurance needs of consumers (risk owners), the standard provides different tools, including: well-formed security components (ISO/IEC 15408-2 and ISO/IEC 15408-3) as well as a mechanism to define extended assurance components (ISO/IEC 15408-1). Predefined packages including those for evaluation assurance levels (ISO/IEC 15408-5), a framework for defining evaluation methods and activities (ISO/IEC 15408-4) and a companion evaluation methodology (ISO/IEC 18045).

6.3.2 Security Targets

6.3.2.1 General

Subclause 6.3.2 presents a simplified view of the ST construct. A more detailed and complete description of the ST concept and the content requirements shall be found in Clause 11.3.3 and Annex D.

ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs undergoing evaluation.

6.3.2.2 The purpose of a ST

The ST is a key document that begins with determining the security problem definition (SPD) for the TOE. This includes specifying the assets to be protected and the threats to those assets. The ST then considers any relevant assumptions and describes the security controls that need to be in place in order to demonstrate that these threats are countered. If the security controls do what they claim to do, the threats are countered.

The two groups of security controls are:

a) the security objectives for the TOE: these describe the security control(s) for which correctness will be determined in the evaluation;

b) the security objectives for the operational environment: these describe the security controls for which correctness will not be determined in the evaluation.

The reasons for this division are:

- ISO/IEC 15408 (all parts) is only suitable for assessing the correctness of IT security controls. Therefore, the non-IT security controls are always in the operational environment.

  EXAMPLE Non-IT security controls include human fences, security guards, procedures.

- Assessing the correctness of security controls costs time and money, possibly making it infeasible to assess the correctness of all IT security controls.

- The correctness of some IT security controls may already have been assessed in another evaluation. It is therefore not cost-effective to assess this correctness again.

The ST further details the security objectives for the TOE by means of specifying Security Functional Requirements (SFRs). These SFRs are formulated in a standardized language (described in ISO/IEC 15408-2) to ensure precision and facilitate comparability.

In summary, the ST demonstrates that:

- The SFRs meet the security objectives for the TOE;
- The security objectives for the TOE and the security objectives for the operational environment counter the threats;
- And therefore, the SFRs and the security objectives for the operational environment counter the threats.

From this it follows that a correct TOE, i.e. A TOE that meets the SFRs, in combination with a correct operational environment, i.e. one that meets the security objectives for the operational environment, will counter the threats. In the next two subclauses correctness of the TOE and correctness of the operational environment are discussed separately.

In some cases, defining a Security Target that omits security objectives and directly maps the SFRs to the security problem definition (SPD) is appropriate. This is a "Direct Rationale" ST, and is explained in detail in Clause 11.3.3 and Annex D.

A ST may be defined as standalone document for a specific TOE or may comply with one or more pre-existent PP-Configurations or PP(s). These documents allow for generic definitions of a TOE type to be made allowing for comparability in evaluation results between TOEs as well as efficiencies to be made.

PPs, PP-Configurations, PP modules and packages that may contribute to the specification of a ST are introduced in 6.3.3.1, 6.3.3.2 and 6.3.3.3.

6.3.2.3 Correctness of the TOE

A TOE can be incorrectly designed and implemented and therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers could be able to damage and/or abuse the assets.

These vulnerabilities can arise from poor design, accidental errors made during development, intentional addition of malicious code, poor configuration management etc.

To determine the correctness of the TOE, various activities may be performed such as:

- testing the TOE;
- examining various design representations of the TOE;
- examining the physical security of the development environment of the TOE.

The ST provides a structured description of these activities to determine correctness in the form of Security Assurance Requirements (SARs). These SARs are formulated in a standardized language described in ISO/IEC 15408-3 to ensure precision and facilitate comparability.

If the SARs are met, there exists assurance in the correctness of the TOE and the TOE is therefore less likely to contain vulnerabilities that can be exploited by attackers. The amount of assurance that exists in the correctness of the TOE is determined by the SARs themselves.

6.3.2.4 Correctness of the operational environment

The operational environment could also be incorrectly specified or implemented and therefore contain errors that lead to vulnerabilities. By exploiting these vulnerabilities, attackers could damage and/or abuse the assets.

However, in ISO/IEC 15408 (all parts), no assurance is obtained regarding the correctness of the operational environment. Or, in other words, the operational environment is not evaluated.

As far as the evaluation is concerned, the operational environment is assumed to be a correct instantiation of the security objectives for the operational environment.

This does not preclude a consumer of the TOE from using other methods to determine the correctness of his operational environment.

EXAMPLE

If, for an Operating System TOE, the security objectives for the operational environment state “The operational environment must ensure that entities from an untrusted network can only access the TOE using the FTP protocol”, the consumer could select an evaluated firewall, and configure it to only allow FTP access to the TOE;

NOTE The Internet is an example of an untrusted network

If the security objectives for the operational environment state: “The operational environment shall ensure that all administrative personnel will not behave maliciously”, the consumer could adapt his contracts with administrative personnel to include punitive sanctions for malicious behaviour, but this determination is not part of an evaluation using ISO/IEC 15408 (all parts) as a basis.

6.3.3 Communicating security requirements

6.3.3.1 Packages

Packages describe a set of related security requirements that are frequently used together. Packages are often designed to be re-used bringing some comparability between those PPs, PP-Modules and STs that use them.

Security functional packages may be used to define security protocols, or other security functional concepts.

Security assurance packages may be used to define the conditions and processes such as specification, design, development, testing and delivery under which the TOE is developed and configured.

Core requirements for packages shall be found in Clause 9 and Annex A provides additional description and requirements about packages. ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs and PPs undergoing evaluation that may use packages. ISO/IEC 15408-5 provides some pre-defined packages that may be used by PP and ST authors.

6.3.3.2 Protection Profiles (PPs)

PPs describe a TOE type and the security assurance requirements (SAR), security functional requirements (SFRs) expected to be provided for that type of TOE.

PPs based on other PPs may be used to further refine a TOE type.

PPs may take either a standard or a Direct Rationale approach.

Core requirements for PPs shall be found in Clause 10 and Annex B. ISO/IEC 15408-3 provides PPs’ evaluation criteria.

6.3.3.3 PP Modules and PP-Configurations

PP-Configurations build upon the concept of PP and PP-Modules.

A PP-Module may be used to refine the generic TOE type of a base PP, or to add security requirements for particular technologies which may be optionally associated with the TOE type defined in the base PPs. PP-Modules may also be based on other PP-Modules. Further, PP-Configurations describe which PPs and PP-Modules may be legitimately combined.

This concept shall be described in more detail in Clause 11 and Annex C.

EXAMPLE

A PP-Module describes the security functional requirements for Bluetooth technology. Another PP-Module describes the security functional requirements for wireless LAN clients. Using a PP-Configuration, the security function requirements for each of these technologies can be combined with PPs describing a TOE type, such as an operating system PP, or a mobile device PP. In this context the PP describing the TOE type is referred to as a base PP. A PP-Configuration describes which PPs and PP-Modules are combined to define an implied PP that includes all the requirements given in the PPs and PP-Modules.

In this example it would be possible to specify six PP-Configurations:

1. Operating system with Bluetooth,
2. Operating system with Wireless client,
3. Operating system with Bluetooth and Wireless client,

4. Mobile device with Bluetooth,
5. Mobile device with Wireless client,
6. Mobile device with Bluetooth and Wireless client.

6.3.4 Meeting the needs of consumers (risk owners)

6.3.4.1 General

In today's world, consumers (risk owners) can have different approaches to the assurance that the products they use to address the SPD. Subclauses 6.3.4.2 and 6.3.4.3 introduce these approaches.

6.3.4.2 Multi-assurance evaluation

The standard evaluation approach consists in applying a single set of standard assurance requirements to the entire TOE. However, the standard also provides a method (ISO/IEC 15408-4) to specialize the standard assurance components and evaluation activities and a multi-assurance evaluation framework to apply different assurance requirements to different parts of the TSF (sub-TSFs), while enforcing a global set of SARs for the entire TOE.

The multi-assurance evaluation paradigm:

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

Technically, a multi-assurance evaluation is driven by a ST that complies with one (and only one) multi-assurance PP-Configuration. The multi-assurance PP-Configuration ensures that applying different assurance requirements to different parts of the TSF is consistent with their security needs. In this evaluation approach, each sub-TSF enforces some security functionality, e.g. an authentication protocol, a firewall policy, the boot process, encryption/decryption operations, and in some cases, the sub-TSF may be associated with a subset of TOE components, for instance a TPM, a cryptographic library or a card reader.

EXAMPLE

The multi-assurance paradigm is relevant in particular in the following situations:

- A product where some security functionality requires a higher assurance than the rest, for instance, a key storage and processing unit, a secure boot module, etc.
- A product where some parts of the security functionality do not require the same high evaluation assurance as other more exposed parts, for instance an internet gateway with support for personal area network protocols.
- A family of products where some security functionality is shared across all the products with the same assurance, and some security functionality is implemented in different ways for different use cases, for instance in a tamper-resistant module or in a software module or through COTS, requiring a different assurance.

  An example is a family of biometric authentication devices, with either match-on-device or match-on-SE, or both. This can give rise to a PP for the authentication device excluding the matching function, and two PP-Modules for the different types of matching functions, each with a dedicated set of assurance requirements. Three PP-Configurations can be defined for the device: PP with each of the PP-Modules, PP with both PP-Modules. A similar situation arises, for instance, for a family of mobile applications which uses either software crypto library secured by with-box techniques or a hardware-based crypto library, or for a family of payment terminals with either IC and/or magstripe readers.
- Multi-assurance is also relevant for products claiming conformance to different PPs with different assurance packages: by defining and evaluating a PP-Configuration, the multi-assurance paradigm allows better control over possible inconsistencies between these PPs. The evaluation of electronic passports implementing both Basic Access Control and Extended Access Control constitutes a typical example, as these access control mechanisms are subject to different security problems and assurance requirements.

Editor's Note:

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

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

The developer will document each sub-TSF as usual since sub-TSFs are closed by dependencies, objectives, and SPD. The vulnerability analysis of each sub-TSF complies with the current definition of AVA_VAN which considers the whole TOE as the attack surface.

This note will be removed in the following draft.

6.3.4.3 Conformance types

Three different types of conformance to PPs and PP-Configurations have been defined to meet the needs of consumers (risk owners). These are exact, strict and demonstrable conformance. They are described in detail in Annex E.

7 Specifying security requirements

7.1 Security problem definition

7.1.1 Introduction

The SPD defines the security problem that is to be addressed and may appear in PPs, PP-Modules and STs. The SPD is, as far as ISO/IEC 15408 is concerned, axiomatic. That is, the process of deriving the SPD falls outside the scope of ISO/IEC 15408.

NOTE 1 The usefulness of the results of an evaluation strongly depends on the quality of the SPD. It is therefore often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good SPD. ISO/IEC 15446 presents guidance in regard to deriving an SPD.

NOTE 2 According to ISO/IEC 15408-3, it is not mandatory to have statements in all sections, a PP with threats does not need to have OSPs and vice versa. Also, any PP could omit assumptions.

NOTE 3 Where the TOE is physically distributed, it can be better to discuss the relevant threats, OSPs and assumptions separately for distinct domains of the TOE operational environment.

7.1.2 Threats

This section of the SPD describes the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

A threat consists of an adverse action performed by a threat agent on an asset.

Adverse actions influence one or more properties of an asset from which that asset derives its value.

Threat agents may be described as individual entities, but in some cases, it may be better to describe them as types of entities, groups of entities, etc.

EXAMPLE

Examples of threat agents are:

- hackers;
- users;
- computer processes; and
- accidents.

Threat agents can be further described by attributes such as expertise, resources, opportunity, and motivation.

Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network;
- a worm seriously degrading the performance of a wide-area network;

- a system administrator violating user privacy; and
- someone on the Internet listening in on confidential electronic communication.

7.1.3 Organizational security policies (OSPs)

This section of the SPD describes the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

OSPs are security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future in the operational environment. OSPs can be made by an organization controlling the operational environment of the TOE, or they can be made by legislative or regulatory bodies. OSPs can apply to the TOE and/or the operational environment of the TOE.

EXAMPLE

Examples of OSPs are:

- All products that are used by the Government must conform to the National Standard for password generation and encryption;
- Only users with System Administrator privilege and clearance of Department Secret shall be allowed to manage the Department Fileserver.

7.1.4 Assumptions

This section of the SPD describes the assumptions that are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE could be unable to provide all of its security functionality. Assumptions may be on physical, personnel and connectivity of the operational environment.

EXAMPLE

Examples of assumptions are:

- Assumptions on the non-TOE part of the product:
  - It is assumed that the TOE will be integrated into a device that provides a hardware-based root of trust.
- Assumptions on physical aspects of the operational environment:
  - It is assumed that the TOE will be placed in a room that is designed to minimize electromagnetic emanations;
  - It is assumed that the administrator consoles of the TOE will be placed in a restricted access area.
- Assumptions on personnel aspects of the operational environment:
  - It is assumed that users of the TOE will be trained sufficiently in order to operate the TOE;
  - It is assumed that users of the TOE are approved for information that is classified as National Secret;
  - It is assumed that users of the TOE will not write down their passwords.
- Assumptions on connectivity aspects of the operational environment:
  - It is assumed that a PC workstation with at least 10GB of disk space is available to run the TOE on;
  - It is assumed that the TOE is the only non-OS application running on this workstation;
  - It is assumed that the TOE will not be connected to an untrusted network.

NOTE During an evaluation these assumptions are considered to be true: they are not tested in any way. For these reasons, assumptions can only be made on the operational environment. Assumptions can never be made on the behaviour of the TOE because an evaluation consists of evaluating assertions made about the TOE and not by assuming that assertions on the TOE are true. Nevertheless, the ST, PP and PP-Configuration evaluations should detect unrealistic assumptions for the type of TOE and operational environment, which may become unacceptable.

7.2 Security objectives

7.2.1 General

The security objectives are a concise statement of the intended solution to the security problem. The role of the security objectives is threefold:

- provide a high-level, natural language solution of the problem. The security objectives consist of a set of statements without overly much detail that together form a high-level solution to the security problem. The level of abstraction of the security objectives aims at being clear and understandable to knowledgeable potential consumers of the TOE. The security objectives are in natural language;
- divide this solution into two part-wise solutions, that reflect the roles of the TOE and its operational environment to address each part of the problem. In a ST the high-level security solution, as described by the security objectives, is divided into two part-wise solutions. These part-wise solutions are called the security objectives for the TOE and the security objectives for the operational environment;
- demonstrate that these part-wise solutions form a complete solution to the problem.

7.2.2 Security objectives for the TOE

The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This part-wise solution is called the security objectives for the TOE and consists of a set of objectives that the TOE shall achieve in order to solve its part of the problem.

EXAMPLE

Examples of security objectives for the TOE are:

- The TOE shall keep confidential the content of all files transmitted between it and a Server;
- The TOE shall identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE;
- The TOE shall restrict user access to data according to the Data Access policy described in Annex 3 of the PP.

If the TOE is physically distributed, it may be better to subdivide the section containing the security objectives for the TOE into several subsections to reflect this.

NOTE In Direct Rationale STs security objectives for the TOE are not included: See D.4.

7.2.3 Security objectives for the operational environment

The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). This pair-wise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment shall achieve.

EXAMPLE

Examples of security objectives for the operational environment are:

- The operational environment shall provide a workstation with the OS Linux version 3.01b to execute the TOE on;
- The operational environment shall ensure that all human TOE users receive appropriate training before allowing them to work with the TOE;
- The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel;
- The operational environment shall ensure the confidentiality of the audit logs generated by the TOE before sending them to the central Audit Server.

If the operational environment of the TOE consists of multiple physical sites, each with different properties, it may be better to subdivide the section containing the security objectives for the operational environment into several sub-sections to reflect this.

Third party components that cannot be evaluated due to unavailability of evaluation evidence are included in the operational environment, and the security objectives for the operational environment shall include that the third-party component works as intended.

7.2.4 Relation between security objectives and the SPD

The ST also contains a security objectives rationale containing two sections:

- a tracing that shows which security objectives address which SPD-elements (threats, OSPs and assumptions);
- a set of justifications that shows that all SPD-elements are effectively addressed by the security objectives.

NOTE In Direct Rationale PPs a security objectives Rationale is not included: See D.4.

EXAMPLE

A threat “T17: Threat agent X reads the Confidential Information in transit between A and B”, a security objective for the TOE: “OT12: The TOE shall ensure that all information transmitted between A and B is kept confidential”, and a demonstration “T17 is directly countered by OT12”.

7.2.5 Tracing between security objectives and the SPD

The tracing shows how the security objectives trace back to the threats, OSPs and assumptions as described in the SPD.

a) *No spurious objectives*: Each security objective traces to at least one SPD-element (threat, OSP or assumption).

b) *Complete with respect to the security problem definition*: Each SPD-element has at least one security objective tracing to it.

c) *Correct tracing*: Since assumptions are always made by the TOE on the operational environment, security objectives for the TOE do not trace back to assumptions. The tracings allowed by ISO/IEC 15408-3 are depicted in Figure 3.

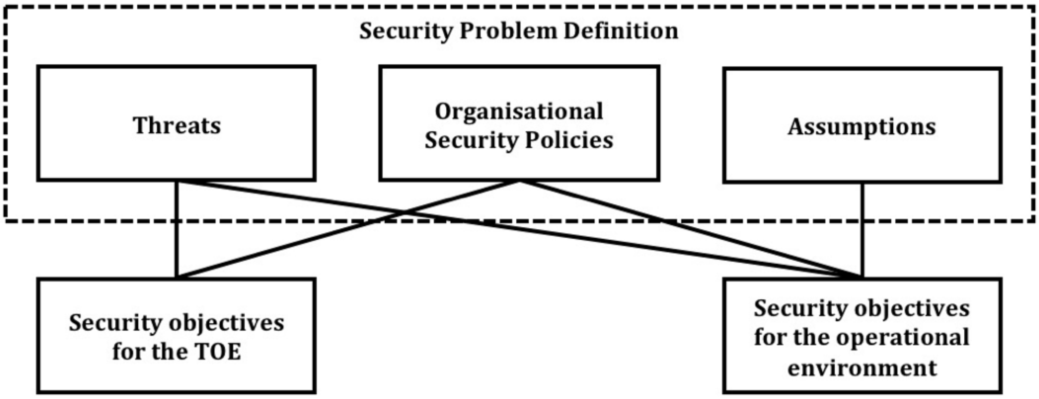

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment

Figure 3 — Tracings between security objectives and the SPD

Multiple security objectives may trace to the same threat, indicating that the combination of those security objectives counters that threat. A similar argument holds for OSPs and assumptions.

7.2.6 Providing a justification for the tracing

The security objectives rationale also demonstrates that the tracing is effective: All the given threats, OSPs and assumption are addressed (i.e. countered, enforced, and upheld respectively) if all security objectives tracing to a particular threat, OSP or assumption are achieved.

This demonstration analyses the effect of achieving the relevant security objectives on countering the threats, enforcing the OSPs and upholding the assumptions and leads to the conclusion that this is indeed the case.

In some cases, where parts of the SPD very closely resemble some security objectives, the demonstration may be straightforward.

7.2.7 On countering threats

Countering a threat does not necessarily mean removing that threat, it may also mean sufficiently diminishing that threat or sufficiently mitigating that threat.

EXAMPLE

Examples of removing a threat are:

- removing the ability to execute the adverse action from the threat agent;
- moving, changing, or protecting the asset in such a way that the adverse action is no longer applicable to it;
- removing the threat agent;
  E.g. removing machines from a network that frequently crash that network.

Examples of diminishing a threat are:

- restricting the ability of a threat agent to perform adverse actions;
- restricting the opportunity to execute an adverse action of a threat agent;
- reducing the likelihood of an executed adverse action being successful;
- reducing the motivation to execute an adverse action of a threat agent by deterrence;
- requiring greater expertise or greater resources from the threat agent.

Examples of mitigating the effects of a threat are:

- making frequent back-ups of the asset;
- obtaining spare copies of an asset;
- insuring an asset;
- ensuring that successful adverse actions are always timely detected, so that appropriate action can be taken.

7.2.8 Security objectives: conclusion

Based on the security objectives and the security objectives rationale, the following conclusion is drawn: if all security objectives are achieved then the security problem as defined in Security problem definition (ASE_SPD) is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

7.3 Security requirements

7.3.1 General

As mentioned in clauses 6.3.2 and 6.3.3, packages, PPs, PP-Modules and STs specify the detailed security requirements applicable to a TOE that have been derived from the stated SPD. Security functional requirements and security assurance requirements shall be drawn from security components defined in ISO/IEC 15408-2 and ISO/IEC 15408-3 respectively, which are a template for security requirements written in a standardized language. The process of deriving a security requirement from a security component involves tailoring the components and is known as "completion".

NOTE In 7, the term "author" includes authors of STs, PPs, PP-Modules, and packages.

Security requirements are specified as a result of the refinement of the SPD in a ST and possibly PP, PP-Module, and packages. Security requirements are specified by a tailoring the components given in ISO/IEC 15408-2, ISO/IEC 15408-3 or that have been defined as extended components in accordance with 8.4. The tailoring process uses the operations in 7.3.2 and 7.3.3.

NOTE Since a ST specifies the security requirements for a specific TOE it presents only fully completed components. PPs, PP-Modules and packages may present uncompleted security components allowing authors basing documents upon them appropriate flexibility.

The security requirements consist of two groups of requirements:

a) *the security functional requirements* (SFRs): a translation of the security objectives for the TOE into a standardized language;

b) *the security assurance requirements* (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

NOTE SARs concern the adherence of the TOE to the ST. SARs play no role in the coverage of the SPD, which is covered by security objectives and security functional requirements.

These two groups are discussed in 7.3.2 and 7.3.3.

7.3.2 Security Functional Requirements

7.3.2.1 General

The SFRs are a translation of the security objectives for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives shall be completely addressed). ISO/IEC 15408 (all parts) requires this translation into a standardized language for several reasons:

- to provide a precise description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardized language enforces a more precise description of the functionality of the TOE.

- to allow comparison between two STs. The standardized language enforces using the same terminology and concepts. This allows comparison of STs even when authors use different terminology in describing their SPD and security objectives (this situation does not arise when the STs conform to the same PPs/PP-Configurations).

In the context of PPs and PP-Modules, the SFRs shall be independent of any specific technical solution (implementation).

There is no translation required in this document for the security objectives for the operational environment, because the operational environment is not evaluated and does therefore not require a description aimed at its evaluation.

NOTE See the bibliography for items relevant to the security assessment of operational systems.

It can be the case that parts of the operational environment are evaluated in another evaluation, but this is out of scope for the current evaluation.

EXAMPLE

An OS TOE may require a firewall to be present in its operational environment. Another evaluation may subsequently evaluate the firewall, but this evaluation has nothing to do with the evaluation of the OS TOE.

7.3.2.2 How this translation is supported

ISO/IEC 15408 (all parts) supports this translation in three ways:

a) by providing a pre-defined “language” designed to describe precisely what is to be evaluated. This language is defined as a set of components defined in ISO/IEC 15408-2. The use of this language as a well-defined translation of the security objectives for the TOE to SFRs is mandatory, though some exceptions exist and are given in 8.4.

b) by providing operations: mechanisms that allow the author of the package, ST, PP or PP-Module to complete and modify the SFRs to provide a more accurate translation of the security objectives for the TOE or TOE type. This document defines the four allowed operations: assignment, selection, iteration, and refinement. These are described further in 8.2.

c) by providing dependencies: a mechanism that supports a more complete translation to SFRs. In ISO/IEC 15408-2 language, an SFR may have a dependency on other SFRs. This signifies that if a ST uses that SFR, it generally needs to use those other SFRs as well. This makes it much harder for the ST author to overlook including necessary SFRs and thereby improves the completeness of the ST. Dependencies are described further in 8.3.

7.3.2.3 Relation between SFRs and security objectives

PPs, PP-Modules, STs and packages contain a security requirements rationale, consisting of two sections about SFRs:

- a tracing that shows which SFRs address which security objectives for the TOE;
- a set of justifications that shows that all security objectives for the TOE are effectively addressed by the SFRs.

NOTE In the Direct Rationale approach the tracing and rationale is provided between the SFRs and the SPD.

7.3.2.4 Tracing between SFRs and the security objectives for the TOE

The tracing shows how the SFRs trace back to the security objectives for the TOE as follows:

a) *No spurious SFRs*: Each SFR traces back to at least one security objective.

b) *Complete with respect to the security objectives for the TOE*: Each security objective for the TOE has at least one SFR tracing to it.

Multiple SFRs may trace to the same security objective for the TOE, indicating that the combination of those security requirements meets that security objective for the TOE.

7.3.2.5 Providing a justification for the tracing

The security requirements rationale demonstrates that the tracing is effective: if all SFRs tracing to a particular security objective for the TOE are satisfied, that security objective for the TOE is achieved.

This demonstration analyses the effects of satisfying the relevant SFRs on achieving the security objective for the TOE and lead to the conclusion that this is indeed the case.

7.3.2.6 Types of SFR

7.3.2.6.1 Optional requirements

Optional requirements are “optional” in the sense that they do not need to be included in a ST in order for the PP/ST to claim conformance (of any type) to a PP or PP-Configuration.

Packages, PPs, PP-Modules may define optional requirements in one of two categories. Each category is specified explicitly by the author.

The first category of optional requirements is elective. Requirements in this category do not need to be included in a ST in order for the ST to claim conformance (of any type) to the PP. In this case, it is not obligatory that the ST includes the requirement, even if the TOE implements the functionality described by the requirement.

The second category of optional requirements is conditional. If the TOE implements the described functionality then the optional requirement shall be included in the ST. If the TOE does not implement the functionality covered by the optional requirement, then the requirement is not included in the ST.

NOTE Optional requirements can be written in response to SPD-elements that exist in the package, PP or PP-Module, or SPD-elements that are specifically associated with the requirement. Such associations are identified in the PP. Direct Rationale PPs do not have security objectives for optional requirements that have associated SPD elements, while regular PPs include security objectives for the associated SFRs and SPD elements.

7.3.2.6.2 Selection-based requirements

Packages, PPs and PP-Modules may identify a set of selection-based SFRs. In this case, the author additionally ensures that the package/PP/PP-Module clearly indicates the dependencies between a particular selection in a security functional component and/or SFR included in the package/PP/PP-Module and the associated selection-based SFR(s) that shall be included if that selection is chosen by another PP/ST author. This is explained in 8.2.4.2.

7.3.3 Security assurance requirements (SARs)

7.3.3.1 General

The SARs are a description of how the TOE is to be evaluated that may be defined in packages, PPs, PP-Modules, PP-Configurations and STs. This description uses a standardized language for two reasons:

- to provide a precise description of how the TOE is to be evaluated.
- to allow comparison between two STs. The standardized language enforces using the same terminology and concepts.

This standardized language is defined as a set of components defined in ISO/IEC 15408-3. The use of this language is mandatory, though some exceptions exist. ISO/IEC 15408 enhances this language in two ways:

a) by providing operations: mechanisms that allow the PP/ST author to modify the SARs. ISO/IEC 15408 has four operations: assignment, selection, iteration, and refinement. These are described further in 8.2.

b) by providing dependencies: a mechanism that supports a more complete translation to SARs. In ISO/IEC 15408-3 language, a SAR can have a dependency on other SARs. This signifies that if a ST, PP, PP-Module or PP-Configuration uses that SAR, it generally needs to use those other SARs as well. This makes it much harder for the author to overlook including necessary SARs and thereby improves the completeness of STs, PPs, PP-Modules or PP-Configurations. Dependencies are described further in 8.3.

NOTE The SARs defined in ISO/IEC 15408-3 do not allow use assignment or selections. However, it is possible to define extended assurance components which allow those operations.

7.3.3.2 SARs and the security requirement rationale

PPs, PP-Modules, PP-Configurations, assurance packages and STs also contain a security requirements rationale that explains why the chosen set(s) of SARs was(were) deemed appropriate. There are no specific requirements for this explanation. The goal for this explanation is to allow the readers to understand the reasons why this particular set was chosen.

NOTE: In the case of exact conformance a PP-Module inherits the SARs from its base PPs hence no rationale for the SARs is required.

SARs contribute to the confidence that a risk owner can place in an evaluation. Many SARs given in ISO/IEC 15408-3 relate to the design and development processes used in the implementation of a TOE by a developer and to developer testing. Some SARs relate to an operational TOE such as secure delivery process and flaw remediation. Some SARs relate specifically to evaluator vulnerability analysis and independent functional and penetration testing.

EXAMPLE

An example of an inconsistency in the selection of SARs is if the SPD mentions threats where the threat agent is very capable, and a low (or no) vulnerability analysis (AVA_VAN) is included in the SARs.

7.3.4 Security requirements: conclusion

In the SPD section of the PP, PP-Module, functional package and ST, the security problem is defined as consisting of threats, OSPs and assumptions. In the security objectives section of the ST, the solution is provided in the form of two sub-solutions:

- security objectives for the TOE;
- security objectives for the operational environment.

Additionally, a security objectives rationale is provided showing that if all security objectives are achieved, the security problem is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

In the security requirements section, the security objectives for the TOE are translated to SFRs and a security requirements rationale is provided showing that if all SFRs are satisfied, all security objectives for the TOE are achieved.

Additionally, a set of SARs is provided to show how the TOE is evaluated, together with an explanation for selecting these SARs. The set of SARs shall be in line with the security expectations derived from the SPD. The explanation for SAR selection may be made in the SAR rationale.

The operational environment itself is not within the scope of the evaluation, although when the AGD assurance class is included in a ST then the TOE guidance must fully reflect these security objectives for the operational environment, and is assessed as part of the evaluation using the AGD class.

All of the above are combined into the statement: If all SFRs and SARs are satisfied and all security objectives for the operational environment are achieved, then there exists assurance that the security problem as defined in ASE_SPD is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld. This is illustrated in Figure 4.

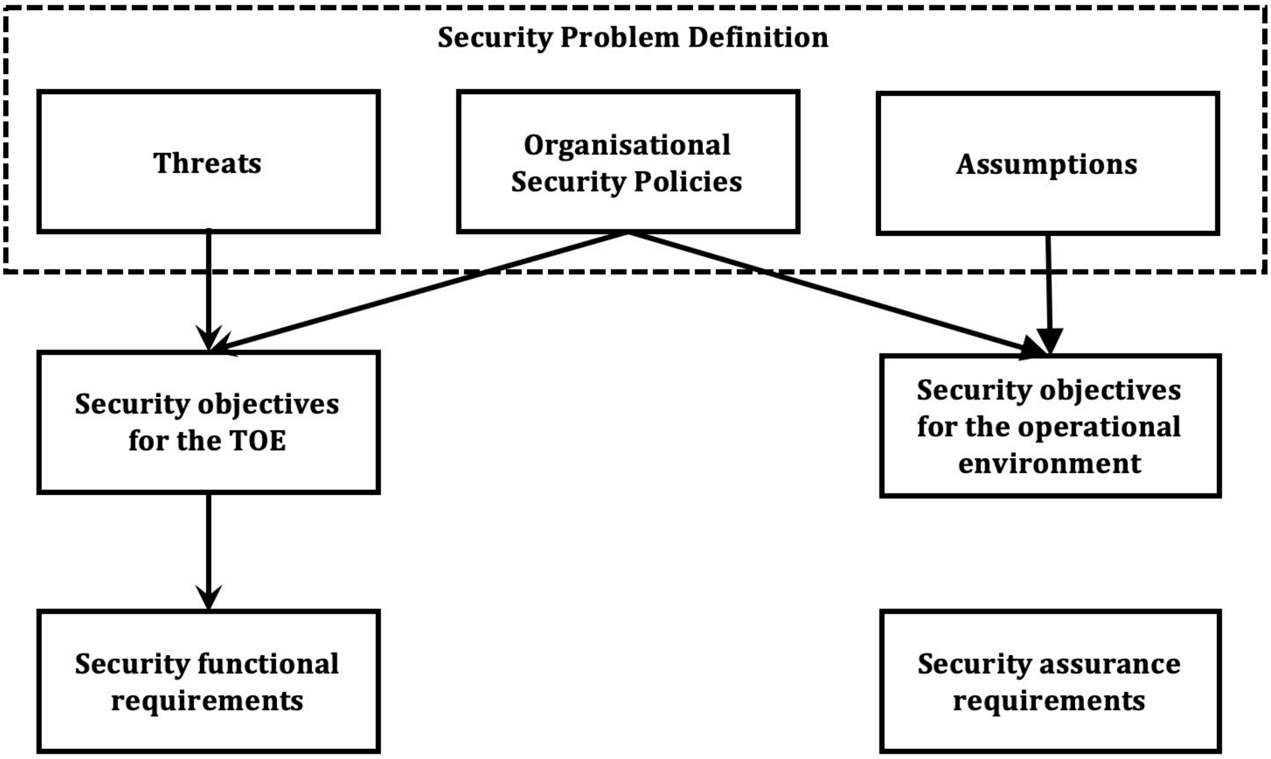

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure 4 — Relations between the SPD, the security objectives, and the security requirements

The amount of assurance obtained is defined by the SARs, and whether this amount of assurance is sufficient to risk-owners using the ST is described in the explanation given for choosing these SARs.

8 Security components

8.1 Hierarchical structure of security components

8.1.1 General

ISO/IEC 15408-2 and ISO/IEC 15408-3 provide catalogues of security components that shall be used when specifying security requirements. The catalogues have organized the components into a hierarchical structure at four levels:

- Classes, consisting of
- Families, consisting of
- Components, consisting of
- Elements, which cannot be decomposed.

8.1.2 Class

The requirements for functional classes are given in ISO/IEC 15408-2 subclause 6.1.2.

A class consists of a set of families.

EXAMPLE

An example of a class is the "FIA: Identification and authentication" class that is focused at identification of users, authentication of users and binding of users and subjects.

8.1.3 Family

The requirements for functional families are provided in ISO/IEC 15408-2 subclause 6.1.3.

A family consists of a set of components.

EXAMPLE

An example of a family is the "User authentication (FIA_UAU)" family which is part of the "FIA: Identification and authentication class". This family concentrates on the authentication of users.

8.1.4 Component

The requirements for functional component structure are provided in ISO/IEC 15408-2 subclause 6.1.4.

A component consists of a set of elements.

EXAMPLE

An example of a component is "FIA_UAU.3 Unforgeable authentication", which concentrates on unforgeable authentication.

8.1.5 Element

The requirements for functional elements are provided in ISO/IEC 15408-2 subclause 6.1.4.

EXAMPLE

An example of an element is "FIA_UAU.3.2", which concentrates on the prevention of use of copied authentication data.

8.2 Operations

8.2.1 General

ISO/IEC 15408-2 and 15408-3 provide catalogues of security components, and this document provides authors with the ability to extend the component catalogues in some circumstances. By applying operations to these security components, they may be tailored precisely to the author's needs when writing PPs, PP-Modules, packages and STs'.

Security components may be used precisely as defined in ISO/IEC 15408-2 and ISO/IEC 15408-3, or they may be tailored through the use of permitted operations.

When using operations, the author should be careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all security requirements. The operations are described in more detail below.

The ISO/IEC 15408-2:20XX annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions shall be followed unless the author justifies the deviation:

a) "None" is only available as a choice for the completion of a selection if explicitly provided.

   The lists provided for the completion of selections shall be non-empty. If a "None" option is chosen, no additional selection options may be chosen. If "None" is not given as an option in a selection, it is permissible to combine the choices in a selection with "and"s and "or"s, unless the selection explicitly states "choose one of".

   Selection operations may be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration should not overlap the subject of the other iterated selection, since they are intended to be exclusive

b) For the completion of assignments, the ISO/IEC 15408-2:20XX annexes shall be consulted in order to determine when "None" would be a valid completion.

8.2.2 The iteration operation

The iteration operation may be performed on every component. The author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component shall be different from all other iterations of that component, which is realized by completing assignments and selections in a different way, or by applying refinements to it in a different way.

Different iterations shall be uniquely identified to allow clear rationales and tracings to and from these requirements. Iteration identifiers should be meaningful to readers.

EXAMPLE

FCS_COP.1 Cryptographic operation being iterated twice in order to require the implementation of two different cryptographic algorithms. An example of each iteration being uniquely identified is:

- Cryptographic operation (RSA signatures) (FCS_COP.1(RSA signatures))
- Cryptographic operation (AES data encryption/decryption) (FCS_COP.1(AES data encryption/decryption))

NOTE Sometimes an iteration operation can be used with components where it is also possible to perform an assignment operation with a range or list of values instead of iterating them. In that case, the author can select the most appropriate alternative, considering if there is a necessity of providing a whole rationale for the range of values or if it is necessary to have a separate one for each of them. The author should also keep in mind if individual traces are required for those values.

8.2.3 The assignment operation

An assignment operation occurs where a given component contains an element with a parameter that may be set by the author. The parameter may be an unrestricted variable, or a rule that narrows the variable to a specific range of values.

Whenever an element in a PP, PP-Module or package within a PP/PP-Module contains an assignment, the author shall do one of four things:

a) leave the assignment uncompleted;

EXAMPLE 1
The author could include FIA_AFL.1.2 in the PP, PP-Module or package.
"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall [assignment: list of actions]**."

In this case, the ST author could complete FIA_AFL.1.2 thus:
"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent that external entity from binding to any subject in the future."

b) complete the assignment;

EXAMPLE 2
The author could include FIA_AFL.1.2 in the PP, PP-Module or package.

"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall prevent that external entity from binding to any subject in the future."

c) narrow the assignment to further limit the range of values that is allowed;

EXAMPLE 3
The author could include FIA_AFL.1.1 in the PP, PP-Module or package.
"The TSF shall detect when [assignment: positive integer] unsuccessful authentication attempts occur ..."

In this case, the ST author could complete FIA_AFL.1.1 thus:
"The TSF shall detect when **3** unsuccessful authentication attempts occur ..."

d) transform the assignment to a selection, thereby narrowing the assignment.

EXAMPLE 4
The author could include FIA_AFL.1.2 in the PP, PP-Module or package.
"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**selection: prevent that user from binding to any subject in the future, notify the administrator]**."

In this case, the ST author could complete FIA_AFL.1.2 thus:
"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent that user from binding to any subject in the future**."

An ST author shall complete all the assignments.

The values chosen in options b), and c) shall conform to the indicated type required by the assignment.

When an assignment is to be completed with a set, an author should provide a description of the set from which the elements of the set may be derived as long as it is clear which subjects are meant.

EXAMPLE 5

Where the set is "subjects"

- all subjects,
- all subjects of type X,
- all subjects except subject a.

8.2.4 The selection operation

8.2.4.1 General

The selection operation occurs where a given component contains an element where a choice from several items has to be made by the author.

Whenever an element in a PP, PP-Module or package contains a selection, the author may do one of three things:

a) leave the selection uncompleted,

b) complete the selection by choosing one or more items,

c) restrict the selection by removing some of the choices but leaving two or more.

Whenever an element in a PP, PP-Module or package contains a selection, a ST author shall complete that selection, as indicated in b) above. Options a) and c) are not allowed for STs.

The item or items chosen in b) and c) shall be taken from the items provided in the selection.

8.2.4.2 Selection-based security functional components and SFRs

A PP, PP-Module or package may define a set of security functional components and/or SFRs called selection-based SFRs. This set of components and/or SFRs is associated with a selection made in another component and/or SFRs in the PP, PP-Module or package. The related selection-based components and/or SFRs shall be included in a PP, PP-Module, package or ST if:

- a selection choice identified in the PP, PP-Module or package indicates that it has an associated selection-based SFR, and
- that selection is made by the author.

The PP, PP-Module or package may be organized so that selection-based components and/or SFRs are grouped together.

For the case that an author needs to leave a selection operation uncompleted, the author shall leave the selection-based components and/or SFRs that are related to the uncompleted selection operation, unchanged.

For the case in which the author needs to complete the selection, authors should include the appropriate selection-based components and/or SFRs in the list of SFRs for the PP, PP-Module, package or ST.

For the case in which the selection operation is to be restricted, i.e. some but not all of the selections are removed, the author shall remove any selection-based components and/or SFRs from the list that corresponds to the choices removed from the selection.

EXAMPLE 1

An example of an element with a selection is:

FPT _TST.1.1 “The TSF shall run a suite of self-tests [selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]] to demonstrate the correct operation of...”

The following is another example of such an SFR:

EXAMPLE 2

An example of a selection-based SFR, where FTP_ITC.1.1 is the SFR with the selection and FCS_IPSEC.1 is the selection-based SFR is:

FTP_ITC.1.1 The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between...

Application Note:

In the selection for FTP_ITC.1.1, the ST author selects the mechanism or mechanisms supported by the TOE, and then ensures that the selection-based requirements in Appendix B of this PP that correspond to the selected mechanism or mechanisms are included in the ST.

And in Appendix B of the example PP:

The following SFRs are included in the ST if the ST author selects “IPsec” in FTP_ITC.1.1:

FCS_IPSEC.1 [...]

8.2.5 The refinement operation

The refinement operation may be performed on every requirement. The author performs a refinement by altering that requirement.

NOTE A series of refined iteration operations can be used to cover all of the subjects, objects, operations, security attributes and/or external entities, but where each individual refinement does not.

The first rule for a refinement is that a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP, PP-Module, package or ST, i.e. a refined requirement shall be "stricter" than the original requirement. If a refinement does not meet this rule, the resulting refined requirement is considered to be an extended requirement and shall be treated as such in accordance with 7.3.

NOTE Refining an audit component with an extra element on prevention of electromagnetic radiation is not allowed.

EXAMPLE 2 An example of a valid refinement is:

FIA_UAU.2.1 "The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user." being refined to "The TSF shall require each user to be successfully authenticated by username/password before allowing any other TSF-mediated actions on behalf of that user."

The only exception to this rule is that an author may refine a SFR to apply to some but not all subjects, objects, operations, security attributes and/or external entities. However, this exception does not apply to refining SFRs that are taken from PPs, PP-Modules or package to which conformance is being claimed; these SFRs shall not be refined to apply to fewer subjects, objects, operations, security attributes and/or external entities than the SFR in the originating PP, PP-Module or package.

EXAMPLE 3 An example of a such an exception is:

FIA_UAU.2.1 "The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user." being refined to "The TSF shall require each user originating from the internet to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user."

The second rule for a refinement is that the refinement shall be related to the original component.

A special case of refinement is an editorial refinement, where a small change may be made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar, or to make it more understandable to the reader. This change is not allowed to modify the meaning of the requirement in any way.

EXAMPLE 4

An example of an editorial refinement is:

The SFR FPT_FLS.1, "The TSF shall continue to preserve a secure state when the following failures occur: **breakdown of one CPU**"

could be refined to FPT_FLS.1, "The TSF shall continue to preserve a secure state when the following failure occurs: **breakdown of one CPU**"

or even FPT_FLS.1, "The TSF shall continue to preserve a secure state when **one CPU breaks down**".

8.3 Dependencies between components

Dependencies may exist between components. Dependencies arise when a component is not self-sufficient and relies upon the presence of another component to provide security functionality or assurance.

The functional components in ISO/IEC 15408-2 typically have dependencies on other functional components. Some of the assurance components in ISO/IEC 15408-3 also have dependencies, which in turn, may have dependencies on other ISO/IEC 15408-3 components.

ISO/IEC 15408-2 dependencies on ISO/IEC 15408-3 components may also be defined. Extended functional/assurance components may define dependencies similarly.

Component dependency descriptions are determined by consulting the component definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, or the extended components definition. In order to ensure completeness of the TOE security requirements, dependencies should be satisfied when requirements based on components with dependencies are incorporated into PPs, PP-Modules, packages or STs. Dependencies should also be considered when constructing packages.

In other words: if component A has a dependency on component B, this means that whenever a PP, PP-Module, package or ST contains a security requirement based on component A, the PP, PP-Module, package or ST shall also contain one of:

a) a security requirement based on component B, or

b) a security requirement based on a component that is hierarchically higher than B, or

c) a justification why the PP, PP-Module, package or ST does not contain a security requirement based on component B.

In cases a) and b), when a security requirement is included because of a dependency, it may be necessary to complete operations (assignment, iteration, refinement, selection) on that security requirement in a particular manner to make sure that it actually satisfies the dependency.

In case c), the justification that a security requirement is not included should address either:

— why the dependency is not necessary or useful, or

— that the dependency has been addressed by the operational environment of the TOE, in which case the justification should describe how the security objectives for the operational environment address this dependency, or

— that the dependency has been addressed by the other SFRs in some other manner (extended SFRs, combinations of SFRs etc.).

8.4 Extended components

8.4.1 General

Security requirements shall be based on components from ISO/IEC 15408-2 or ISO/IEC 15408-3 with three exceptions:

a) there are security objectives for the TOE that cannot be translated to SFRs using components in ISO/IEC 15408-2,

b) a security objective for the TOE that can be translated to SFRs, but only with great difficulty and/or complexity based on components in ISO/IEC 15408-2, there are third party requirements that cannot be translated to SARs using components in ISO/IEC 15408-3,

EXAMPLE

Laws and/or regulation regarding the evaluation of cryptography.

In these cases, the author is required to define new components called extended components. A precisely defined extended component is needed to provide context and meaning to the extended SFRs and SARs based on that component.

After the new components have been defined correctly, the author may then base one or more SFRs or SARs on these newly defined extended components and use them in the same way as the other SFRs and SARs. From this point on, there is no further distinction between SFRs and SARs drawn from ISO/IEC 15408 (all parts) and SFRs and SARs based on extended components.

Refer to ISO/IEC 15408-3:20XX, Extended components definition (APE_ECD) and Extended components definition (ASE_ECD) for further requirements on extended components. Further information on extended components is also given in D.3.6.

8.4.2 Defining extended components

Whenever an author of a PP, PP-Module, package or ST defines an extended component, this has to be done in a similar manner to the existing ISO/IEC 15408 series components: clear, unambiguous and evaluable (it is possible to systematically demonstrate whether a requirement based on that component holds for a TOE). Extended components shall use similar labelling, manner of expression, and level of detail as the existing ISO/IEC 15408 series components.

The author also has to make sure that all applicable dependencies of an extended component are included in the definition of that extended component. Examples of possible dependencies are:

a) if an extended component refers to auditing, dependencies to components of the FAU: Security audit class may have to be included;

b) if an extended component modifies or accesses data, dependencies to components of the Access control policy (FDP_ACC) family may have to be included;

c) if an extended component uses a particular design description a dependency to the appropriate ADV: Development family may have to be included.

In the case of an extended functional component, the author also has to include any applicable audit and associated operations information in the definition of that component, similar to existing ISO/IEC 15408-2 components. In the case of an extended assurance component, the author also has to provide suitable evaluation methodology for the component, similar to the method provided in ISO/IEC 18045.

Extended components may be placed in existing families, in which case the author has to show how these families change. If they do not fit into an existing family, they shall be placed in a new family. New families have to be defined similarly to those given in ISO/IEC 15408-2 or ISO/IEC 15408-3.

New families may be placed in existing classes in which case the author has to show how these classes change. If they do not fit into an existing class, they shall be placed in a new class. New classes have to be defined similarly to those defined in ISO/IEC 15408-2 or ISO/IEC 15408-3.

9 Packages

9.1 General

A package is a named set of security components or security requirements.

A package may be defined by any party and is intended to be re-usable. To this goal, it contains requirements that are useful and effective in combination.

Where two or more packages are related to each other, they may be presented as part of a package family, see A.2.

Packages may be claimed by PPs, PP-Modules, PP-Configurations and STs, and used to construct larger packages. Authors shall not rename the claimed or used packages.

NOTE 1 Although no separate criteria are given in ISO/IEC 15408 (all parts) for evaluating packages, once such packages are included in a PP, PP-Module or ST they will be evaluated using the APE, ACE, or ASE criteria.

NOTE 2 ISO/IEC 15408-5 provides commonly used packages, such as Evaluation Assurance Levels (EAL) that have been pre-defined and can be used by PP, PP-Modules, PP-Configurations or ST authors.

NOTE 3 In the case of exact conformance, assurance packages cannot be used in the construction of PP-Modules.

Further information on packages is given in Annex A.

9.2 Package types

9.2.1 General

A package shall be either:

- a functional package, containing functional components or requirements, but no assurance components or requirements, or
- an assurance package, containing assurance components or requirements, but no functional components or requirements.

Mixed packages containing both functional and assurance components or requirements shall not be specified.

All packages shall include

a) The package identification giving a unique name, short name, version, date, sponsor, and the ISO/IEC 15408 edition;

b) The type of the package, either an assurance package or a functional package;

c) A package overview giving a narrative description of the purpose of the package;

d) Application notes, describing additional information in regard to the package including a reference to any evaluation methods(s) and/or activities specified to be used in conjunction with the package;

e) One or more security components or requirements;

f) If extended components have been specified then the package includes an extended components definition;

g) A component rationale that provides the rationale for selecting the functional or assurance components/requirements included in the package

9.2.2 Assurance packages

An assurance package contains a set of assurance components or requirements that may be drawn from ISO/IEC 15408-3, may be extended assurance components, or that may be some combination of both.

An assurance package shall not include an SPD or security objectives.

Assurance packages may be used within PPs, PP-Configurations and STs and, with the exception of the exact conformance case, in PP-Modules.

EXAMPLE

The evaluation assurance levels (EALs) that are defined in ISO/IEC 15408-5 are comprised of SARs drawn from ISO/IEC 15408-3 and comprise a family of security assurance packages.

9.2.3 Functional packages

A functional package contains a set of functional components or requirements that may be drawn from ISO/IEC 15408-2, or may be extended functional components or requirements or some combination of both.

A functional package may include an SPD and security objectives derived from that SPD. If the package defines an SPD then the functional package security objectives shall be given. The objectives include the security objectives for the TOE (these are omitted if the Direct Rationale approach is used), security objectives for the operational environment, and the security objectives rationale.

NOTE When a Direct Rationale approach is used security objectives for the TOE are not included.

Functional packages may be used within PPs, PP-Modules and STs as a means to structure security functionality into building blocks.

Functional packages may have dependencies on other functional packages. Such dependencies shall be documented in the functional package and may also be documented in a PP, PP-Module or ST.

EXAMPLE

A PP defines and includes functional package A; package A has no dependencies. Functional packages B, C, and D are defined elsewhere. Package D has no dependencies, but package C depends on package B. A ST can then claim conformance to the following combinations of PPs and packages:

- The ST claims conformance to the PP (which includes functional package A),
- The ST claims conformance to the PP and functional package B,
- The ST claims conformance to the PP and functional packages B and C,
- The ST claims conformance to the PP and functional package D,
- The ST claims conformance to the PP and functional packages B, C, and D.

The following would not be allowed:

- The ST claims conformance to the PP and functional package C (this is not allowed because package C depends on package B, so it cannot be claimed independently.)

9.3 Package dependencies

A package may not satisfy all of the dependencies of the components contained within it. However, the dependencies shall be met by a PP, PP-Module, PP-Configuration or ST that includes the package. This means that it is the responsibility of the author to ensure either that all the dependencies are met or to include a rationale that explains why the dependencies are not met. This is explained in 8.3.

9.4 Evaluation method(s) and/or activities

Packages may include evaluation methods and/or activities that have been derived from ISO/IEC 18045. Evaluation methods and/or activities that are associated with the package shall be provided in the security requirement section with the relevant security requirement. Application notes, when appropriate, should be associated with the specific requirements in the package.

NOTE ISO/IEC 15408-4 provides a framework to perform such derivations.

10 Protection Profiles

10.1 General

A PP is intended to describe a general TOE type. Therefore, a PP may be used:

- as a ST template for any TOEs that meet the PP's TOE type;
- as a template for other PPs in order to further refine the TOE type;
- as a basis for a PP-Module, in which context it is known as a base PP.

A detailed description of PPs is given in Annex B.

EXAMPLE

A TOE type could be "Firewall";

A refined TOE type could be "Stateful inspection firewalls";

A specific TOE related to that TOE type could be the "MinuteGap Firewall v18.5".

A PP describes the general requirements for a TOE type, and is therefore typically sponsored by:

- A technical user community seeking to come to a consensus on the requirements for a given TOE type;
- A developer of a TOE, or a group of developers of similar TOEs wishing to establish a minimum baseline for that type of TOE;
- An organization, such as a government or large corporation, specifying its security requirements as part of its acquisition process.

NOTE 1 A ST describes requirements for a specific TOE and is typically sponsored by the developer of that TOE.

A PP shall be identified with a reference.

NOTE 2 The reference identifier for a PP must be unique within a catalogue.

10.2 Conformance claims and conformance statements

The conformance claims of PPs:

a) shall state the **edition of ISO/IEC 15408** to which the PP claims conformance;

b) shall describe the conformance to ISO/IEC 15408-2 (security functional requirements) as either:

- **ISO/IEC 15408-2 conformant -** A PP is ISO/IEC 15408-2 conformant if all SFRs in that PP are based only upon functional components in the ISO/IEC 15408-2; or
- **ISO/IEC 15408-2 extended -** A PP is ISO/IEC 15408-2 extended if at least one SFR in that PP is not based upon functional components in ISO/IEC 15408-2;

c) shall describe the conformance to ISO/IEC 15408-3 (security assurance requirements) as either:

- **ISO/IEC 15408-3 conformant -** A PP is ISO/IEC 15408-3 conformant if all SARs in that PP are based only upon assurance components in ISO/IEC 15408-3; or
- **ISO/IEC 15408-3 extended -** A PP is ISO/IEC 15408-3 extended if at least one SAR in that PP is not based upon assurance components in ISO/IEC 15408-3;

d) may include a package conformance claim. More than one package may be claimed in a PP.

If a package claim is made, it shall consist of one of the following statements for each package claim:

- **Package name Conformant -** A PP is conformant to a package if:
  - For functional packages, all constituent parts (SPD, security objectives, and SFRs) of the functional package are present in the corresponding parts of the PP without modification.
  - For assurance packages, the SARs of that PP are identical to the SARs in the assurance package.
  - A PP that restricts some selections of SFRs in a package may still claim it is package conformant.
- **Package name Augmented** - A PP claims an augmentation of a package if:
  - For functional packages, all constituent parts (SPD, security objectives, and SFRs) of that PP contain all constituent parts given in the functional package but shall have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package.
  - For assurance packages, the SARs of that PP contain all SARs in the assurance package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package;
- **Package name Tailored -** A PP claims tailoring of a package if:
  - For functional packages, all constituent parts (SPD, Security Objectives, and SFRs) of that PP contain all constituent parts given in the functional package, but shall have at least one additional SFR; one SFR that is hierarchically higher than an SFR in the functional package; or additional selection items for an SFR with existing selections in the package.
  - This claim is not valid for assurance packages;

e) may also include a conformance claim with respect to other PPs:

- **PP Conformant** - A PP meets other specific PP(s);

f) shall provide a Conformance Statement: This statement describes the manner in which other PPs or STs shall conform to this PP: The conformance statement shall be one of:

- **Exact conformance**: If the PP states that exact conformance is required, a ST shall conform to the PP in an exact manner;
- **Strict conformance**: If the PP states that strict conformance is required, a PP/ST shall conform to the PP in a strict manner;

— **Demonstrable conformance**: If the PP states that demonstrable conformance is required, the PP/ST shall conform to the PP in a strict or demonstrable manner.

NOTE 1 The meaning of exact, strict and demonstrable conformance is the following:

- Exact conformance: If the PP states that exact conformance is required, a conformant PP/ST shall contain SPD and objectives identical to the PP's, and the same set of PP's SFRs with all the assignments and selections resolved;
- Strict conformance: If the PP states that strict conformance is required, a conformant PP/ST shall contain a superset of PP's SPD, objectives and SFRs, where the new assumptions (if any) do not weaken the PP's SPD, and all the PP's SFRs have their assignments and selections resolved;

  Strict conformance allows the conformant PP/ST not to add any element to the PP's SPD, set of objectives and SFRs, i.e. the superset defined in the PP/ST may be identical to the PP's, with all the SFRs resolved;
- Demonstrable conformance: If the PP states that demonstrable conformance is required, a conformant PP/ST shall contain a SPD, set of objectives and set of SFRs that are equivalent to a superset of PP's SPD, objectives and SFRs, where the new assumptions (if any) do not weaken the PP's SPD, and where the set of the conformant PP/ST SFRs imply the PP's SFRs;

  Demonstrable conformance allows the conformant PP/ST to use different but equivalent statements, and it allows as well to simply define a superset as in the strict conformance case, without changing the statements given in the PP.

NOTE 2 In other words, a PP/ST is only allowed to conform to a PP in a demonstrable manner if the PP explicitly allows this.

NOTE 3 PP-Modules and PP-Configurations cannot claim conformance to a PP. For more information, see clauses 11.2 and 11.3 .

g) may also include a reference to any evaluation methods and/or activities that have been derived from ISO/IEC 18045.

— If evaluation methods and/or activities that have been derived from ISO/IEC 18045 are associated with the PP, then the Conformance Statement shall also include a statement in the following form:

"This PP requires the use of evaluation methods and/or evaluation activities defined in <reference>."

In this statement, *<reference>* is replaced by the identification of the location of the relevant evaluation methods and evaluation activities. This reference may be to the PP itself, or to one or more separate documents.

NOTE 4 Either a PP/ST conforms to a PP or it does not. ISO/IEC 15408 (all parts) does not recognize "partial" conformance. It is therefore the responsibility of the PP author to ensure the PP is not overly onerous, prohibiting PP/ST authors from claiming conformance to the PP. For more information on the conformance statements and claims for PPs, see Annex B.

10.2.1 Assurance requirements

A PP which complies with ISO/IEC 15408-3 (possibly extended) shall define the set of SARs that applies to the entire TOE.

A PP may define a distinctive name for the set of SARs that are applicable. However, if the set of SARs is an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference, then the same name shall be used.

10.3 Additional requirements common to strict and demonstrable conformance

10.3.1 Conformance claims and conformance statements

If a PP/ST claims either strict or demonstrable conformance to multiple PPs, it shall conform to each PP in the manner stated by that PP; that is, either strictly or demonstrably. This means that the PP/ST may conform strictly to some PPs and demonstrably to other PPs.

A PP/ST conforms to a PP if the PP/ST is equivalent or more restrictive than this PP, that is, if:

- all TOEs that meet the PP/ST also meet the PP, and
- all operational environments that meet the PP also meet the PP/ST.

In other words, the PP/ST shall levy the same or more, requirements on the TOE and the same or less conditions on the operational environment of the TOE.

This general statement holds for the different constructs of the PP/ST, namely the Security Problem Definition, the security objectives for the TOE, the security objectives for the Environment, and the security functional and security assurance requirements.

10.3.2 Security problem definition

The conformance rationale in the PP/ST shall demonstrate that the SPD in the PP/ST is equivalent or more restrictive than the SPD in the PP. This means that:

- all TOEs that meet the SPD in the PP/ST also meet the SPD in the PP;
- all operational environments that meet the SPD in the PP also meet the SPD in the PP/ST.

10.3.3 Security objectives

The conformance rationale in the PP/ST shall demonstrate that the security objectives in the PP/ST are equivalent or more restrictive than the security objectives in the PP. This means that:

- all TOEs that meet the security objectives for the TOE in the PP/ST also meet the security objectives for the TOE in the PP;
- all operational environments that meet the security objectives for the operational environment in the PP also meet the security objectives for the operational environment in the PP/ST.

10.4 Additional requirements specific to strict conformance

10.4.1 Requirements for the security problem definition

The PP/ST shall contain the SPD of the PP and may specify additional threats and OSPs; it shall contain all assumptions as defined in the PP, with two possible exceptions as explained in the next two bullets;

- an assumption (or a part of an assumption) specified in the PP may be omitted from the PP/ST if all security objectives for the operational environment defined in the PP addressing this assumption (or this part of an assumption) are replaced by security objectives for the TOE in the PP/ST;
- a new assumption may be added in the PP/ST to the set of assumptions defined in the PP, if this new assumption does not mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP and if this assumption doesn't fulfil an OSP (or a part of an OSP) meant to be addressed by security objectives for the TOE in the PP.

10.4.2 Requirements for the security objectives

The PP/ST:

- shall contain all security objectives for the TOE of the PP but may specify additional security objectives for the TOE;
- shall contain all security objectives for the operational environment as defined in the PP with two exceptions as explained in the next two bullet points;
- may specify that certain security objectives for the operational environment in the PP are security objectives for the TOE in the PP/ST. This is called re-assigning a security objective. If a security objective is re-assigned to the security objectives for the TOE the security objectives

justification has to make clear which assumption or part of the assumption may not be necessary anymore;

- may specify additional security objectives for the operational environment, if these new objectives do not mitigate a threat (or part of a threat) meant to be addressed by security objectives of the TOE in the PP and if these new objectives do not fulfil an OSP (or a part of an OSP) meant to be addressed by security objectives of the TOE in the PP.

10.4.3 Requirements for the security requirements

The PP/ST:

- shall contain all SFRs and SARs in the PP;
- may claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST shall be internally consistent with that in the PP; either the same completion will be used in the PP/ST as that in the PP or one that makes the requirement more restrictive.
  NOTE the rules of refinement apply.

10.5 Additional requirements specific to demonstrable conformance

Demonstrable conformance allows a PP author to describe a common security problem to be solved and provide generic guidelines to the requirements necessary for its resolution, in the knowledge that there is likely to be more than one way of specifying a resolution.

The PP/ST shall contain a rationale on why the PP/ST is considered to be “equivalent or more restrictive” than the PP.

10.6 Additional requirements specific to exact conformance

10.6.1 General

Exact conformance is used when a PP author needs to control what a ST may claim conformance to with respect to the PP that they have written. It is used in cases where the PP author requires that STs which claim conformance to the PP do not include additional SPD, security objectives or requirements that have not been considered by the PP author.

A PP that requires exact conformance in its conformance statement may define optional SFRs and any SPD-elements that are required to support these SFRs. A ST (or PP-Module) may then include these optional SFRs (and any required SPD elements) in its set of requirements while maintaining its exact conformance claim.

A PP with exact conformance type shall not claim conformance to any other PPs of any conformance type. A PP with exact conformance type shall not be included in a PP-Configuration which also includes PPs or PP-Modules with strict or demonstrable conformance type.

NOTE 1 This is because, it is impossible to claim conformance to both a strict/demonstrable conformance PP and an exact conformance PP, since it would mean adding requirements or SPD-elements to the exact conformance PP, which explicitly prohibits this operation.

In the “simple” case where a ST claims exact conformance to a PP, there is no ambiguity whether the ST is exactly conformant or not because the correspondence between the SPD, security objectives, SFRs, and SARs is demonstrated during evaluation without the need to seek PP author input.

However, other cases are allowed where multiple sets of SPD-elements, security objectives, and SFRs may be combined, these cases require mechanisms that preserve the ability of the exact conformance PP authors to control a conformance claim against their PP. These mechanisms are described in the following subclauses.

EXAMPLE

A complex case might be if a PP-Module aims to use a PP as its base PP, or if a ST claims conformance to two PPs.

NOTE 2 If a PP requires exact conformance, then only those SFRs and SARs specified by that PP are allowed in the conformant ST. These security requirements are related to the SPD and security objectives specified in the PP, which are also included in the conformant ST.

10.6.2 Conformance claims and statements

If a PP requires exact conformance in its conformance statement then

a) the PP shall state which other PPs and PP-Modules are allowed to be combined with that PP, specifying which of these are allowed to be claimed in conjunction with the PP by a ST or used together in a PP-Configuration;

b) all the additional PPs to which a ST may claim exact conformance shall also have an exact conformance requirement; and

c) all of the additional PPs shall identify the PP in their respective conformance statements.

d) all of the additional PP-Modules claimed through a PP-Configuration shall identify the PP in their respective conformance statements.

NOTE A PP-Module does not have to identify its own base PPs/PP-Module(s) in its conformance statement; the base PPs/PP-Modules are identified elsewhere in the PP-Module and thus are implicitly allowed to be used with the PP-Module.

10.7 Using PPs

If a PP/ST claims to be conformant to one or more PPs and possibly one or more packages, the evaluation of that PP/ST will include a demonstration that the PP/ST actually conforms to the claimed PPs and/or packages. Details of this determination of conformance is found in Annex A and Annex B.

This allows the following process:

a) An organization seeking to acquire a particular type of IT security product develops their security needs into a PP, then has this PP evaluated and publishes it;

b) A developer takes this PP, writes a ST that claims conformance to the PP and has this ST evaluated;

c) The developer then builds a TOE (or uses an existing one) and has this evaluated against the ST.

The result is that the evaluated TOE meets the requirements of the organization as defined in the PP and that the organization can therefore have confidence that the TOE meets their security needs. A similar line of reasoning applies to packages.

10.8 Conformance statements and claims in the case of multiple PPs

10.8.1 General

ISO/IEC 15408 (all parts) allows both STs and PPs to claim conformance to multiple PPs. The case for a ST claiming conformance to multiple PPs is covered in 11.3.3. Subclause, 10.8, covers the case where a PP claims conformance to multiple PPs.

10.8.2 Where strict or demonstrable conformance is specified

Allowing a PP to claim conformance to multiple PPs permits chains of PPs to be constructed, each PP in the chain is based on the previous PP(s).

EXAMPLE

PPs for an Integrated Circuit and for a Smart Card OS, can be used to construct a Smart Card PP (IC and OS) that claims conformance to both. In turn, this Smart Card PP could be used to develop specific PPs for different use cases, e.g. tachograph card, payment card, electronic passport, etc. A developer could then construct a ST conformant to any of those PPs.

10.8.3 Where exact conformance is specified

A PP shall not claim exact conformance to another PP or combination of PPs.

NOTE 1 In cases where such a combination of functionality is needed, this may be achieved by creating PP-Configurations, where PP-Modules are used to specify additional functionality to one or more base PPs.

11 Modular Requirements Construction

11.1 General

In order to allow a modular description of the TOE's security features, STs can claim conformance to a PP-Configuration instead of PPs. Such PP-Configurations, are built out of PPs, PP-Modules and base PPs/PP-Modules.

PP-Configurations can be constructed to accommodate either a “single-assurance” evaluation approach or a “multi-assurance” evaluation approach. In a single-assurance evaluation approach, a single set of assurance requirements applies to all components of the PP-Configuration. In a multi-assurance evaluation approach, there is a single global set of assurance requirements that applies to all components of the PP-Configuration, but additionally each component (PP-Module, PP) has its own set of assurance requirements to which it is subject. The multi-assurance approach is not allowed for components that require exact conformance. The following sections present the content-related details for these two evaluation approaches; the actual evaluation particulars using these approaches is discussed in Clause 13.

Editor's note: The fact that multi-assurance cannot be used with exact conformance PP-configurations is not part of the definition of the multi-assurance approach. The restriction could be relaxed.

11.2 PP-Modules

11.2.1 General

A PP-Module is an internally consistent set of SPD-elements, security objectives for the TOE and the operational environment, and security functional requirements, defined in the context of one or more PPs and possibly other PP-Modules.

Unlike PPs, PP-Modules address those security features of a given TOE type that cannot be required uniformly for all products of this TOE type.

Unlike PPs, PP-Modules can be used only in PP-Configurations. A PP/ST cannot claim conformance with a PP-Module directly.

EXAMPLE

Examples of features that cannot be required uniformly for all products within a TOE type are authentication using biometrics, Bluetooth security functions, and Wireless Local Area Network clients.

11.2.2 Base PP/PP-Module

For a given PP-Module, a base PP/PP-Module is a PP/PP-Module that is required anytime the given PP-Module is used in a PP-Configuration. See Clause 10 and Annex B.

NOTE 1 In the exact conformance case, a base PP is a PP that has been written with a goal of being used in a PP-Configuration in association with PP-Modules and is allowed to.

NOTE 2 In the demonstrable/strict conformance case, any PP/PP-Module may become the basis of another PP-Module.

11.2.3 Requirements for PP-Modules

11.2.3.1 General

A PP-Module shall be identified with a reference identifier.

NOTE 1 The reference identifier for a PP-Module must be unique within a catalogue.

A PP-Module shall refer to a set of one or more base PPs/PP-Modules, which are required to be used with the PP-Module. A PP-Module may refer to one or more base PP-Modules, provided the base PPs of all the PP-Modules are also required. A PP-Module may refer to alternative sets of base PPs/PP-Modules.

A PP-Module shall specify the TOE type and shall specify additional security functional requirements. A PP-Module may introduce new SPD-elements and objectives and may also refine or interpret some of the SPD-elements of its base PP/PP-Modules.

NOTE 2 The TOE type defined in the PP-Module may supplement the TOE type defined in its base PPs/PP-Modules.

A PP-Module shall provide a **consistency rationale** ensuring that the union of the elements defined in the PP-Module and in its base PPs/PP-Modules do not lead to contradiction.

NOTE 2 In a Direct Rationale PP-Module, security objectives for the TOE are not included.

NOTE 3 The evaluation of a PP-Module alone is meaningless. A PP-Module has to be evaluated as part of a PP-Configuration, at least with its base PPs/PP-Modules.

Further information on PP-Modules is given in C.1.

A PP-Module may complete and/or refine the SPD-elements and security objectives of the base PPs/PP-Modules and shall define a non-empty set of SFRs that are refinement of the SFRs of the base PPs/PP-Modules or new.

A ST that claims conformance to a PP-Configuration including the PP-Module shall then include the PP-Module SPD-elements, security objectives and SFRs, combined with those of the base PPs/PP-Modules.

11.2.3.2 Direct Rationale

A PP-Module may use the Direct Rationale approach, provided that its base PPs/PP-Modules also use the Direct Rationale approach.

11.2.3.3 Conformance type, conformance claims and conformance statements

The conformance claims of a PP-Module:

a) shall state the **edition of ISO/IEC 15408** to which the PP-Module claims conformance;

b) shall describe the conformance to ISO/IEC 15408-2 as either:

  - **ISO/IEC 15408-2 conformant -** A PP-Module is ISO/IEC 15408-2 conformant if all SFRs in that PP-Module are based only upon functional components in the ISO/IEC 15408-2; or
  - **ISO/IEC 15408-2 extended -** A PP-Module is ISO/IEC 15408-2 extended if at least one SFR in that PP-Module is not based upon functional components in ISO/IEC 15408-2;

c) may include a conformance claim made with respect to functional packages. More than one functional package may be claimed by a PP-Module.

   If a package claim is made, it shall consist of one of the following claims for each package:

  - **Package Name Conformant** - PP-Module is conformant to a package if:
    - all constituent parts of the functional package, including the SPD, security objectives, and SFRs, of that functional package are present in the corresponding parts of the PP-Module without modification;
  - **Package Name Augmented** - A PP-Module claims an augmentation of a package if:
    - all constituent parts of the functional package, including the SPD, security objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but shall also contain at least one SFR that is either additional or hierarchically higher than those SFRs contained in the package;

   NOTE 1 A PP-Module does not claim conformance to a functional package that one of its base PPs claims conformance to. The exception to this rule is when the PP-Module augments the functional package as it is instantiated in the base PPs/PP-Modules; in this case the PP-Module would claim the functional package as “Package Name Augmented” in its package conformance claim statement.

- **Package name Tailored -** A PP-Module claims tailoring of a package if:
  - all constituent parts of the functional package, including the SPD, Security Objectives, and SFRs, contained in the PP-Module are identical to those given in the functional package, but shall have at least one additional SFR; one SFR that is hierarchically higher than an SFR in the functional package; or additional selection items for an SFR with existing selections in the package;

d) In the case of strict and demonstrable conformance,

- shall describe the conformance to ISO/IEC 15408-3 as either:
  - ISO/IEC 15408-3 conformant - A PP is ISO/IEC 15408-3 conformant if all SARs in that PP are based only upon assurance components in ISO/IEC 15408-3; or
  - ISO/IEC 15408-3 extended - A PP is ISO/IEC 15408-3 extended if at least one SAR in that PP is not based upon assurance components in ISO/IEC 15408-3;
- may include a conformance claim made with respect to assurance packages. More than one assurance package may be claimed by a PP-Module. If a package claim is made, it shall consist of one of the following claims for each package:
- **Package Name Conformant -** PP-Module is conformant to an assurance package if:
  - all constituent parts of the assurance package are present in the PP-Module without modification;
- **Package Name Augmented** - A PP-Module claims an augmentation of an assurance package if:
  - all constituent parts of the assurance package contained in the PP-Module are identical to those given in the assurance package, but shall also contain at least one SAR that is either additional or hierarchically higher than those SARs contained in the package;

e) In the case of exact conformance:

- the Conformance Statement shall state which other PPs and PP-Modules (which are not in the set of base PPs/PP-Modules) are allowed to be used in a PP-Configuration with that PP-Module;
- the base PPs/PP-Modules for the PP-Module and all of the additional PPs and PP-Modules shall identify the PP-Module in their respective conformance statements.

NOTE 2 Base PPs/PP-Modules do not need to be specified in the PP-Modules' conformance statement.

h) shall provide a Conformance Statement: This statement describes the manner in which STs shall conform to this PP-Module as part of a PP-Configuration: The conformance statement shall be one of:

- **Exact conformance**: The PP-Module shall require exact conformance if and only if all its base PPs/PP-Modules are of exact conformance. A ST shall conform to the PP-Module, as part of a PP-Configuration, in an exact manner;
- **Strict conformance**: If the PP-Module states that strict conformance is required, a ST shall conform to the PP-Module in a strict manner;
- **Demonstrable conformance**: If the PP-Module states that demonstrable conformance is required, the ST shall conform to the PP-Module in a strict or demonstrable manner.

NOTE 1 In the case of exact conformance, all of the referenced base PPs/PP-Modules shall also require exact conformance.

NOTE 2 A PP-Module can require strict or demonstrable conformance although its base PPs/PP-Modules do not all require strict or demonstrable conformance. The combination of demonstrable and strict conformance shall be validated in the PP-Configuration evaluation.

NOTE 3 The explicit declaration of strict or demonstrable conformance allows sponsors to make the most appropriate statement in each PP-Module, independently of its base PPs/PP-Modules.

NOTE 4 A ST is only allowed to conform to a PP-Module in a demonstrable manner if the PP-Module explicitly allows this.

f) may also include a reference to any evaluation methods and/or activities that have been derived from ISO/IEC 18045.

— If evaluation methods and/or activities that have been derived from ISO/IEC 18045 are associated with the PP-Module, then the Conformance Statement shall also include a statement in the following form:

"This PP-Module requires the use of evaluation methods and/or evaluation activities defined in <reference>."

In this statement, *<reference>* is replaced by the identification of the location of the relevant evaluation methods and evaluation activities. This reference may be to the PP-Module itself, or to one or more separate documents.

For more information on the conformance types, claims and statements for PP-Modules, see Annex C.

11.2.3.4 Assurance requirements

A PP-Module of demonstrable or strict conformance shall define the set of SARs that applies to the TSF defined in the PP-Module, which can be either inherited from the base PPs/PP-Modules or explicitly declared by the PP-Module author.

A PP-Module may define a distinctive name for its set of SARs. However, if the PP-Module declares an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference or inherits the set of SARs from its base PPs/PP-Modules, then the same name shall be used.

A PP-Module of demonstrable or strict conformance shall provide an **assurance rationale** that justifies the internal consistency of its set of SARs, that is:

- the consistency of the set of SARs with regard to the threat model as defined in the SPD of the PP-Module,
- if the PP-Module does not inherit its set of SARs from its base PPs/PP-Modules, the consistency of the set of SARs with all the sets of SARs defined in the base PPs/PP-Modules of the PP-Module.

NOTE 1 Consistency refers to the absence of contradiction. An example of an inconsistency between SARs and SPD would be to consider highly skilled threat agents together with a low AVA_VAN level that cannot consider these threat agents by definition.

NOTE 2 The PP-Module assurance rationale ensures that the set of SARs defined in the PP-Module does not undermine the security that is expected for the assets that are shared between the PP-Module and its base PPs/PP-Modules (if shared assets exist).

NOTE 3 The assurance rationale at PP-Module level contributes but is not sufficient to ensure the consistency of the assurance requirements at PP-Configuration level. See clause 11.3.2.4.

NOTE 4 The assurance rationale may rely on the relationship of the set of SARs in the PP-Module with the predefined EALs to demonstrate the internal consistency.

A PP-Module of exact conformance type does not have a set of SARs explicitly associated with it; it "inherits" the SARs of its base PP(s). If the PP-Module specifies a set of base PPs, the base PPs must have identical SARs.

11.3 PP-Configurations

11.3.1 General

A PP-Configuration is a set of meta-data giving the specification for the construction of a set of requirements—to which conformance can be claimed.

A PP-Configuration is intended to describe a general TOE type. A PP-Configuration:

- may be used as a ST template for any TOEs that meet the PP-Configuration's TOE type;
- cannot be used as a template for other PP-Configurations, PPs or PP-Modules.

A PP-Configuration contains a set of PPs and PP-Modules (the PP-Configuration components) and cannot not claim conformance to any functional packages, except indirectly through its PPs/PP-Modules. PP-Configurations may contain SARs and claim conformance to assurance packages.

Two types of PP-Configurations are identified, each has different requirements for their construction and are applicable depending on the needs of the consumer (risk owner). These are:

- *Single Assurance PP-Configuration:* This describes a configuration type in which all the SARs in the PP-Configuration components are identical. Conformance types of the PPs/PP-Modules may be exact, strict or demonstrable.
- *Multi Assurance PP-Configuration:* This describes a configuration type in which the SARs in the PP-Configuration components may not be identical. Conformance types of the PPs/PP-Modules may be strict or demonstrable.

11.3.2 Requirements for PP-Configurations

11.3.2.1 General

A PP-Configuration shall be identified with a reference.

NOTE 1 The reference identifier for a PP-Configuration must be unique within a catalogue.

A PP-Configuration shall define the PP-Configuration **components list** that uniquely identifies all the PPs and PP-Modules that compose, by reference, the PP-Configuration. A PP-Configuration shall contain one PP and at least another component. It may contain a PP-Module provided its set of base PPs/PP-Modules are also included in the PP-Configuration. It may contain PPs that have no associated PP-Module.

A PP-Configuration shall define the **TOE type** to which it applies.

A PP-Configuration contains exactly, by reference, the SPD, security objectives, SFRs, and functional packages defined in its PPs/PP-Modules; the specification of any additional element shall be done in one of its PPs/PP-Modules.

A PP-Configuration shall provide a **consistency rationale** ensuring that the union of the elements defined in its components do not lead to contradiction.

A multi-assurance PP-Configuration shall describe the organization of the TSF in terms of the sub-TSFs that are defined in its PPs/PP-Modules and shall define for each sub-TSF a set of SARs that is consistent with the corresponding PP/PP-Module.

NOTE 2 In the case of a multi-assurance PP-Configuration containing one PP and one PP-Module with different sets of SARs, the TSF organization is the following: the TSF is the union of the SFRs defined in the PP and in the PP-Module, and there are two sub-TSFs, which consist of the PP's TSF and the PP-Module's TSF. The same organization holds for a PP-Configuration composed of two PPs, which define the two sub-TSFs.

NOTE 3 The sub-TSFs contained in a multi-assurance PP-Configuration may have some overlap. This does not impact on the applicable assurance requirements: Each sub-TSF shall be evaluated against its own set of SARs. This means that the overlapping parts may be evaluated against multiple sets of assurance requirements.

A PP-Configuration:

- may be used in context with the Direct Rationale approach described in B.5 and C.2.4. In this case, all of the components of the PP-Configuration shall also use the Direct Rationale approach;
- shall not contain any additional content beyond that described in this document.

NOTE 4 An instantiated PP-Configuration is analogous to a PP that includes all the elements from the PPs and the PP-Modules it contains.

11.3.2.2 Components statement

A PP-Configuration

- shall identify all the components of the PP-Configuration in a components statement. The components statement shall contain two or more PP or PP-Modules, at least one of which shall be a PP.

  NOTE 1 These components include all the base PPs/PP-Modules required by the PP-Modules.

  NOTE 2 The components statement is further described in C.3.1.3.

- shall not claim conformance to another PP-Configuration

  NOTE 3 If this is desired, the effect can be achieved by directly including all components from both PP-Configurations in one new defined PP-Configuration, where exact conformance can be checked and maintained.

- shall include the base PPs/PP-Modules of all the PP-Modules included in the PP-Configuration. If a PP-Module defines alternative sets of base PPs/PP-Modules then only one of these sets shall be used in a PP-Configuration;
- may select more PPs than the base PPs/PP-Modules of the PP-Modules;
- for PP-Configurations using the single-assurance evaluation approach, may identify the sub-TSF that corresponds to each component defined by the PP-Configuration;
- for PP-Configurations using the multi-assurance evaluation approach, shall identify the sub-TSF that corresponds to each component defined by the PP-Configuration.

For an exact PP-Configuration, all PP-Configuration components shall allow each other to be allowed to be used together in their respective conformance statements.

NOTE 4 This is implicit for the base PPs/PP-Modules of a PP-Module. In all other cases, this allowance must be explicitly stated.

11.3.2.3 Conformance claims and conformance statement

The conformance claims of a PP-Configuration

a) shall state the **edition of ISO/IEC 15408** to which the PP claims conformance.

b) shall describe the conformance to ISO/IEC 15408-2 (security functional requirements) as either:

   — **ISO/IEC 15408-2 conformant -** A PP-Configuration is ISO/IEC 15408-2 conformant if all the PPs and PP-Modules in the PP-Configuration are ISO/IEC 15408-2 conformant; or

   — **ISO/IEC 15408-2 extended -** A PP-Configuration is ISO/IEC 15408-2 extended if at least one PP or PP-Module is not based upon functional components in ISO/IEC 15408-2;

c) shall describe the conformance to ISO/IEC 15408-3 (security assurance requirements) as either:

   — **ISO/IEC 15408-3 conformant -** A PP-Configuration is ISO/IEC 15408-3 conformant if all SARs in that PP-Configuration, which may be simply inherited from its components, are based only upon assurance components in ISO/IEC 15408-3; or

   — **ISO/IEC 15408-3 extended** - A PP-Configuration is ISO/IEC 15408-3 extended if at least one SAR in that PP-Configuration, which may be simply inherited from its components, is not based upon assurance components in ISO/IEC 15408-3;

d) may include an assurance package conformance claim. More than one package may be claimed in a PP-Configuration. If an assurance package claim is made, it shall consist of one of the following statements for each package claim:

   — **Package name Conformant** - A PP-Configuration is conformant to an assurance package if:

  - The SARs of that PP-Configuration, which may be inherited from its components, are identical to the SARs in the assurance package.

- **Package name Augmented** - A PP-Configuration claims an augmentation of an assurance package if:
  - The SARs of that PP-Configuration, which may be inherited from its components, contain all SARs in the assurance package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package;

e) shall not include a functional package conformance claim. Functional packages may be claimed by the components of the PP-Configuration;

f) shall not include a conformance claim with respect to other PP-Configurations, PPs or PP-Modules;

g) shall provide a Conformance Statement. This statement describes the manner in which STs shall conform to this PP-Configuration:

- For a PP-Configuration where all its PPs and PP-Modules are of the same conformance type, the conformance statement shall provide a single conformance type, that is one of:
  - **Exact conformance**: If the PP-Configuration states that exact conformance is required, a ST shall conform to the PP-Configuration in an exact manner.
  - **Strict conformance**: If the PP-Configuration states that strict conformance is required, a ST shall conform to the PP-Configuration in a strict manner.
  - **Demonstrable conformance**: If the PP-Configuration states that demonstrable conformance is required, a ST shall conform to the PP-Configuration in a strict or demonstrable manner.
- For a PP-Configuration where the PPs and PP-Modules do not require all the same conformance type, the conformance statement shall provide the **list of the conformance types** that are required by each of the PPs and PP-Modules composing the PP-Configuration. A ST shall conform to the PP-Configuration by conforming to each of the PPs and PP-Modules in the manner they require.

  NOTE 1 This applies only to strict and demonstrable conformance, since the combination of exact conformance with other types of conformance is not allowed in a PP-Configuration.

  NOTE 2 The compatibility of the multiple conformance shall be validated in the ST evaluation, in the same manner as when a ST claims conformance to several PPs that require different conformance.

g) may also include a reference to any evaluation methods and/or activities that have been derived from ISO/IEC 18045.

- If evaluation methods and/or activities that have been derived from ISO/IEC 18045 are associated with the PP-Configuration, then the Conformance Statement shall also include a statement in the following form:

  “This PP-Configuration requires the use of evaluation methods and/or evaluation activities defined in <reference>.”

  In this statement, *<reference>* is replaced by the identification of the location of the relevant evaluation methods and evaluation activities. This reference may be to the PP-Configuration itself, or to one or more separate documents.

NOTE 3 There are implications for conformance statements in PP-Modules in the exact conformance case that are covered in C.2.2.5.

NOTE 4 Guidance on the conformance statement is given in B.3.3.

11.3.2.4 Assurance requirements

A PP-Configuration shall provide a **SAR statement** where the applicable assurance requirements and associated rationale are defined.

A PP-Configuration intending to be used in the single-assurance evaluation approach shall define a single set of SARs for all the components in the PP-Configuration. This set of SARs identified shall be identical to or augment those declared in the individual PP-Configuration components.

A PP-Configuration intending to be used in the multi-assurance evaluation approach (meaning that it consists of demonstrable and/or strict conformance components only) shall define:

- The global set of SARs that applies to the entire TOE. This may be an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference or a set of SARs that is defined within the PP-Configuration itself.
- For each sub-TSF, the set of SARs that applies. This may be the same set of SARs inherited from the PP or PP-Module defining the sub-TSF, or a larger set (augmentation) which requires the update of the SAR rationale provided in the PP/PP-Module.

NOTE 1 The multi-assurance approach allows applying multiple predefined EALs to products with assets of different sensitivity. However, for the same reasons as for PPs in the general model, PP-Configurations can claim sets of SARs that are different from predefined EALs and/or that contain extended SARs.

A PP-Configuration may define distinctive names for the sets of SARs that apply to the entire TOE and to each sub-TSF. However, the use of an (augmented) predefined EAL or an (augmented) assurance package defined in one of the PP-Configuration's components or in another external reference requires the usage of the same name.

A multi-assurance PP-Configuration shall provide an **assurance rationale** for:

- the consistency of the global set of SARs with regard to the threat models as defined in the SPDs of the PPs and PP-Modules in the PP-Configuration, and
- the consistency of the global set of SARs and all the sets of SARs for the sub-TSF with each other.

NOTE 2 In most cases, the global set of SARs can be built as the common set of SARs that apply to all of the sub-TSFs. However, as it is the case with STs in the general model, the PP-Configuration can require additional or higher SARs. The evaluation of the PP-Configuration will ensure the consistency of the claim, similar to the general model for the compliance with two or more PPs defining different sets of SARs, and similar to the approach for a multi-assurance ST which can extend the sets of SARs defined in the PP-Configuration the ST claims conformance to.

NOTE 3 A PP-Configuration cannot claim less assurance requirements as the global set of SARs/assurance package than those contained in the common set of SARs that apply to all of the sub-TSFs. NOTE 4 The PP-Configuration assurance rationale contributes to ensuring that the multiple sets of SARs do not undermine the security expected for the assets that are shared between the PPs and PP-Modules in the PP-Configuration. The PP-Configuration assurance rationale should rely on and/or reuse the assurance rationales given in the PPs and PP-Modules.

Figure 6 shows an example of multi-assurance PP-Configuration with one PP, A, and two PP-Modules, X and Y. SAR_C is the common set of SARs defined in A, X and Y, which has been chosen as the global set of SARs for the entire TOE. In the example, the sets of SARs that apply to the sub-TSFs defined in A, X and Y are unchanged as well.

NOTE 4 The rules allow to augment the sets of SARs.

NOTE 5 SARc may be empty, i.e. there is no common SAR in A, X, Y. In such a case, the author of the PP-Configuration must choose another global set of SARs.

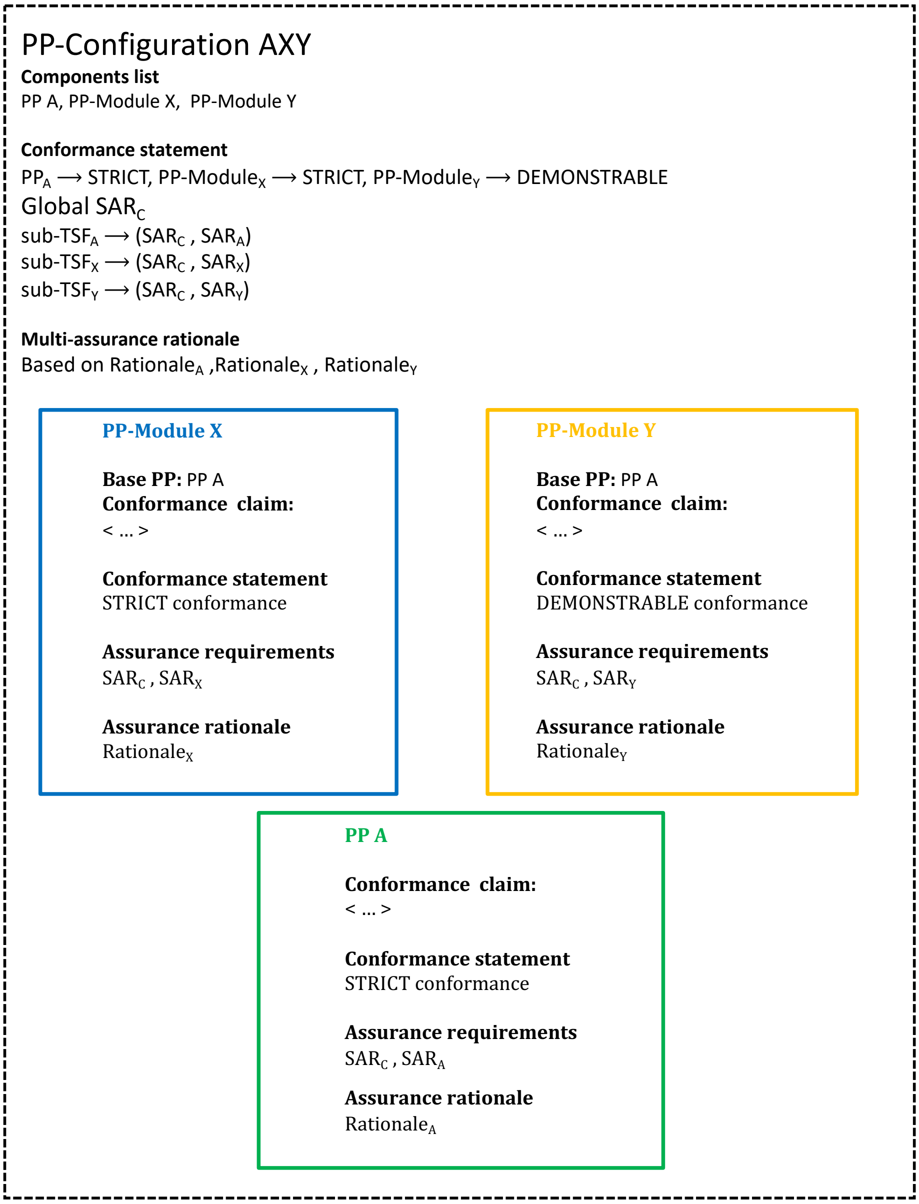

PP-Configuration AXY
Components list
PP A, PP-Module X, PP-Module Y
Conformance statement
PP_A ⟶ STRICT, $PP\text{-}Module_X$ ⟶ STRICT, $PP\text{-}Module_Y$ ⟶ DEMONSTRABLE
Global SAR_C
$sub\text{-}TSF_A$ ⟶ (SAR_C , SAR_A)
$sub\text{-}TSF_X$ ⟶ (SAR_C , SAR_X)
$sub\text{-}TSF_Y$ ⟶ (SAR_C , SAR_Y)
Multi-assurance rationale
Based on $Rationale_A$,$Rationale_X$, $Rationale_Y$
PP-Module X
Base PP: PP A
Conformance claim:
< … >
Conformance statement
STRICT conformance
Assurance requirements
SAR_C , SAR_X
Assurance rationale
$Rationale_X$
PP-Module Y
Base PP: PP A
Conformance claim:
< … >
Conformance statement
DEMONSTRABLE conformance
Assurance requirements
SAR_C , SAR_Y
Assurance rationale
$Rationale_Y$
PP A
Conformance claim:
< … >
Conformance statement
STRICT conformance
Assurance requirements
SAR_C , SAR_A
Assurance rationale
$Rationale_A$

Figure 5 — Example of PP-Configuration

11.3.3 Usage of PP-Configurations

Figure 6 shows the usage of single and multi-assurance PP-configurations.

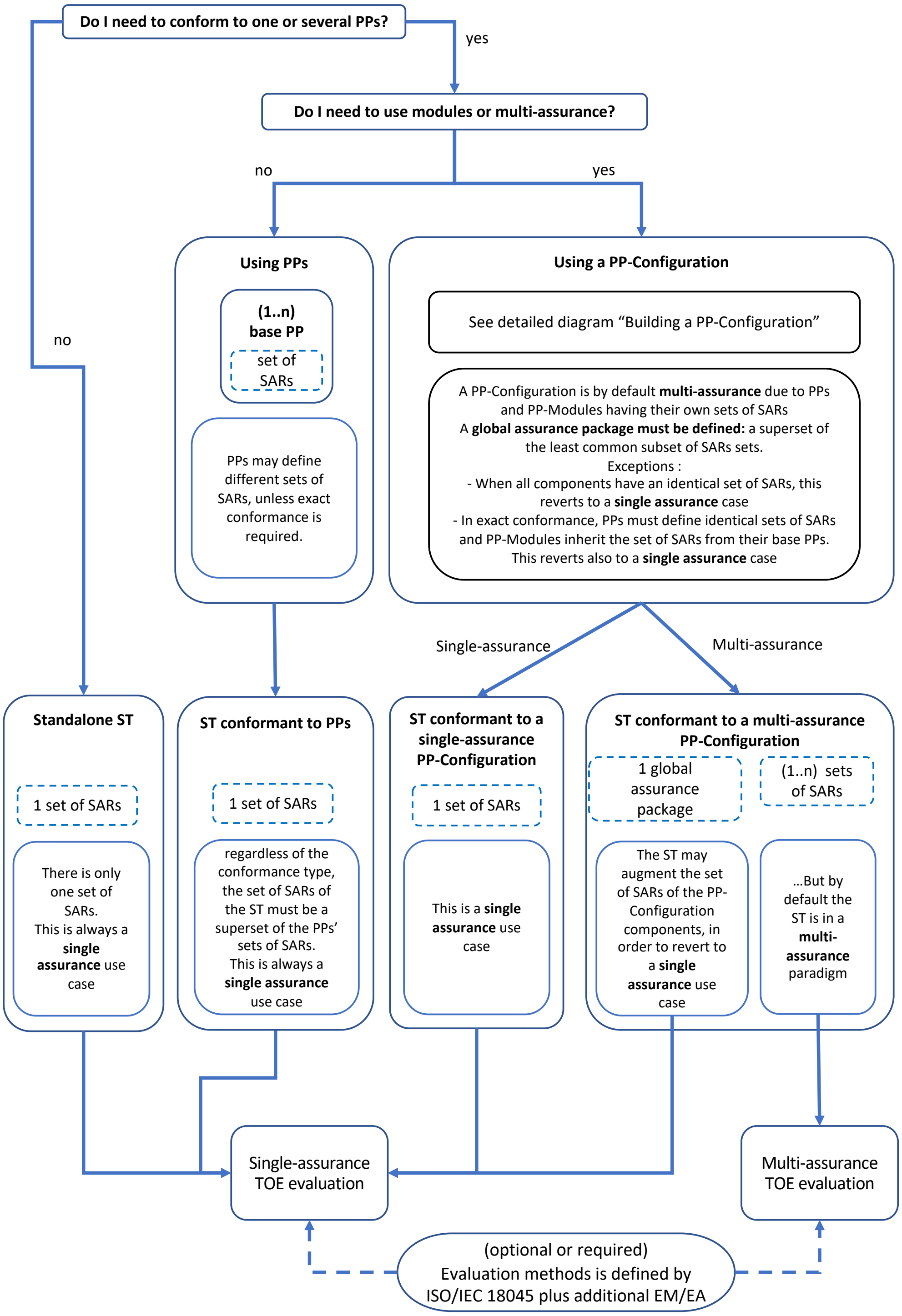

Do I need to conform to one or several PPs?
yes
no
Do I need to use modules or multi-assurance?
no
yes
Using PPs
(1..n) base PP
set of SARs
PPs may define different sets of SARs, unless exact conformance is required.
Using a PP-Configuration
See detailed diagram "Building a PP-Configuration"
A PP-Configuration is by default **multi-assurance** due to PPs and PP-Modules having their own sets of SARs
A **global assurance package must be defined:** a superset of the least common subset of SARs sets.
Exceptions :
- When all components have an identical set of SARs, this reverts to a **single assurance** case
- In exact conformance, PPs must define identical sets of SARs and PP-Modules inherit the set of SARs from their base PPs. This reverts also to a **single assurance** case
Single-assurance
Multi-assurance
Standalone ST
1 set of SARs
There is only one set of SARs. This is always a **single assurance** use case
ST conformant to PPs
1 set of SARs
regardless of the conformance type, the set of SARs of the ST must be a superset of the PPs' sets of SARs. This is always a **single assurance** use case
ST conformant to a single-assurance PP-Configuration
1 set of SARs
This is a **single assurance** use case
ST conformant to a multi-assurance PP-Configuration
1 global assurance package
(1..n) sets of SARs
The ST may augment the set of SARs of the PP-Configuration components, in order to revert to a **single assurance** use case
...But by default the ST is in a **multi-assurance** paradigm
Single-assurance TOE evaluation
Multi-assurance TOE evaluation
(optional or required)
Evaluation methods is defined by ISO/IEC 18045 plus additional EM/EA

Figure 6 — Usage of single and multi-assurance PP-Configurations

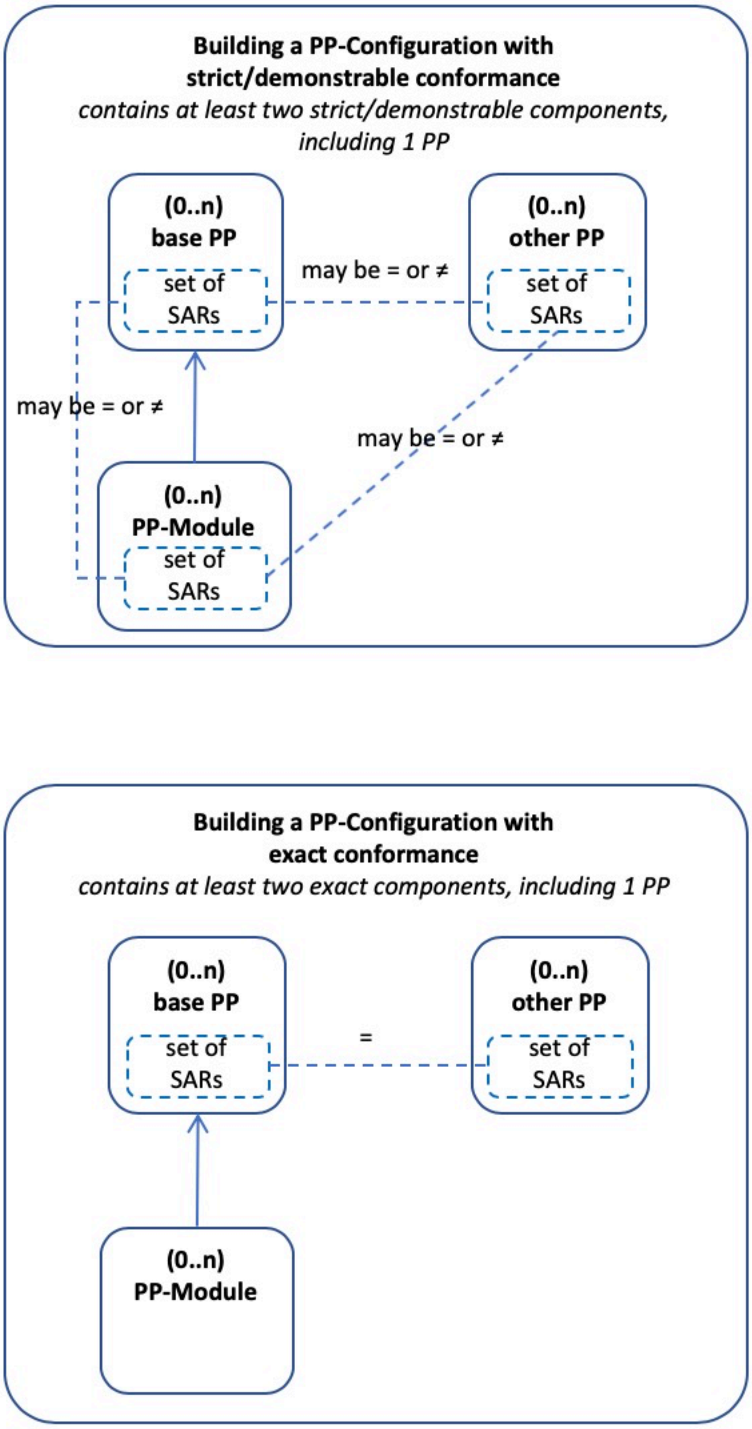

Building a PP-Configuration with
strict/demonstrable conformance
contains at least two strict/demonstrable components, including 1 PP
(0..n)
base PP
set of SARs
may be = or ≠
(0..n)
other PP
set of SARs
may be = or ≠
may be = or ≠
(0..n)
PP-Module
set of SARs
Building a PP-Configuration with
exact conformance
contains at least two exact components, including 1 PP
(0..n)
base PP
set of SARs
=
(0..n)
other PP
set of SARs
(0..n)
PP-Module

Figure 7 — Components of PP-Configurations

12 Security Targets

12.1 General

A ST is a document that describes a specific TOE, the conformance claims applicable to the evaluation of the TOE, the security problem to be addressed, the security objectives for the TOE and its operational environment, the security requirements applicable to solving the stated security problem, and additional material necessary to describe the TOE sufficiently for evaluation. STs are generally based upon PPs or PP-Configurations that describe a security problem and security requirements for a TOE type that is relevant to the specific TOE.

A ST is typically produced by a developer and the audience for the ST includes evaluators, certifying bodies and end users of the evaluated TOE.

Annex D provides further information about STs that shall be used in conjunction with the present clause.

12.2 Conformance claims

The conformance claims of a ST:

a) shall state the edition of **ISO/IEC 15408** to which the ST claims conformance.

b) shall describe the conformance to ISO/IEC 15408-2 (security functional requirements) as either:

- **ISO/IEC 15408-2 conformant** – A ST is ISO/IEC 15408-2 conformant if all SFRs in that ST are based only upon functional components in the ISO/IEC 15408-2, or

- **ISO/IEC 15408-2 extended –** A ST is ISO/IEC 15408-2 extended if at least one SFR in that ST is not based upon functional components in ISO/IEC 15408-2.

NOTE 1 When a TOE is successfully evaluated to a ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also claim to be ISO/IEC 15408-2 conformant.

c) shall describe the conformance to ISO/IEC 15408-3 (security assurance requirements) as either:

- **ISO/IEC 15408-3 conformant** – A ST is ISO/IEC 15408-3 conformant if all SARs in that ST are based only upon assurance components in ISO/IEC 15408-3, or

- **ISO/IEC 15408-3 extended** – A ST is ISO/IEC 15408-3 extended if at least one SAR in that ST is not based upon assurance components in ISO/IEC 15408-3.

d) may include a claim made with respect to packages.
NOTE 1 More than one package can be claimed in a ST.

Where STs claim conformance to PPs or PP-Configurations they shall not also claim conformance to the packages included in the PPs or the PP-Configuration’s components unless, for the case of multi-assurance the package has been augmented by the ST.

For the exact conformance case, STs shall not claim nor augment any packages.

NOTE 2 For exact conformance, it is allowed to claim conformance to a PP that claims conformance to a package, or a PP-Configuration that has components that claim conformance to a package, but those are not reflected in the ST’s conformance claim.

If a package claim is made, it shall consist of one of the following claims for each package:

- **Package name Conformant** - A ST is conformant to a package if:
  - For functional packages, all constituent parts (security problem definition, security objectives, and SFRs) of that ST are identical to the SFRs in the functional package,
  - For assurance packages, the SARs of that ST are identical to the SARs in the assurance package.

- **Package name Augmented** – A ST claims augmentation of a package if:
  - For functional packages, all constituent parts (SPD, security objectives, and SFRs) of that ST contain all constituent parts given in the functional package but shall contain at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.

  - For assurance packages, the SARs of that ST contain all SARs in the assurance package, but shall contain at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package;

- **Package name Tailored** – This claim is not valid for STs.

e) may also include a conformance claim with respect to PPs:

- **PP Conformant** - A PP or TOE meets specific PP(s).
- A Direct Rationale ST may only claim conformance to one or more other Direct Rationale PPs (see Annex B).

f) may also include a conformance claim with respect to PP-Configurations:

- A ST may claim conformance with one or more PP-Configurations when the conformance statement for the PP-Configuration requires strict, demonstrable or a list of strict and demonstrable conformance.

  NOTE 1 A multi-assurance ST must conform to one multi-assurance PP-Configuration, and no other PP or PP-Configuration. For more details, see clause 12.5.

- A ST shall not claim conformance to more than one PP-Configuration when the conformance statement for the PP-Configuration requires exact conformance.
- A Direct Rationale ST shall only claim conformance to a PP-Configuration if that PP-Configuration uses the Direct Rationale approach.

  NOTE 2 PP-Configurations may be used by STs in a manner similar to that employed for PPs.

  NOTE 3 The evaluation of a PP-Configuration can be performed upfront, independently of any product evaluation. Alternatively, the evaluation of a PP-Configuration can be performed during the evaluation of a conformant ST, prior to evaluating the ST conformance claim. See 13.3 for a discussion of the evaluation of PP-Configurations.

  NOTE 4 PP-Modules are used to build specific PP-Configurations on top of one or more base PPs/PP-Modules. Hence, PP-Modules shall only be used by STs through claimed PP-Configurations.

g) If evaluation methods and/or evaluation activities are identified in the conformance statement of any package, PP or PP-Module within the PP-Configuration to which the ST claims conformance, then the conformance claim shall also include a statement in the following form:

"The TOE is evaluated using evaluation methods and/or evaluation activities defined in *<reference>*."

In this statement, *<reference>* is replaced by the identification of the location of the relevant evaluation methods and evaluation activities.

STs that reference evaluation methods and/or activities are not required to reproduce the text of the evaluation methods and/or activities within the ST.

A ST shall only make a conformance claim for evaluation methods and/or evaluation activities that are included in a package, PP, or PP-Module in a PP-Configuration claimed by the ST.

NOTE 1 In the case of PP-Configurations, packages can also include evaluation methods and/or activities, in this case the packages are included in the PP or PP-Module using them.

NOTE 2 The reader is reminded that it could be the case that a ST claims no PP or PP-Configuration but can still directly specify a package.

NOTE 3 A ST may claim conformance with several PPs/PP-Configurations with different types of conformance. The consistency of the combination of demonstrable and strict conformance shall be validated as part of the ST evaluation.

For more information on the conformance statements for STs see Annex D.

For more information on conformance types see Annex E.

12.3 Assurance requirements

A ST that claims conformance with ISO/IEC 15408-3 (possibly extended) shall define the global set of SARs that applies to the TOE.

A ST may define a distinctive name for the set of SARs that are applicable. However, the use of an (augmented) predefined EAL or an (augmented) assurance package defined in an applicable external reference shall require the usage of the same name.

12.4 Additional requirements in the exact conformance case

12.4.1 Additional requirements for the conformance claim

A ST shall not claim conformance to an exact conformance PP/PP-Configuration and, at the same time, to other PPs/PP-Configurations which are not of exact conformance type, i.e. a PP/PP-Configuration of exact conformance shall not be combined with strict or demonstrable conformance.

12.4.2 Additional requirements for the SPD

A ST claiming exact conformance:

- shall contain the SPD of all the packages and the PPs or PP-Configuration to which it is claiming exact conformance, including all SPD elements.
- shall not include any SPD-elements that are not present in the packages or PPs/PP-Configuration to which it is claiming exact conformance.

NOTE The SPD that is instantiated in the ST from a PP-Configuration contains exactly the SPD-elements present in the PP-Configuration’s components (PPs and PP-Modules). It should be noted that PP-Configuration components can combine to change or eliminate SPD-elements (e.g., an assumption in a base PP may become a threat that is countered by a PP-Module on top of that base PP), so the result that appears in the ST considers these kinds of modifications. See 11.3.

12.4.3 Additional requirements for the security objectives

A ST claiming exact conformance:

- shall contain all the security objectives for the TOE specified in all of the PPs to which it claims conformance;
- shall not specify additional security objectives for the TOE that are not specified in the combination of the PPs to which it claims conformance;
- shall contain all of the security objectives for the operational environment that are specified in the combination of PPs to which it claims conformance; and
- shall not specify additional security objectives for the operational environment that are not present in the combination of PPs to which it claims conformance.

NOTE The same is true for PP-Configurations. The security objectives that are instantiated in the ST from a PP-Configuration contain exactly the security objectives present in the PP-Configuration’s components. It should be noted that PP-Configuration components can combine to change or eliminate security objectives (e.g., a security objective for the environment in a base PP may become a TOE security objective in a PP-Module using that base PP), so the resulting ST reflects these kinds of modifications.

12.4.4 Additional requirements for the security requirements

A ST shall contain all the SARs present in the PPs, and all the SFRs present in the PP-Configuration components(s), with the following exceptions:

- ST authors shall not include additional or hierarchically higher security requirements;
- SFRs designated as selection-based SFRs in the PPs or PP-Modules shall be excluded if the selection that requires their inclusion is not chosen by the ST author;
- SFRs designated as optional SFRs in the PPs or PP-Modules may be included or excluded while maintaining its exact conformance claim.

NOTE 1 See 7.3.2.6 for further information in regard to optional and selection-based SFRs.

NOTE 2 See Annex E for further information on PP conformance.

12.5 Additional requirements in the multi-assurance case

A multi-assurance ST shall claim conformance to exactly one multi-assurance PP-Configuration and no other PP or PP-Configuration.

A multi-assurance ST shall organize the TSF in sub-TSFs, and claim a specific set of SARs for each of the sub-TSFs and a global set of SARs for the entire TOE: this can be achieved exclusively through the conformance to a multi-assurance PP-Configuration. The TSF structure defined in the ST is inherited from the PP-Configuration, and the sets of SARs that apply to them in the ST are either identical to the ones defined in the PP-Configuration or augmented.

A multi-assurance ST may extend the PP-Configuration with additional SFRs (and related SPD and security objectives as necessary) so that each new element completes at a minimum one PP or PP-Module of the PP-Configuration provided the required conformity rules are satisfied. That is, the new SFRs are aimed at extending the sub-TSFs defined by the components of the PP-Configuration. As a consequence, the extended sub-TSFs are subject to the set of SARs as defined in the original PPs/PP-Modules.

A multi-assurance ST may claim the sets of SARs defined in the multi-assurance PP-Configuration, or may provide a rationale to claim "augmented" sets of SARs, similar to STs in the general model.

NOTE 1 In order to conform with two or more PPs according to their respective sets of SARs, a multi-assurance PP-Configuration composed of the PPs must be defined and claimed by the ST.

NOTE 2 A ST that claims conformance with a multi-assurance PP-Configuration and augments all the applicable sets of SARs to reach the same set of SARs for the entire TOE and all of the sub-TSFs becomes a single-assurance ST. In this case, the evaluation of the TOE shall follow the single-assurance evaluation approach.

NOTE 3 A ST that claims conformance with several PPs/PP-Configurations can only define a global set of SARs that applies to the entire TOE, thus giving rise to a single-assurance ST. The ASE rules for ensuring the consistency of the assurance requirements of the single-assurance ST with regard to the PPs/PP-Configurations apply.

NOTE 4 A ST that claims conformance with one single-assurance PP-Configuration, i.e. which defines only one set of SARs for the entire TOE and its parts, cannot become a multi-assurance ST. The reason is that the multi-assurance consistency rules are defined at PP-Configuration level. In order to achieve this, a multi-assurance PP-Configuration derived from the PP-Configuration must be defined and evaluated.

For more information on multi-assurance PP-Configurations and STs see 12.4.2. A ST that claims conformance with exactly one multi-assurance PP-Configuration may become a **multi-assurance ST** by defining, for each sub-TSF, the applicable set of SARs. This will either be the same set of SARs inherited from the PP-Configuration, or a larger set (augmentation) which requires the update of the assurance rationale provided in the PP-Configuration.

A multi-assurance ST may define distinctive names for the sets of SARs that apply to the entire TOE and to each sub-TSF. The names shall be consistent with the names given in the PP-Configuration. In general, the use of an (augmented) predefined EAL or an (augmented) assurance package defined in an applicable external reference requires the usage of the same name.

A multi-assurance ST that extends the sets of SARs of the PP-Configuration it claims conformance to shall provide an assurance rationale that justifies the consistency of the extension.

A multi-assurance ST shall conform to each and all of the individual conformance types that are identified in the conformance statement of the multi-assurance PP-Configuration.

NOTE 5 A ST that claims conformance with more than one PP/PP-Configuration can only define a global set of SARs, which applies to the entire TOE. In such a case, the ASE rules for ensuring the consistency of the assurance requirements of the ST with regard to the PPs/PP-Configurations apply.

NOTE 6 A ST that claims conformance with one single-assurance PP-Configuration cannot become a multi-assurance ST. The reason is that the multi-assurance consistency rules are defined in ACE at PP-Configuration level. In order to define a multi-assurance ST, a multi-assurance PP-Configuration should be derived from the single-assurance PP-Configuration first.

Figure 8 shows an example of a multi-assurance ST that claims conformance to PP-Configuration “AXY” composed of PP A and two PP-Modules X and Y. The TSF structure consists of the sub-TSF defined in A, X and Y. The global set of SARs (SAR$_C$) and the multiple sets of SARs applicable to the sub-TSFs come from the PP-Configuration without any augmentation.

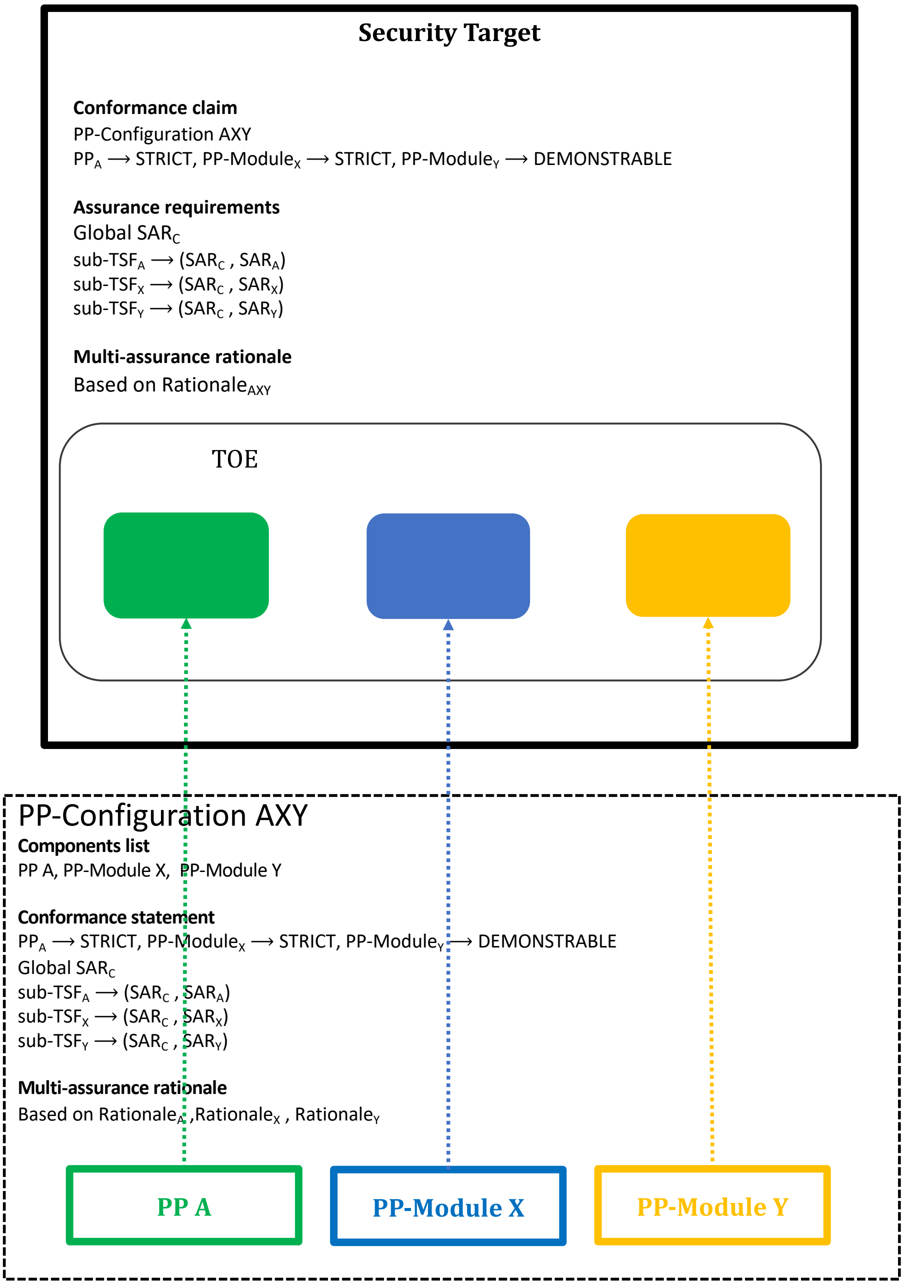

Security Target
Conformance claim
PP-Configuration AXY
PP$_A$ ⟶ STRICT, PP-Module$_X$ ⟶ STRICT, PP-Module$_Y$ ⟶ DEMONSTRABLE
Assurance requirements
Global SAR$_C$
sub-TSF$_A$ ⟶ (SAR$_C$, SAR$_A$)
sub-TSF$_X$ ⟶ (SAR$_C$, SAR$_X$)
sub-TSF$_Y$ ⟶ (SAR$_C$, SAR$_Y$)
Multi-assurance rationale
Based on Rationale$_{AXY}$
TOE
PP-Configuration AXY
Components list
PP A, PP-Module X, PP-Module Y
Conformance statement
PP$_A$ ⟶ STRICT, PP-Module$_X$ ⟶ STRICT, PP-Module$_Y$ ⟶ DEMONSTRABLE
Global SAR$_C$
sub-TSF$_A$ ⟶ (SAR$_C$, SAR$_A$)
sub-TSF$_X$ ⟶ (SAR$_C$, SAR$_X$)
sub-TSF$_Y$ ⟶ (SAR$_C$, SAR$_Y$)
Multi-assurance rationale
Based on Rationale$_A$,Rationale$_X$, Rationale$_Y$
PP A
PP-Module X
PP-Module Y

Figure 8 — Example of multi-assurance ST

13 Evaluation and evaluation results

13.1 General

This Clause 13 presents the expected results from PP, PP-Configuration and ST/TOE evaluations performed according to either ISO/IEC 18045, and/or additional evaluation methods and activities.

The goal of evaluation is to provide objective and repeatable results that can be cited as evidence, even if there is no absolute objective scale for representing the results of a security evaluation.

NOTE A trade-off between following the relevant state of the art and achieving perfect repeatability may be required. Therefore, properties such as objectivity and repeatability are not seen as absolute by the standard, but rather as goals that can be approached in different ways. For example, ISO/IEC 15408-4 provides one such framework for preserving objectivity and repeatability when deriving evaluation activities from ISO/IEC 18045.

An evaluation result represents the findings of a specific type of investigation of the security properties of a TOE. Such a result does not automatically guarantee fitness for use in any particular application environment. The decision to accept a TOE for use in a specific application environment is based on consideration of many security issues including the evaluation findings.

Figure 9 describes the various evaluations that are needed to provide confidence in the evaluation results for a TOE.

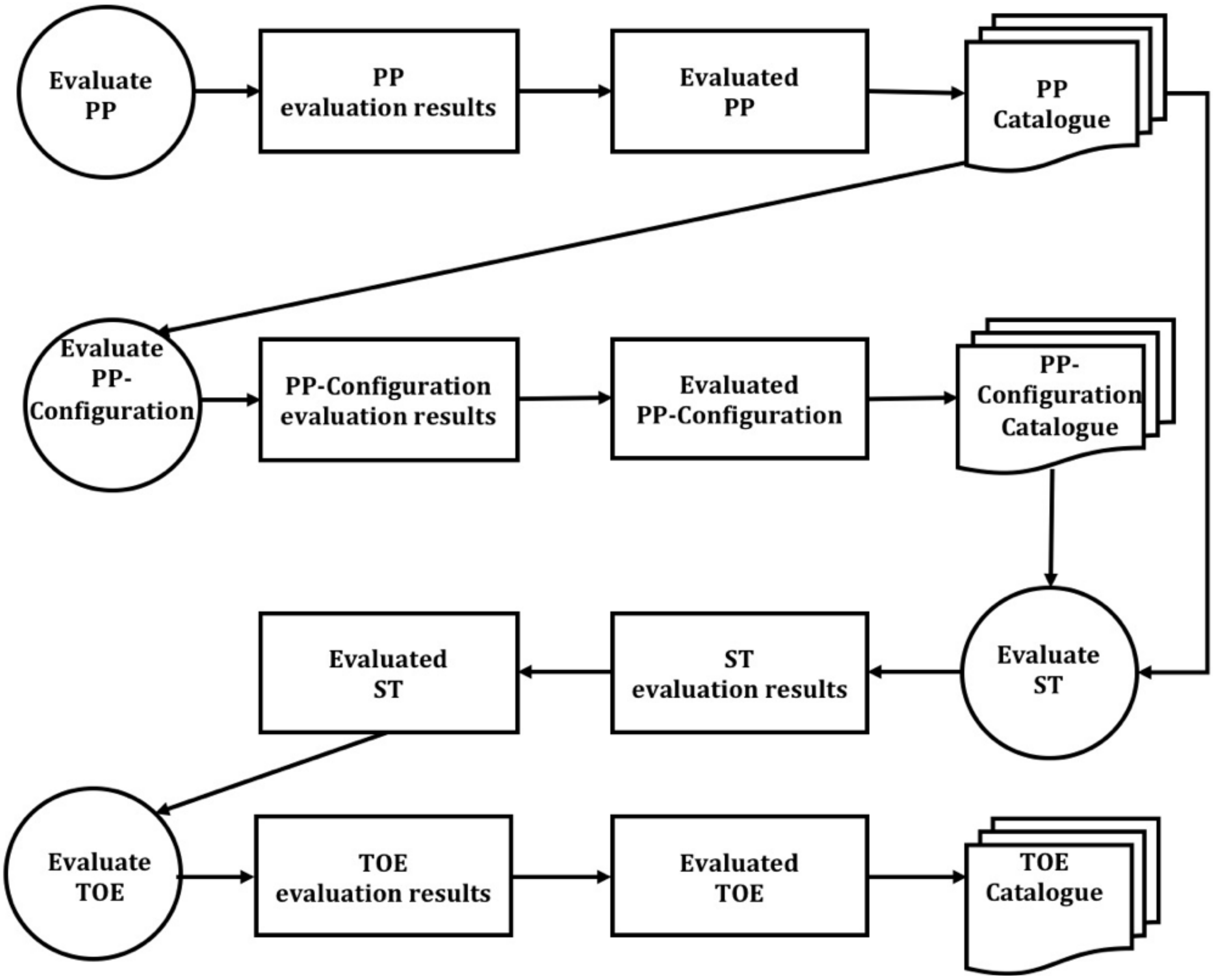


Figure 9 — Evaluation Flow

ISO/IEC 15408 (all parts) gives criteria for four types of evaluation:

a) A PP evaluation which is based on the APE class given in ISO/IEC 15408-3, described in 13.3,

b) A PP-Configuration evaluation which is based on the ACE class given in ISO/IEC 15408-3, described in 13.3,

c) A ST evaluation which is based on the ASE class given in ISO/IEC 15408-3, described in 13.4, and

d) A TOE evaluation, which is based on an evaluated ST and the criteria for evaluating the security requirements claimed by the ST, described in 13.5.

PP and PP-Configuration evaluations provide confidence that the PP and/or PP-Configuration meets the requirements of ISO/IEC 15408 (all parts). Catalogues of PPs and PP-Configurations can be maintained by authorities or others which define the criteria for inclusion in the catalogue.

NOTE 1 The criteria for inclusion in a catalogue are out of scope for ISO/IEC 15408 (all parts).

PP-Modules are only evaluated as part of an evaluation based on a PP-Configuration.

Packages are only evaluated as part of a PP-Configuration, PP, or ST evaluation.

NOTE 2 In practice, a ST that claims conformance with some non-evaluated PP-Configurations may still be evaluated by performing the PP-Configuration evaluation first.

A ST evaluation leads to an intermediate result that is used in the frame of a TOE evaluation. Optionally, STs may be developed with conformance claims to packages, PPs and PP-Configurations.

ST/TOE evaluations can lead to catalogues of evaluated TOEs. In many cases these catalogues refer to the IT products that the TOEs are derived from rather than the specific TOE. Therefore, the existence of an IT product in a catalogue cannot be construed as meaning that the whole IT product has been evaluated; instead the actual ST defines the actual extent of the TOE evaluation.

Refer to the bibliography for examples of such catalogues.

13.2 The evaluation context

In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an evaluation scheme.

NOTE 1 The ISO/IEC 15408 (all parts) does not state requirements for such evaluation schemes.

Supporting greater comparability between evaluation results is also achieved through the use of common evaluation methods producing these evaluation results. Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results can be submitted to a certification process.

NOTE 2 ISO/IEC 14508 does not provide requirements to assess the competences of developers or evaluators. ISO/IEC 19896-3 provides competency requirements for ISO/IEC 15408 evaluators that can be used as a support in the evaluation process. However, it only addresses basic methodology competences and does not address the way to assess:

— technology-specific knowledge and skills such as those required to perform ADV, ATE or AVA_VAN evaluation on a given product type;

— sector-specific knowledge that is typically required to perform ASE, APE or ACE evaluation.

Additionally, specific skills required by ISO/IEC 15408 evaluations may require additional competence assessment methods. For example, to assess skills related to formal methods.

For ISO/IEC 15408 (all parts), the generic methodology for IT security evaluations is given in ISO/IEC 18045. More specific evaluation methods and activities may be derived from ISO/IEC 18045 by using the framework given in ISO/IEC 15408-4, by refining standard assurance components or by defining extended assurance components.

EXAMPLE

It may be necessary for PP authors to augment the generic methodology for IT security evaluations given in ISO/IEC 18045 with a method that includes technology-specific evaluation activities.

A certification process, which is outside the scope of ISO/IEC 15408 (all parts), can include an independent inspection of the results of the evaluation leading to the production of a final certificate or approval, which can be made publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.

13.3 Evaluation of PPs and PP-Configurations

Basing a PP or a ST on an evaluated PP has two advantages:

- There is much less risk that there are errors, ambiguities, or gaps in the PP. If any problems with a PP, that would have been found during the evaluation of that PP, are found during the writing or evaluation of the new ST, significant time can elapse before the PP is corrected.
- Evaluation of the new PP/ST can re-use the evaluation results of the evaluated PP, resulting in less effort being employed in the evaluation of the new PP/ST.

If the evaluation of a PP is required then the APE criteria, given in ISO/IEC 15408-3 shall be used.

If the evaluation of a PP-Configuration is required then the ACE criteria given in ISO/IEC 15408-3 shall be used.

The goal of such evaluations is to demonstrate that the PP, or PP-Configuration is complete, internally consistent, and technically sound and suitable for use as a template on which to build a ST or another PP.

The method of stating evaluation results for PPs and PP-Configurations is described in 13.7.

NOTE PP-Modules are not evaluated separately; they are evaluated in the course of evaluating the PP-Configuration that uses them.

13.4 Evaluation of STs

A ST evaluation determines the sufficiency of the TOE, the operational environment and the internal consistency of the descriptions and requirements it contains.

The ST evaluation shall be carried out by applying the ASE evaluation criteria, defined in ISO/IEC 15408-3. The precise methods and activities used to apply the ASE criteria is determined by the evaluation methodology that is associated with the ST, which may be either ISO/IEC 18405 or evaluation methods and/or activities that have been derived from ISO/IEC 18045.

The method of stating ST evaluation results is described in 13.7. These results also identify any PP(s) and package(s) to which the ST claims conformance.

13.5 Evaluation of TOEs

A TOE evaluation determines that the correctness of the TOE against the criteria defined in the ST. As said earlier, the TOE evaluation does not assess the correctness of the operational environment.

The TOE evaluation is more complex. The principal inputs to a TOE evaluation are the evaluation evidence, which includes the TOE and the ST, but will usually also include input from the development environment, such as design documents or developer test results.

The TOE evaluation consists of applying the SARs (from the ST) to the evaluation evidence. The precise method to apply a specific SAR to a TOE is determined by the ISO/IEC 18045 and by evaluation methods and/or activities that are derived from ISO/IEC 18045. Such EMs/EAs are validated outside of the ISO/IEC 15408 and ISO/IEC 18045 framework. Users of this document/series should be aware that evaluation schemes may not approve the use of particular EMs/EAs. A ST may require EMs/EAs, and an evaluation scheme may decide not to carry out evaluations following this ST.

How the results of applying the SARs are documented, and what reports need to be generated and in what detail, is determined by both the evaluation methodology that is used and the evaluation scheme under which the evaluation is carried out.

The TOE evaluation may be carried out after TOE development has finished, or in parallel with TOE development, provided that the appropriate assurance components are chosen for this evaluation.

The method of stating ST/TOE evaluation results is described in 13.7.

13.6 Evaluation methods and activities

Generic IT evaluation methods and activities for each of the security assurance classes given in ISO/IEC 15408-3 are provided in ISO/IEC 18045. The evaluation methods and activities given in ISO/IEC 18045 are high level and depending on the technology type, the assurance level, or the security problem described, the provision of more specific evaluation methods and activities may be needed.

Such evaluation methods and/or activities that have been derived from ISO/IEC 18045. Such methods and activities may be published either as an inclusion in PPs, PP-Modules and packages or as separate supporting documents.

13.7 Evaluation results

13.7.1 Results of a PP evaluation

The results of the PP evaluation shall include a “Conformance Claim” in accordance with 10.2.

NOTE ISO/IEC 15408-3 provides evaluation criteria for PPs in the APE class.

13.7.2 Results of a PP-Configuration evaluation

The results of a PP-Configuration evaluation shall include a “conformance claim” in accordance with 11.3.

Once a PP-Configuration has been evaluated, a ST evaluation may rely on the results of the PP-Configuration evaluation.

NOTE 1 ISO/IEC 15408-3 provides evaluation criteria for PP-Configurations in the ACE class.

NOTE 2 The evaluation of a PP-Configuration can arise in two situations, with no impact on the evaluation methodology:

- Independently of any product evaluation, or
- As the first step of the evaluation of a ST that claims conformity with the PP-Configuration. Otherwise the conformance claim is meaningless and the ST evaluation would fail in this aspect.

13.7.3 Results of a ST/TOE evaluation

13.7.3.1 General

The results of a ST evaluation shall include a “Conformance Claim” as defined in 12.2..

A successful TOE evaluation requires a successful ST evaluation. The result of the TOE evaluation process is either:

- A statement that all SARs have been met, and that therefore there is the specified level of assurance that the TOE meets the SFRs as stated in the ST;
- A statement that not all SARs have been met and that therefore there is not the specified level of assurance that the TOE meets the SFRs as stated in the ST.

NOTE In some cases the evaluation results are subsequently used in a certification process, but this certification process is outside the scope of ISO/IEC 15408.

If the TOE evaluation has resulted in a pass statement, the underlying product can be eligible for inclusion in a catalogue of successfully evaluated products.

13.7.3.2 Use of ST/TOE evaluation results

Once a ST and a TOE have been evaluated, asset owners can have the assurance, as defined in the ST, that the TOE, together with the operational environment, counters the stated threats. The evaluation results may be used by the asset owner as part of a risk-acceptance decision related to exposing the assets to the threats.

However, risk owners should carefully check whether:

a) the SPD in the ST matches their own security problem;

b) their operational environments conform (or can be made to conform) to the security objectives for the operational environment described in the ST;

c) any guidance documents provided by the developer in the context of the TOE evaluation are followed during the installation, configuration, and operation of the TOE.

If any of these conditions do not hold, the assurance may not hold true and the evaluation results should not be relied upon in a risk-acceptance decision.

Additionally, once an evaluated TOE is in operation, it is probable that previously unknown errors or vulnerabilities in the TOE will be identified. In that case, the developer may correct the TOE (to address the vulnerabilities) or change the ST in a way that excludes the newly identified vulnerabilities from the scope of the evaluation. In either case, the old evaluation results may no longer be valid

NOTE If assurance is to be maintained, re-evaluation is needed. ISO/IEC 15408 (all parts) may be used for this re-evaluation, but detailed procedures for re-evaluation are outside the scope of this document.

13.8 Multi-assurance evaluation

For a multi-assurance PP-Configuration, the ACE requirements, given in ISO/IEC 15408-3, ensure that the combination of different sets of SARs does not undermine the expected security of the underlying assets, as defined in the SPDs of the PPs and PP-Modules that compose the PP-Configuration.

For a multi-assurance ST, the ASE requirements, given in ISO/IEC 15408-3, ensure that the ST is conformant to a multi-assurance PP-Configuration which satisfies ACE assurance requirements. This means that the organization of the TSF in sub-TSFs and the sets of SARs that apply to them are consistent with the PP-Configuration. For each sub-TSF this means that the multi-assurance ST requires a set of SARs that is either as defined in the PP-Configuration for the corresponding component (PP or PP-Module) or an augmentation.

The general model of the standard, which holds in a multi-assurance evaluation, requires that the evaluator evaluates the TSF in order to ensure the security of the TOE. In the context of multi-assurance, the evaluator still considers the impact on the entire TOE, when evaluating each of the sub-TSFs.

In practice, a multi-assurance evaluation can be seen as several evaluations on the same TOE, according to different PPs. The multi-assurance approach adds the consistency checks that are required to ensure that these evaluations can be performed together. This means in particular that the sets of SARs associated with a sub-TSF does not impact on the other sub-TSFs. Therefore, the evidences required by the SARs of one sub-TSF cannot be negatively impacted by the SARs that have been chosen for the other sub-TSFs.

EXAMPLE Let us imagine that a PP-Configuration selects AVA_VAN.3 for one sub-TSF. ADV_TDS.3 will then be required by dependency. The evaluation of ADV_TDS.3 for this sub-TSF will, by definition, consider all the subsystems of the TOE, regardless of the ADV_TDS levels of the other sub-TSFs defined in the TOE.

The multi-assurance evaluation of a TOE which complies with a multi-assurance ST consists in evaluating the entire TOE against the global set of SARs and evaluating each of the sub-TSFs against the corresponding sets of SARs, as defined in the ST. The order of the evaluation activities is left to the evaluator. The most suitable order depends on factors such as the actual structure of the TSF in terms of the sub-TSFs and the difference between the global set of SARs and the sets of SARs that apply to the sub-TSFs.

The limitation of multi-assurance evaluation to TOEs (and ST s) that comply with one multi-assurance PP-Configuration and the definition of the multi-assurance consistency rules in ACE allow to limit the impact on the other assurance classes. Performing a multi-assurance evaluation consists in applying a uniform interpretation of all the assurance classes, as defined in ISO/IEC 18405: in the context of a multi-assurance evaluation, whenever a SAR mentions the "TOE" it refers to the entire TOE. Whenever a SAR mentions the “TSF”, it refers to the sub-TSF to which the SAR applies.

NOTE A multi-assurance ST reflects the TSF organization in sub-TSFs defined in the PP-Configuration to which the ST claims conformance. This TSF organization does not describe the organization of the TOE’s implementation in subsystems and modules, but rather associates a given set of security functionalities (sub-TSF) with specific assurance requirements. It may happen that sub-TSFs are implemented by different sets of subsystems/modules, but there may also be some degree of overlap: a subsystem or module may implement functionalities belonging to two different sub-TSFs. This means that the two sets of SARs apply to the common subsystem or module (i.e. the union of the sets of SARs applies). In both cases, for each sub-TSF, all of the other sub-TSFs belong to the TOE and the corresponding subsystems/modules must be evaluated through the prism of the requirements of the sub-TSF.

14 Composition of assurance

14.1 General

IT Products are almost always composed from several components, whereby some of them may be evaluated and some are not. Independent product components are often evaluated separately, and the question of composing the security assurance of the single components to determine the security assurance of the entire product arises.

EXAMPLE

Software is composed with evaluated hardware to create an IT product.

Composition of assurance is dependent upon:

- the type of composition;
- the security function policies, and organizational security policies that the component evaluation was based on;
- the claimed security assurance, for example the assurance level;
- the overall security policies for the entire product.

Concepts of composition models are described in subclause 14.2. Evaluation methods by which security assurance in such composition models can be provided are given in subclause 14.3. Considerations about the re-use of evaluation results related to individual product components in the composition approach are addressed in subclause 14.4. Subclause 14.5 addresses the relationship between composite and multi-assurance evaluation approaches.

14.2 Composition models

14.2.1 Layered composition model

In this type of composition, one component is built on top of another component, as pictured in Figure 10.

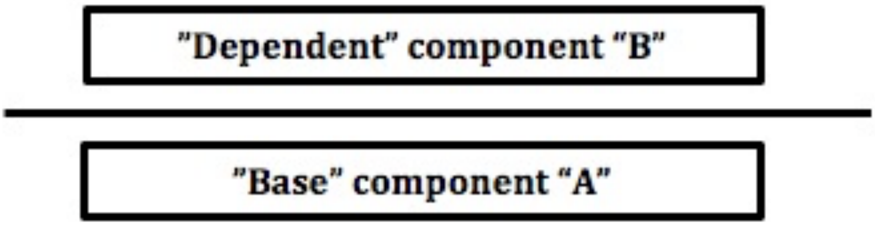


Figure 10 — Layered composition model

The following assumptions are made in regard to the layered composition model:

- The base component is independent from the dependent component;
- The base component is not modified by the dependent component;
- The dependent component uses the functionality of the base component and not vice versa.

Those performing such a composition should consider that:

- the dependent component can depend on other functionality than the security functionality in the scope of the evaluation of the base component.

EXAMPLE

Two examples hereafter can be used to clarify the layered composition model described in Figure 10. The first and main example comes from the smartcard domain, where an evaluation technique has been defined for the layered composition model. In this context, a smartcard is built up with a combination of two parts:

- A hardware integrated circuit (IC) part (as a base component) and
- A software part on top of it (as a dependent component).

The software part can depend on functionality that does not belong to the evaluated security functionality of the underlying hardware. However, in general almost all instructions of the hardware are part of the hardware's security functionality and are used to implement the security functionality. of the software part.

The software part of the smartcard may be layered itself, consisting of an

- 'Operating System' layer with possibly integrated applicative functionality (as a base component) and an
- 'Application' layer on top of it that may contain different applications (as a dependent component).

All these parts can be developed by different actors with specific objectives.

In a second example, applications running on a personal computer follow the same principle, with an operating system (OS) acting as a base component and the application layer as a dependent component: the application uses Identification and Authentication provided by the OS, builds its own objects on top of the OS file system, builds its own application structure on top of the OS address space management and separation, and needs to enforce specific properties (e. g. fault tolerance, information flow control). If the OS has already been evaluated then the security functionality of the application layer can be broken down to the evaluated security functionality of the base component. Where this is not possible, the dependent component implements the security functionality by itself. Furthermore, the dependent component can depend on functionality that does not belong to the evaluated security functionality of the underlying base component.

14.2.2 Network or bi-directional composition model

In this type of composition, a component uses the specific functionality of another component communicating via some communication channel, as pictured in Figure 11.

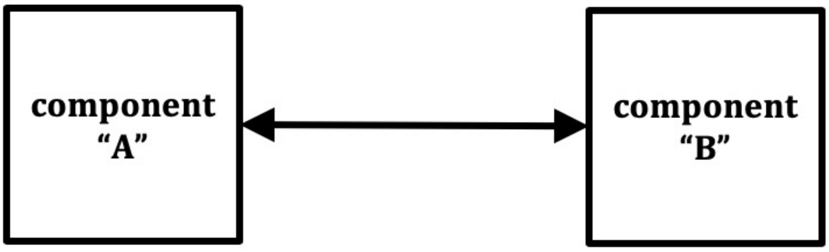


Figure 11 — Network or bi-directional composition model

The following assumptions are made in regard to the network or bi-directional composition model:

- The security interdependencies are clearly described;
- Both products are separated such that there is no other channel or influence than the defined one;
- Both products implement the functionality required to protect the communication channel.

EXAMPLE 1

An application (component "A") using the functionality of an external LDAP server (component "B").

Those performing such a composition should consider that:

- Security functionality might not fit together;

  EXAMPLE 2

Access control may be based on different objects.

- Assumptions made on a component might not be valid;

  EXAMPLE 3

  Assumption on the protection of critical data transferred to another component.

- Security functionality can have unwanted side effects.

  EXAMPLE 4

  A covert channel leaking cryptographic keys.

If these kinds of issues are identified then they should be clearly documented along with the determination of appropriate mitigating controls.

14.2.3 Embedded composition model

In this type of composition, a component is used as part of a larger component or product, as pictured in Figure 12.

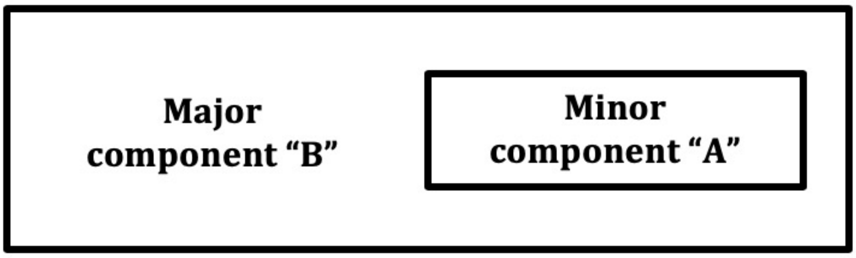


Figure 12 — Embedded composition model

The following assumptions are made in regard to the embedded composition model:

- There is usually no separation between the components;
- Each part can influence the other via channels and interfaces other than the intended ones.

EXAMPLE

A library or subsystem providing specific security functions as part of a larger product.

Those performing such a composition should consider that due to the lack of separation, components may:

- bypass the security functionality of the other components;
- modify the security functionality and security policy of other components and of the whole product;
- introduce a number of critical side effects.

NOTE If separation is specified, ADV_ARC given in ISO/IEC 15408-3 describes the criteria for evaluation.

14.3 Evaluation techniques for providing assurance in composition models

14.3.1 General

To achieve reliable and repeatable evaluation results for the evaluation of IT products (TOEs) that make use of the composition models described in 14.2, a corresponding suitably defined evaluation method is needed.

Subclauses 14.3.2 and 14.3.3 address evaluation techniques for the layered composition model. 14.3.2 describes how the ACO class defined in ISO/IEC 15408-3 may be used for composed TOEs, and in 14.3.3 an evaluation technique for composite products is provided.

14.3.2 ACO class for composed TOEs

The ACO class specified in ISO/IEC 15408-3 addresses a TOE composed of two TOEs using a layered composition model as described in 14.2, both of which have been separately evaluated. These component TOEs can be described as a base TOE and a dependent TOE, as shown in Figure 13. In such case, the ACO class is used for evaluating the composed TOE.

An evaluation of such composed TOE consists of evaluating the interaction between both TOEs, whereby reuse of the evaluation results from both the base TOE and the dependent TOE takes place.

ISO/IEC 15408-5 provides a pre-defined Composed Assurance Packages (CAP) that may be used for determining the composed TOE's assurance level.

The ACO class is applicable up to 'Enhanced-basic' assurance level.

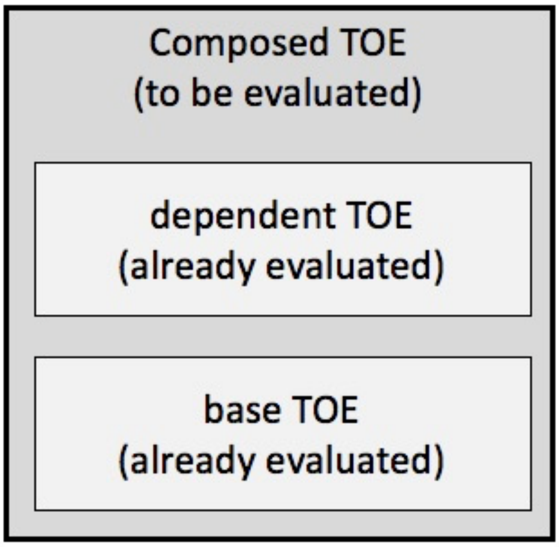


Figure 13 — Composed TOE evaluated using the ACO class

14.3.3 Composite evaluation for composite products

14.3.3.1 General

The composite evaluation technique addresses the layered composition model for composite products as described in 14.2 and is devised to meet the following objectives:

- independently perform the evaluation of a base component to address several dependent components and customers;
- create one or several dependent component(s) to use with an evaluated base component;
- install one dependent component onto an evaluated base component to reduce the evaluation effort keeping a high level of confidence.

The composite evaluation technique describes a way to perform transfer of knowledge and reuse of evidence, in order to meet these objectives.

The COMP related assurance families specified in ISO/IEC 15408-3 for the ADV, ALC, ASE, ATE and AVA classes provide evaluation criteria pertinent to composite products using this layered model.

14.3.3.2 Objectives

This method for composition of assurance applies to layered products that comprise one independently evaluated base component and one dependent component.

NOTE A dependent component may consist of one or more dependent components. For simplification, they are considered as 'one dependent component' in the following.

The composite product is made of the integration of the already evaluated base component (including its base TOE) and the dependent component. Hereby, the base TOE is part of the composite TOE. In the composite evaluation approach, reuse of the evaluation results already obtained for the base TOE is done, and the evaluation of the dependent component is performed within the evaluation of the composite product, whereby in particular focus is laid on the evaluation of the relationship between the base TOE and the dependent component. Therefore, an assurance level is claimed for and applies to the composite product as a whole and not to the dependent component only.

The composite product, with its base component (including the base TOE) and dependent component, is intended to be efficiently evaluated. The specific composite evaluation technique is set up with the objective to optimize the evaluation of such composite product.

Unlike ACO-based evaluation, this allows a direct comparison with similar products that are evaluated at once without using composition techniques. Moreover, there is no limitation in the assurance level, i.e. the composite product can claim any predefined EAL or well-defined assurance package, including resistance up to 'High attack potential' as defined in ISO/IEC 15408-3 AVA_VAN.5, whereas ACO is limited by CAP requirements up to 'Enhanced-basic' attack potential. The aim is not to define an additional assurance class, but to define additional assurance requirements for a composite product evaluation.

EXAMPLE

Examples of smartcard devices requiring high-level assurance include payment and digital signature applications.

14.3.3.3 Design of composite product and composite TOE

The composite product is composed of one base component (including its base TOE) and one dependent component whereby in view of evaluation aspects the following rules and constraints apply for the composite product and its composite TOE part:

- The base component builds the underlying independent layer of the composite product and contains the base TOE. The base component with its base TOE shall have already been evaluated;
- The dependent component builds a supplementary layer of the composite product that is dependent on the base component and that shall be evaluated in the framework of the composite evaluation;
- The composite TOE is part of the composite product and covers the entire dependent component, and the base TOE, more detailed a superset of the base TOE functionalities required for the correct and secure execution of the composite product;

  NOTE A composite TOE may contain parts that are independent from the base component or base TOE respectively. For simplification, such parts are considered as belonging to the dependent component.
- The dependent component cannot rely on base component functionalities that are in the base component, but lie outside the base TOE (that is, functionalities in the non-TOE part of the base component);
- The non-TOE part of the composite product can use base component functionalities, in particular base TOE functionalities. As usual, the composite product evaluation needs to determine that this non-TOE part of the composite product is non-interfering with the dependent component – neither directly nor through the usage of the base component functionalities.
- Non-TOE parts of the composite product, in particular non-TOE parts of the evaluated base component (that is, parts in the base component lying outside the base TOE), are considered part of the operational environment of the composite TOE.

NOTE 1: Composite evaluation can be applied independent of the evaluation assurance level (EAL) for the

composite product aimed. Where some evaluation activities are not applicable due to the EAL chosen, they are also not expected to be applied.

NOTE 2: This standard only addresses cases where the level of assurance of the base component is equivalent or higher compared to the composite evaluation level.

NOTE 3: In the case where both base component and dependent component have already been evaluated using ISO/IEC 15408, a partial evaluation work may be performed regarding the results already obtained from previous dependent component evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

Figure 14 illustrates the general design and layering of a composite product and composite TOE in the framework of the composite evaluation approach.

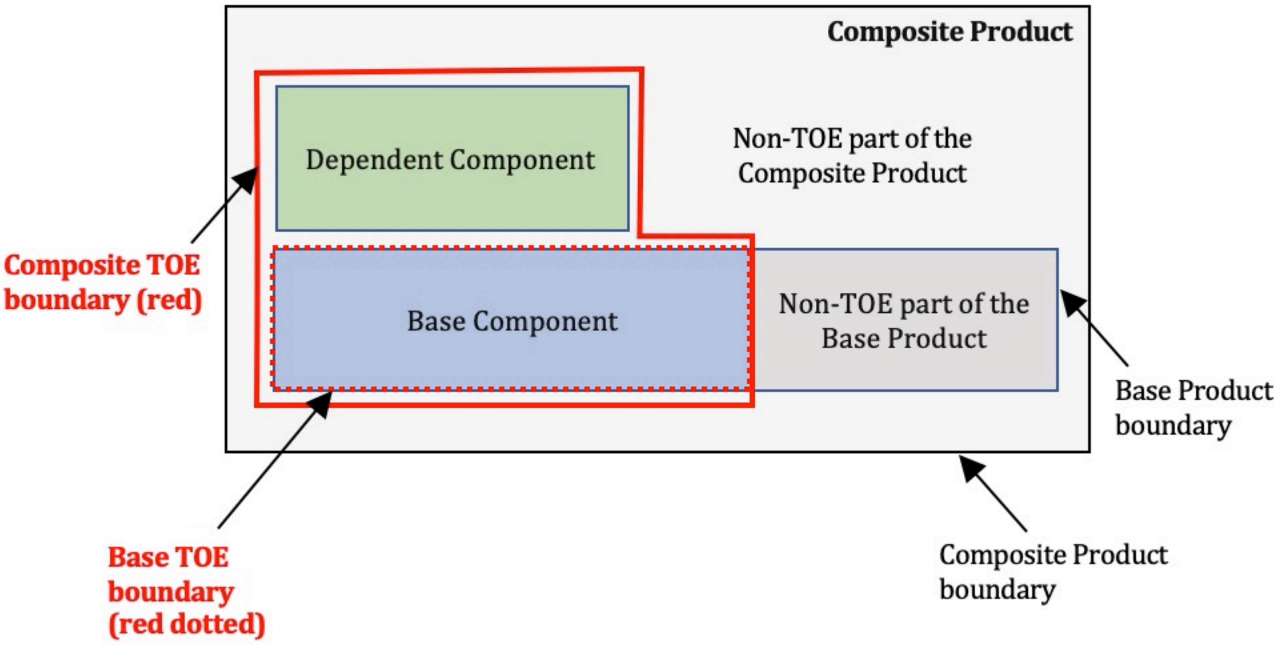

Composite Product
Dependent Component
Non-TOE part of the Composite Product
Composite TOE boundary (red)
Base Component
Non-TOE part of the Base Product
Base Product boundary
Base TOE boundary (red dotted)
Composite Product boundary

Figure 14 — Composite evaluation

Several composition steps can follow each other. In other terms, the base component can itself be a composite product consisting of an own already evaluated base component and a dependent component.

14.3.3.4 Roles

The base component and the composite product, more detailed the base TOE and the composite TOE, are both undergoing an evaluation. Therefore, both of them have a sponsor, a developer, an evaluator, and an evaluation authority.

For the composite evaluation model addressing the evaluation of the composite product, a preceding finalized evaluation of the base component with its base TOE is expected. The composite evaluation performs the evaluation of the composite product by re-using the evaluation results of the already evaluated base component. Hence, the evaluation of the composite product focuses on the evaluation of the dependent component including its relationship to the base component and hereby takes the underlying base TOE with its related evaluation results into account.

In practice, there is no composite product developer since the composite product results from the integration of the dependent component and the base component. Instead, the relevant developer-related roles here are

- the dependent component developer responsible for implementing the dependent component (and further non-TOE parts of the composite product, if applicable),
- the base component developer responsible for implementing the base component, and
- the composite product integrator responsible for the integration of the base component and the dependent component.

In order to address this role model, the composite evaluation approach and technique defines additional evaluation activities for the above mentioned dependent component developer, the base component developer, and the composite product integrator.

NOTE 1: As already mentioned, the dependent component may have undergone a separate evaluation, but the evaluator and evaluation authority of this previous evaluation are not considered here. If the base component and the dependent component were evaluated separately, each of them would have a sponsor, a developer, an evaluator, and an evaluation authority.

NOTE 2 As in the general cases, some actors involved may be the same. The composite evaluation context also leads to specific cases of actors having several roles. Each evaluation will associate particular organizations or persons to these generic roles.

EXAMPLE 1:

- The base component developer may also be the base component sponsor;
- The base component evaluation authority may also be the composite product evaluation authority.

NOTE 3 The composite product integrator is a different role than the developer. While this integrator may, in some cases, also be one of the developers defined previously, this is not always the case.

The following example illustrates the role of the composite product integrator:

EXAMPLE 2:

- Native smartcards: The underlying base component is an integrated circuit and the base component developer is the integrated circuit (chip) manufacturer; the dependent component is a card operating system and its application(s) and the dependent component developer is the developer of the smartcard operating system and the application(s). In this case, the role of the composite product integrator is played by:
  - the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by
  - the card manufacturer usually loading some parts of the operating system and the applications into NV-Memories (EEPROM and/or Flash) of the chip.
- Java Card technology-enabled devices: The underlying base component is the Java Card runtime Environment (Java Card RE) on chip and the base component developer is the card manufacturer/issuer; the dependent component is the Java Card applet, which can be developed by the applet developer as dependent component developer. In this case, another role is the composite product integrator who can be played by the domain/application service provider or by a trust center loading the applet and often personalizing the card electronically.

14.3.3.5 Actions elements and required information

To allow the evaluation of a composite product, the composite evaluation technique identifies two main sets of issues, leading to the following rules:

- The composite product might be insecure due to gaps in the definition, integration or test of the base component and dependent component security mechanisms. In particular, the following properties are to be enforced:
  - The assets to be protected are the final composite product assets defined in a dedicated composite product ST;
  - The security mechanisms involved in the protection of these assets are those provided by the base component and by the dependent component;
  - Some of the security mechanisms and security services provided by the base component may require configuration, programming, or activation by the dependent component;
  - Evaluation is performed and validated on the final composite product.

To this effect, the composite evaluation technique defines specific action elements to be performed by the actors involved in the evaluation of the base component, as well as the evaluation of the dependent component and the composite product:

— The aforementioned action elements may be impossible to perform due to a lack of information sharing between actors. To avoid this, the composite evaluation technique explicitly defines which information is required for each action element.

Table 2 and Table 3 define which SARs shall be selected in the composite product ST, and which information is required to allow a composite evaluation.

Table 2 — Information to be provided to the dependent component developer

SAR defining the action elements	**Information required**	**Originator of the information**
Consistency of composite product ST (ASE_COMP)	ST of the base component. Information related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer
Composite design compliance (ADV_COMP)	Information (usually in the form of a guidance or user's manual) related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer

Table 3 — Information to be provided to the composite product evaluator and composite product evaluation authority

SAR defining the action elements	**Information required**	**Originator of the information**
Consistency of composite product ST (ASE_COMP)	ST of the base component. Information related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer
	ST of the composite product.	Dependent component developer
Integration of components and consistency check of delivery procedures (ALC_COMP)	Organizational evidence of version correctness, on the basis of configuration lists containing unambiguous version information of the base component and the dependent component having been integrated into the final composite product.	Composite product integrator
	Organizational evidence that components (dependent component or base component) transmitted from an actor to another is securely received, accepted and parameterized.	Composite product integrator Base component developer Dependent component developer
Composite design compliance (ADV_COMP)	Base component-related integration recommendations, typically including the user guidance.	Base component developer
	Evidence that the composite product meets the base component-related integration recommendations.	Composite product integrator
	Evaluation evidence for the base component.	Base component evaluation authority
Composite functional testing (ATE_COMP)	Composite product samples suitable for testing.	Composite product integrator
Composite vulnerability assessment	Evidence allowing the composite product evaluator and the respective evaluation authority to understand the considered attack paths, the performed tests, the effectiveness of countermeasures implemented by the	Base component evaluator

SAR defining the action elements	Information required	Originator of the information
(AVA_COMP)	base component, and explanation related to residual vulnerability linked to integration recommendations included in the user guidance.	
	Evaluation evidence for the base component.	Base component evaluation authority

NOTE 1: In the case of composition, the term 'developer' needs further clarification in order to distinguish the actors. Here, the base component developer, the dependent component developer and the composite product integrator can be different entities. Similarly, for the terms 'evaluator' and 'evaluation authority (evaluation scheme)' further distinguishing of the different entities involved needs to be made.

NOTE 2: The composite product evaluator may not need all the detailed results of the base component evaluations. See 14.4 for more detail on re-using evaluation results.

NOTE 3: In the case where both base component and dependent component have already been evaluated, a reduced set of evaluation activities may be performed considering the evaluation results already obtained from the previous dependent component evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

EXAMPLE

Smartcard

The smartcard architecture is composed of a hardware platform and a software application on top of the platform. In this case, the platform is the base component, and the application is the dependent component. In a composite product evaluation, the platform is already evaluated, the application is evaluated as part of the composite evaluation and the results of the platform evaluation are re-used.

The hardware platform provides functionality supporting the protection of the composite product's assets, but the composite product behaviour depends on the software application having to use, configure, and activate the security functionality.

Therefore, the hardware platform evaluation results must provide specific security recommendations and conditions for the software application implementation. The composite product evaluation includes examination that the combination of both components does not lead to any exploitable vulnerability.

A composite evaluation method and associated evaluation activities is developed that includes precise work units with clear statements on the information required from the platform developer and provides an agreed 'framework' for information transfer from the platform evaluator to the composite product evaluator.

The information required is already available from the platform evaluation tasks and no additional work is required from the platform developer.

There are no further requirements for the development class ADV.

The user guidance (AGD) of the platform is considered early in the development of the composite product and provides all of the interfaces on which information is needed.

The development and the evaluation of the composite product rely on the proper implementation of the evaluated interfaces of the platform.

The proper use of all relevant interfaces between the platform and the application is in the scope of the composite product evaluation.

Test (ATE) and vulnerability assessment (AVA) are performed on the composite product taking advantage of the available platform evaluation results.

14.4 Requirements for evaluations using composition techniques

14.4.1.1 Re-use of evaluation results

When composing components into an IT product, it is possible that single components of the product have already been evaluated and that therefore already existing evaluation results for such components could be re-used. However, further evaluation of the IT product (TOE) shall be performed to confirm the security assurance of the entire IT product.

The re-use of evaluation results and evidence related to such components of the IT product (TOE) require their availability for the evaluation of the entire IT product (TOE).

Subclauses 14.3.2 and 14.3.3 address evaluation techniques for the layered composition model. 14.3.2 describes how the ACO class defined in ISO/IEC 15408-3 may be used for composed TOEs, and in 14.3.3 an evaluation technique for composite products is provided.

The re-use of evaluation results and evidence of components of the IT product (TOE) is dependent upon:

- the composition model used for the IT product (TOE);
- the security assurance to be claimed for the entire IT product (TOE), in particular in relationship to its components and their security assurance;
- the security properties claimed for the IT product (TOE) and its components.

EXAMPLE

Separation, Information Flow Control and Fault tolerance are examples of security properties.

14.4.2 Composition evaluation issues

14.4.2.1 Composition rationale

When composing an IT product (TOE) from components using a composition model as described in 14.2 and using composition techniques for its evaluation, a composition rationale shall be provided for the evaluation of the IT product. This includes analysis of at least:

- the composition model used for the IT product (TOE);
- the security assurance to be claimed for the entire TOE, in particular in relationship to its components and their security assurance;
- the interfaces and dependencies of the components and their functionality;
- the composability of the security function policies and organizational security policies of the components;
- the preservation of security properties of the components;
- for the embedded composition model, aspects of correctness.

14.4.2.2 Vulnerability analysis

The IT product composed from components using a composition model as described in 14.2 and using composition techniques for its evaluation shall have a vulnerability analysis, in accordance with the AVA class, performed on the IT product with its components at a level commensurate with the required security assurance for the IT product.

The vulnerability analysis shall be designed in consideration of the analysis of the IT product and its composition of components.

14.4.2.3 Testing

The IT product composed from components using a composition model as described in 14.2 and using composition techniques for its evaluation shall undergo additional testing, using the ATE and IND classes given in ISO/IEC 15408-3. It may be possible to re-use the testing evaluation results from the components, but additional tests for the entire IT product (TOE) shall be designed and performed.

The testing shall be designed in consideration of the analysis of the IT product and its composition of components.

14.4.2.4 Use of the ACO class for composed TOEs

ISO/IEC 15408-3 describes the ACO class which provides security assurance components that may be used in support of the evaluation of composed TOEs.

ISO/IEC 15408-5 provides a family of pre-defined assurance packages for composed TOEs (composed assurance packages (CAP)) which balance the level of assurance obtained with the cost and feasibility of acquiring such assurance for composed TOEs.

NOTE The composed assurance packages are designed to provide assurance that the composition was performed to a specified rigour, and do not imply any evaluation assurance level for the composed IT product.

14.4.2.5 Use of the composite evaluation technique for composite products

ISO/IEC 15408-3 of this standard describes the COMP families in different assurance classes, which provide security assurance components that may be used in support of the evaluation of composite products.

NOTE The COMP families are designed to provide assurance that the composition was performed correctly, without impact on the evaluation assurance level for the composite product.

14.5 Evaluation by composition and multi-assurance

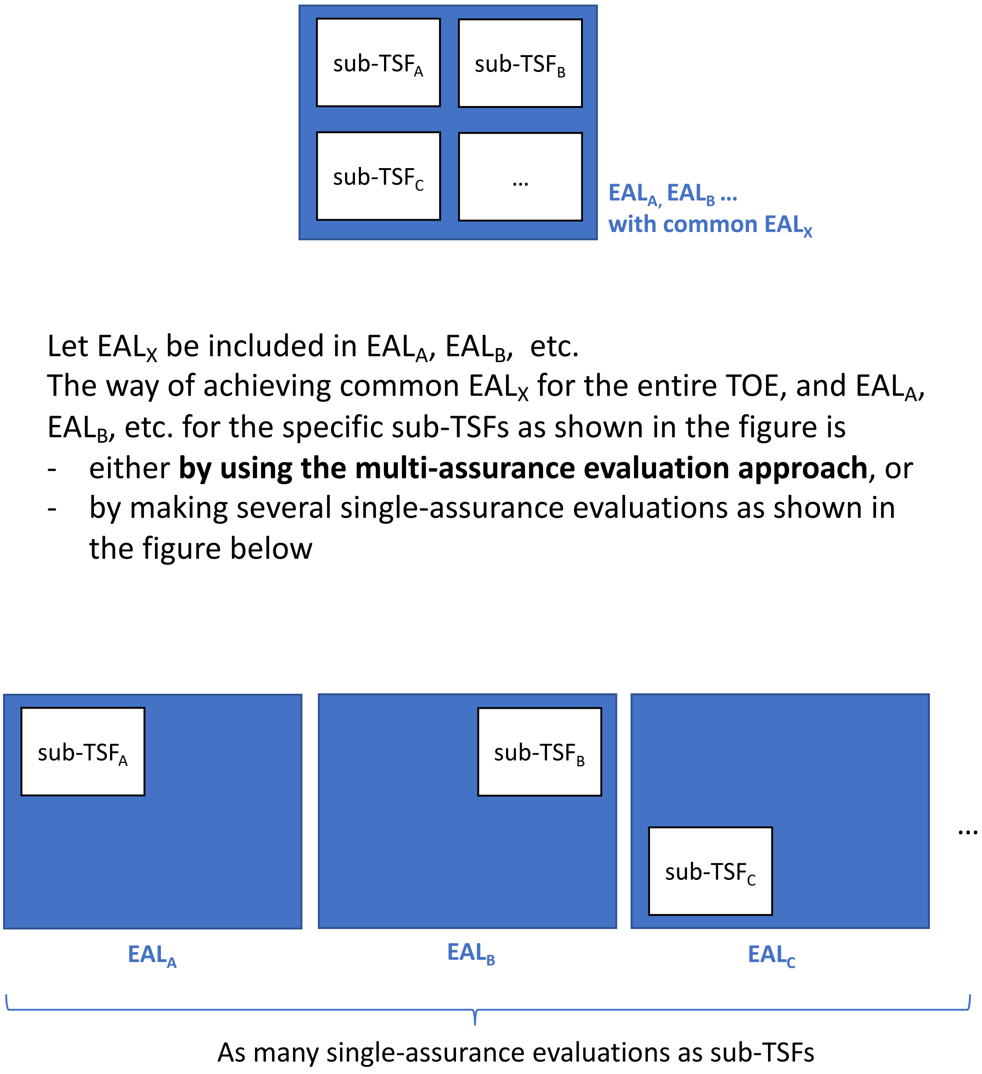
The notions of composition and multi-assurance are aimed at solving different problems. In a nutshell, composed and composite evaluations refer to evaluation processes which are particularly suitable for multi-actor TOEs and allow reusing previous evaluation results, while multi-assurance refers to a 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 may involve multiple parties, each of which take care of the evaluation of the security functionality they develop. ISO/IEC 15408 standardizes two approaches for the reuse of evaluation results in an evaluation process:
  - Composed evaluation allows to obtain a global assurance level (CAP) for a TOE from the individual assurance levels of its interacting sub-TOEs.
  - 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. Before the introduction of multi-assurance, such needs would have forced a sponsor to undergo several evaluations of the same TOE for different STs. By 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 in several interacting sub-TOEs, while composite evaluation applies to a TOE where a dependent layer relies on a base layer.

In practice, multi-assurance and evaluation by composition are not incompatible, and both approaches can be used together in an evaluation.

The following figures show the relationship between composite, single-assurance and multi-assurance evaluation approaches. The notation convention is the following: the TOE is blue, the TSF is white, and grey indicates reuse.

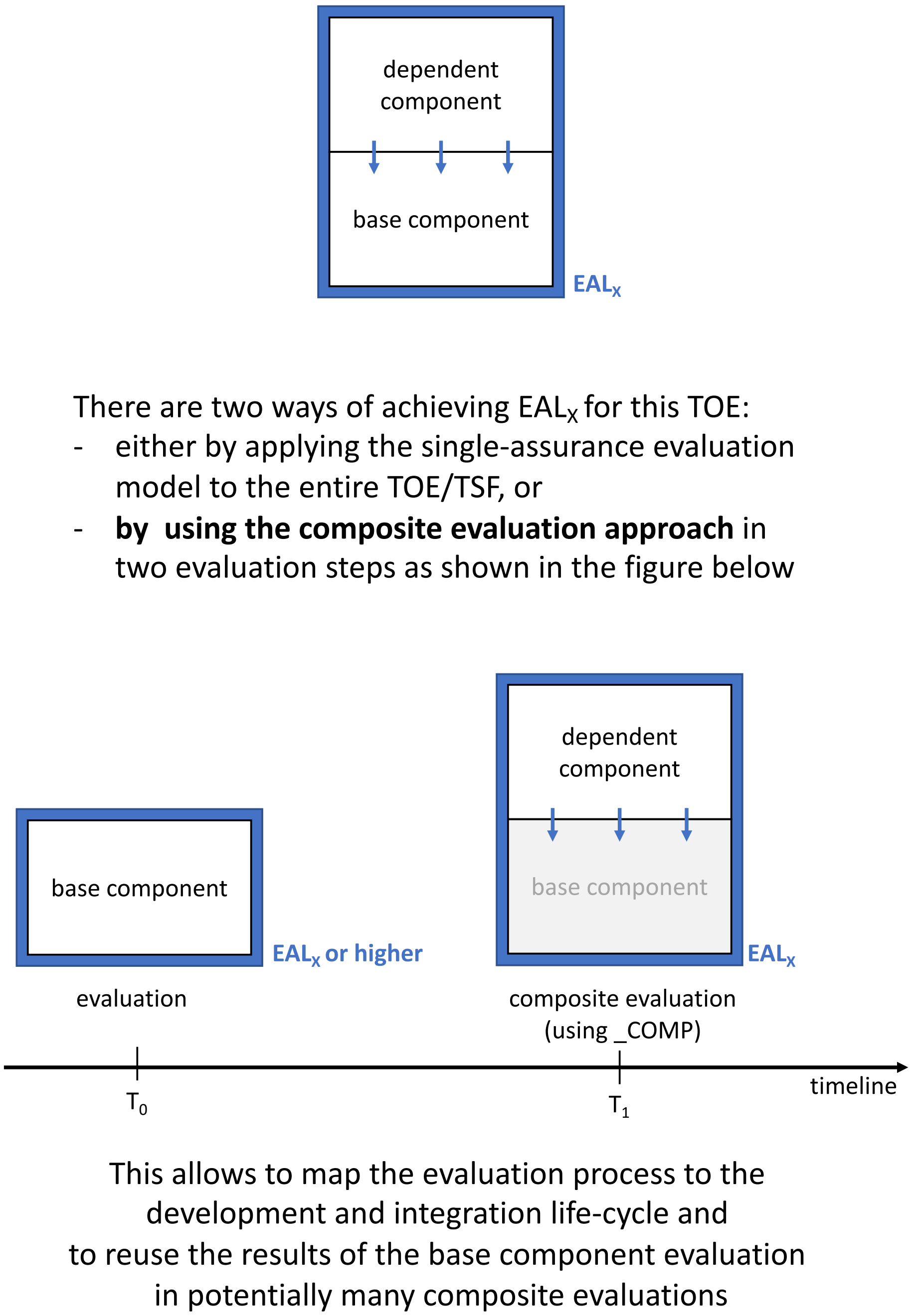


Let EAL$_X$ be included in EAL$_A$, EAL$_B$, etc.
The way of achieving common EAL$_X$ for the entire TOE, and EAL$_A$, EAL$_B$, etc. for the specific sub-TSFs as shown in the figure is

- either **by using the multi-assurance evaluation approach**, or
- by making several single-assurance evaluations as shown in the figure below

The converse does not hold. That is, any set of single-assurance evaluations of a TOE is not equivalent to a multi-assurance evaluation. This happens when two of the EALs are disjoint. Unlike single-assurance, multi-assurance evaluation allows to determine by construction the global assurance level of the TOE.

Figure 15 — Multi-assurance vs single-assurance evaluation

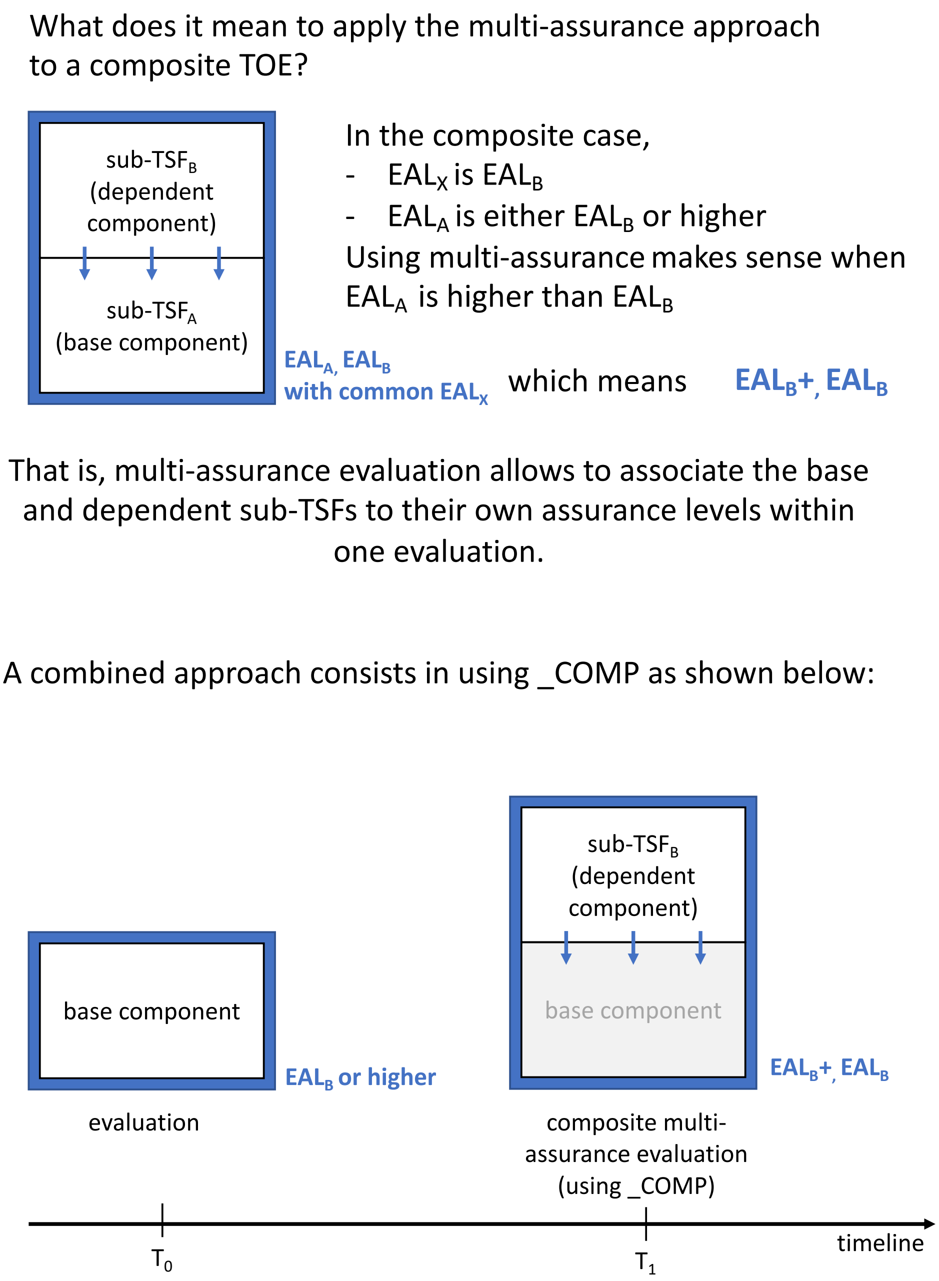


There are two ways of achieving EAL_X for this TOE:

- either by applying the single-assurance evaluation model to the entire TOE/TSF, or
- **by using the composite evaluation approach** in two evaluation steps as shown in the figure below

This allows to map the evaluation process to the development and integration life-cycle and to reuse the results of the base component evaluation in potentially many composite evaluations

Figure 16 — Composite evaluation vs single-assurance evaluation



What does it mean to apply the multi-assurance approach to a composite TOE?

In the composite case,

- EAL_X is EAL_B
- EAL_A is either EAL_B or higher

Using multi-assurance makes sense when EAL_A is higher than EAL_B

That is, multi-assurance evaluation allows to associate the base and dependent sub-TSFs to their own assurance levels within one evaluation.

A combined approach consists in using _COMP as shown below:

sub-TSF_B (dependent component)
sub-TSF_A (base component)
$EAL_{A,}$ EAL_B with common EAL_X
which means
EAL_B+, EAL_B
base component
EAL_B or higher
evaluation
sub-TSF_B (dependent component)
base component
EAL_B+, EAL_B
composite multi-assurance evaluation (using _COMP)
T_0
T_1
timeline

Figure 17 — Multi-assurance evaluation of a composite TOE

Annex A
(Normative)
Specification of Packages

A.1 Goal and structure of this Annex

The goal of this annex is to give further information about the specification of packages.

NOTE ISO/IEC 15408-3 does not define evaluation criteria for packages since packages are not separately evaluated. Evaluation of packages is implicit once a package is incorporated into a PP, PP-Module or ST.

A.2 Package families

A.2.1 General

Figure A.1 shows the structure of a package family. Each part is discussed in the following subclauses.

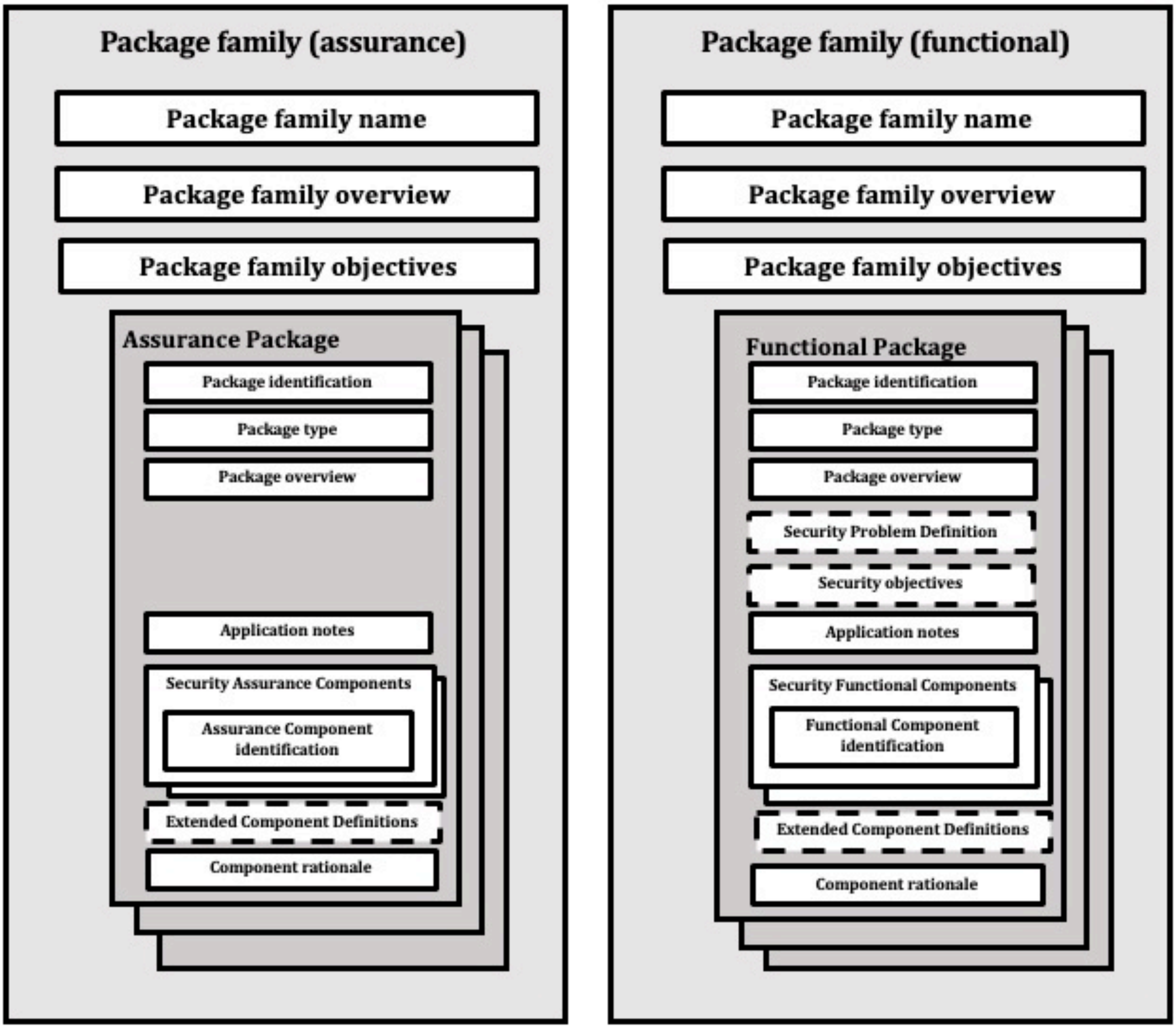

Package family (assurance)
Package family name
Package family overview
Package family objectives
Assurance Package
Package identification
Package type
Package overview
Application notes
Security Assurance Components
Assurance Component identification
Extended Component Definitions
Component rationale
Package family (functional)
Package family name
Package family overview
Package family objectives
Functional Package
Package identification
Package type
Package overview
Security Problem Definition
Security objectives
Application notes
Security Functional Components
Functional Component identification
Extended Component Definitions
Component rationale

Figure A.1 — The structure of a package family with assurance or functional packages

A.2.2 Package family name

Packages with related objectives are presented as a family of packages. In this case, the package family name is mandatory and the package family sponsor endeavors to allocate a unique name.

A.2.3 Package family overview

Packages presented as a family of packages contain a section giving an overview of the family, describing the family at a high-level.

A.2.4 Package family objectives

The objectives section of the package family presents the intent of the family.

A.2.5 Packages

One or more packages, as described below are included in the package family. Packages of SARs and packages of SFRs are not mixed in the same package family.

A.3 Packages

A.3.1 Mandatory contents of a package

A.3.1.1 Package identification

The package identification includes:

a) the name of the package. The name provides a unique descriptive information about the intent of the package;

b) package version information;

c) last updated date;

d) sponsor;

e) reference to the edition of ISO/IEC 15408 (all parts) that is used.

The package may also be given a short name.

EXAMPLE Evaluation Assurance Level 1 is also known as “EAL 1”

NOTE For those packages defined in ISO/IEC 15408-5, items b) – e) are implicit in the edition information of ISO/IEC 15408-5.

A.3.1.2 Package type

A package is identified as one of the following types:

a) Functional package; or

b) Assurance package.

A.3.1.3 Package overview

Packages contain a section giving a high-level overview and the intent of the package.

A.3.1.4 Application notes

Application notes are optional with the following exceptions:

— For functional packages, any additional audit and management requirements relating to the SFRs included in the package shall be specified in the Application notes section.

— Functional packages may have dependencies on other functional packages. Such dependencies shall be documented in the functional package and may also be documented in a PP, PP-Module or ST.

Functional packages may also specify components that have dependencies that are not satisfied by the package, but are expected to be satisfied by another package, PP, PP-Module, or ST that uses the package.

EXAMPLE

A package that contains the specification for a cryptographic protocol (e.g., TLS), where the higher-level SFR components are specified in the package, but the cryptographic primitives are not.

In this case an optional list of the dependent components may be provided in the application notes section of the functional package, and may include further information such as any required selections/assignments for those SFRs.

NOTE Users of packages include authors of PPs, PP-Modules, other packages and STs, integrators, and evaluators.

A.3.1.5 Components (either SFRs or SARs)

The security requirements included in the package are given. This section also provides the rationale for the selection of the requirements.

The security requirements may be selection-based. See 8.2.4.2. Optional security functional requirements (and supporting SPD-elements and objectives, as required) are also allowed to be specified in functional packages.

A.3.1.6 Evaluation Methods/Activities

Evaluation method(s) and/or activities shall either be specified associated with the security requirements in the package itself or in a separate supporting document.

A.3.2 Optional Contents of a Package

A.3.2.1 Security problem definition (Functional Packages)

Assurance packages do not contain this section.

Functional packages may include this section.

This section includes any SPD-elements which describe the security problem addressed by the functional package. SPD-elements associated with optional SFRs may be defined in this section. Application notes shall be used to identify the security objectives (if applicable) and SFRs to which the optional SPD-elements are associated.

A.3.2.2 Security objectives (Functional Packages)

Assurance packages shall not contain this section.

Functional packages may include this section.

In the case of a functional package used for Direct Rationale PPs/STs TOE security objectives shall not be included.

The security objectives section of a functional package presents any additional TOE security objectives or security objectives for the operational environment derived from the SPD. Security objectives for the TOE associated with optional SFRs may be defined in this section, if applicable. Application notes shall be used to identify the SPD-elements and SFRs to which the optional security objectives are associated.

A.3.2.3 Application notes

The inclusion of application notes in a package is optional. See A.3.1.4.

The application notes section may also contain information of particular interest to users of the package. The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention is needed.

A.3.2.4 Extended Components Definition(s)

A package may contain extended components. In this case, packages contain a section giving the extended component definitions.

A.3.2.5 Evaluation methods/activities

Packages may include evaluation methods and/or activities that have been derived from ISO/IEC 18045. Evaluation methods and/or activities that are associated with the package shall be provided in the security requirement section with the relevant security requirement. Application notes, when appropriate, should be associated with the specific requirements in the package. See Clause 9.

Evaluation methods and/or activities may be included in the package associated with the relevant security requirements or provided in a separate document.

Annex B
(Normative)
Specification of Protection Profiles

B.1 Goal and structure of this Annex

The goal of this annex is to summarize the structure and expected content of a PP.

NOTE 1 This annex does not define the requirements for evaluation of PPs. The PP evaluation criteria are found in the APE class given in ISO/IEC 15408-3.

NOTE 2 This annex does not give the requirements for the specification of PP-Configurations and PP-Modules. These are found in Annex C.

This annex consists of the following major parts:

a) *The specification of a PP.* This is summarized in B.2. and includes

— *how to use a PP*

— *how not to use a PP*

a) *What a PP must contain*. This is summarized in B.3 and is described in more detail in B.3.2 to B.3.8. *These* subclauses describe the mandatory contents of the PP, the interrelationships between these contents, and provide examples.

b) *Claiming conformance with standards*. B.4 describes how a PP author can claim that the TOE is to meet a particular standard.

c) *Direct Rationale PPs.* Direct Rationale PPs are PPs in which the threats and organizational security policies in the SPD are mapped directly to the SFRs and possibly to security objectives for the operational environment. They are described in detail in B.5.

B.2 Specification of a PP

B.2.1 Using a PP

B.2.1.1 How to use a PP

A PP is typically a statement of need where a user community, a regulatory entity, or a group of developers define a common set of security needs. A PP gives consumers a means of referring to this set and facilitates future evaluation against these needs.

A PP is therefore typically used as:

— part of a requirement specification for a specific consumer or group of consumers, who will only consider buying a specific type of IT product if it meets the PP;

— part of a regulation from a specific regulatory entity, who will only allow a specific type of IT product to be used if it meets the PP;

— to address a common security problem presented by a variety of consumers, and often defined by a group including several IT product developers, who then produce IT products of this type in order to meet the needs of their common market.

although this does not preclude other uses.

B.2.1.2 How not to use a PP

Two roles, among many, that a PP does not fulfil are:

— a complete specification: A PP is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size, and weight, required voltage etc. should not be part of a PP. This means that in general a PP is a part of a complete specification, but not a complete specification itself.

— a specification of a single product: Unlike a ST, a PP is designed to describe a certain type of IT product, and not a single product. When only a single product is described, it is better to use a ST for this purpose.

B.3 Mandatory Contents of a PP

B.3.1 General

There are two types of PP. Firstly the "regular" PP which is a PP that contains the full contents as described in in B.3.2 to B.3.8. Secondly, in some cases a PP author can write a Direct Rationale PP which has different contents compared to PPs that contain security objectives for the TOE. Direct Rationale PPs, and the reasons and circumstances in which they are used are described in detail in B.5. All other parts of this Annex assume a PP with full contents.

Figure B.1 shows the content for a PP that is given in ISO/IEC 15408-3. Figure B.1 may also be used as a structural outline of the PP, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the PP instead of in the security requirements section. The separate sections of a PP and the contents of those sections are briefly summarized below and explained in much more detail in B.3.2 to B.3.8.

A PP contains:

a) a PP *introduction* containing the PP reference and a narrative description of the TOE type;

b) *conformance claims*, showing

- which edition of ISO/IEC 15408-1 is applicable;
- if ISO/IEC 15408-2 and ISO/IEC 15408-3 have been extended;
- whether the PP claims conformance to any other PPs and/or packages, and if so, to which ones and the type of conformance claimed.
- reference to any evaluation method(s) and/or activities that have been derived from ISO/IEC 18045.

  NOTE 1 Any evaluation methods and/or activities may optionally be included in the PP, or in an associated supporting document.

- In the case of exact conformance, the allowed-with statement appears in this section of the PP.
- The type of conformance demanded of STs and other PPs derived from it;

  NOTE 2 PP-Modules inherit the type of conformance demanded by the PP in its conformance statement when the PP is used by the PP-Module as a base PP;

c) a *security problem definition*, showing threats, OSPs and assumptions;

d) *security objectives*, showing how the solution to the security problem is divided between security objectives for the operational environment and optionally security objectives for the TOE;

e) *extended components definition*, where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) may be defined. These new components are needed to define extended functional and extended assurance requirements;

f) *security requirements*, where a translation of the security objectives for the TOE into a standardized language is provided. This standardized language is in the form of SFRs. Additionally, this section of a PP defines the SARs;

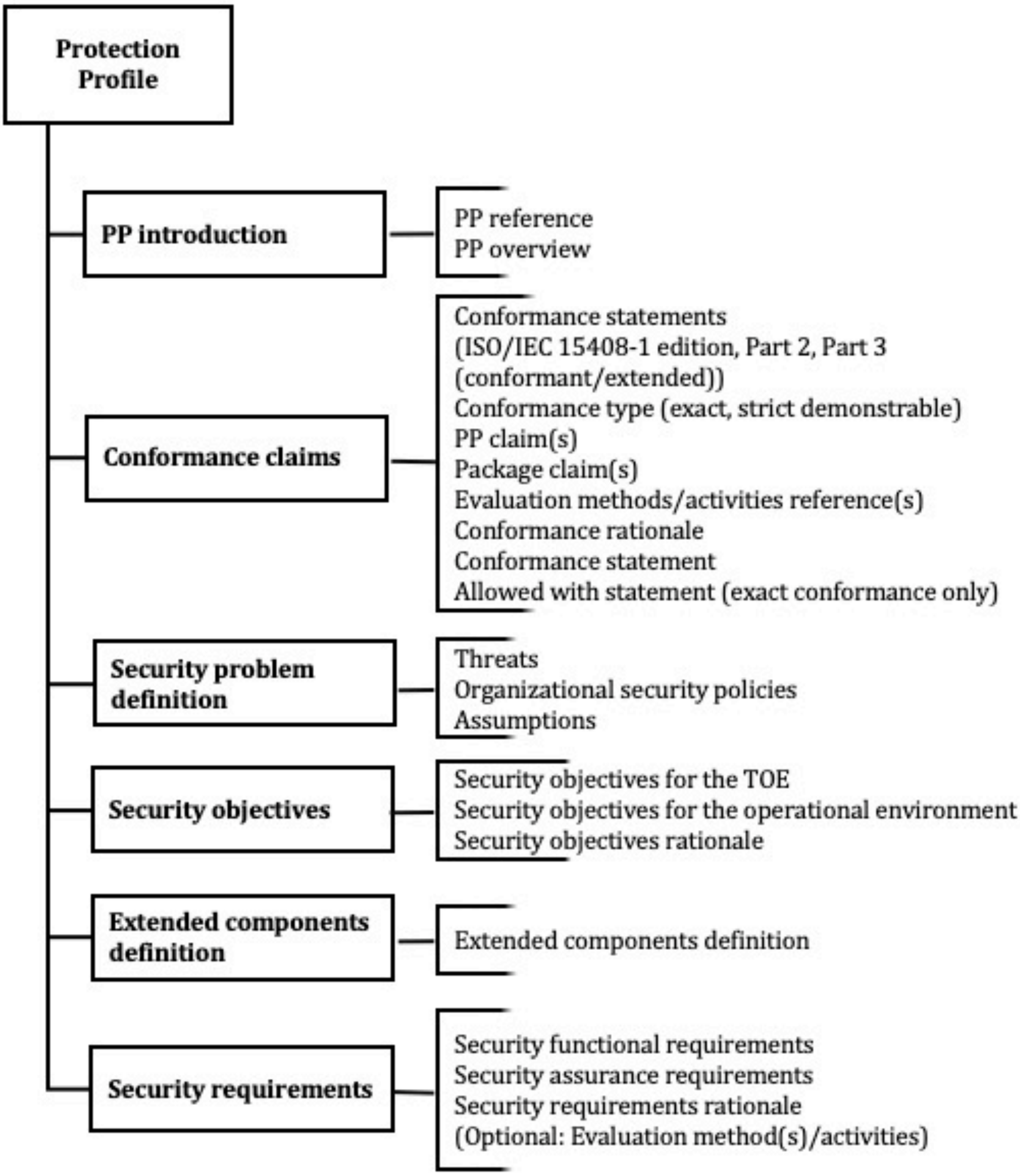

Protection Profile
PP introduction
PP reference
PP overview
Conformance claims
Conformance statements
(ISO/IEC 15408-1 edition, Part 2, Part 3
(conformant/extended))
Conformance type (exact, strict demonstrable)
PP claim(s)
Package claim(s)
Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
Allowed with statement (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)

Figure B.1 — Contents of a Protection Profile

B.3.2 PP introduction (APE_INT)

B.3.2.1 General

The PP introduction describes the TOE in a narrative way on two levels of abstraction:

a) the PP reference, which provides identification material for the PP;

b) the TOE overview, which briefly describes the TOE.

B.3.2.2 PP reference

A PP contains a clear PP reference that identifies that particular PP. A typical PP reference consists of title, version, sponsors, and publication date.

NOTE Here a distinction is made between the sponsor of a PP, i.e. the entity responsible for its development, and the author of a PP which is the entity responsible for its production.

EXAMPLE

An example of a PP reference is "Atlantean Navy CablePhone Encryptor PP, version 2b, Atlantean Navy Procurement Office, April 1, 2020".

The reference should be unique so that it is possible to tell different PPs and different versions of the same PP apart. The PP reference facilitates indexing and referencing the PP and its inclusion in PP catalogues.

B.3.2.3 PP overview

B.3.2.3.1 General

The PP overview is aimed at potential consumers of a TOE type who are looking through catalogues of PPs that can support the specification of their security needs.

The PP overview is also aimed at developers who can use the PP in designing TOEs or in adapting existing products.

The typical length of a PP overview is several paragraphs.

To this end, the PP overview briefly describes the usage of the TOE and its major security features, identifies the TOE type, and identifies any major non-TOE hardware/software/firmware available to the TOE.

B.3.2.3.2 Usage and major security features of a TOE type

The description of the usage and major security features of the TOE type is intended to give a very general idea of what the TOE is capable of, and what it can be used for. This section is written for PP authors, TOE developers, or potential TOE consumers, describing TOE type usage and major security features in terms of business operations, using language that TOE consumers can understand.

EXAMPLE

An example of this is "The Atlantean Navy CablePhone Encryptor is an encryption device that allows confidential communication between ships across the Atlantean Navy CablePhone system. To this end it allows at least 1024 different users and support at least 500 Mbps encryption speed. It allows both bilateral communication between ships and broadcast across the entire network."

B.3.2.3.3 TOE Type

The TOE overview identifies the general type of a TOE addressed by the PP, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server, mobile device, and database, etc. The TOE type definition often includes a characterization of the TOE software and hardware boundaries.

EXAMPLE

This example of TOE type description is drawn from the Security IC Protection Profile: "The Target of Evaluation (TOE) is a security integrated circuit (security IC) which is composed of a processing unit, security components, I/O ports (contact, contactless, or similar interfaces like USB, MMC) and volatile and non-volatile memories (hardware). The TOE may also include IC Developer/Manufacturer proprietary IC Dedicated Software as long as it is delivered by the IC Manufacturer. (…) All other software running on the Security IC is called Security IC Embedded Software and is not part of the TOE."

B.3.2.3.4 Available non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs, notably software TOEs, rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the PP overview is required to identify the non-TOE hardware/software/firmware.

As a PP is not written for a specific product, in many cases only a general idea can be given of the available hardware/software/firmware. In some other cases, more specific information can be provided.

EXAMPLE 1

An example where more specific information is provided would be a requirements specification for a specific consumer where the platform is already known.

EXAMPLE 2

Examples of hardware/software/firmware identifications include:

- None (for a completely stand-alone TOE);
- a standard PC with a dual core 2.10 GHz or faster processor and 4GB or more RAM, running the Yaiza operating system for professionals, version 53.0 Update 6b, c, or 7, or version 54.0;
- a standard 64-bit server with a 2xQuad-Core core processor and 16GB or more RAM, running the Yaiza operating system, server edition version 7.0 Update 6d, and the WonderMagic 12.0 Graphics card with the 1.01 WM Driver Set;
- a CleverCard SB17067 integrated circuit;
- a CleverCard SB17067 integrated circuit running v12.0 of the QuickOS smart card operating system;
- Yaiza mobile-OS 3.1.6 on smartphone and tablet devices using the FP9 processor.

B.3.3 Conformance claims and conformance statement (APE_CCL)

B.3.3.1 General

This section of a PP describes how the PP:

- States the applicable edition of ISO/IEC 15408-1;
- Conforms with ISO/IEC 15408-2 and ISO/IEC 15408-3 (i.e. conformant or extended);
- Claims other PPs (if any);
- Claims Packages (if any);
- References to evaluation method(s) and/or activities derived from ISO/IEC 18405 (if any);
- Is allowed to be used in conjunction with other PPs and PP-Modules in PP-Configuration (required in the exact conformance case only).

The description of how the PP conforms to ISO/IEC 15408 (all parts) consists of two items: the edition of ISO/IEC 15408-1 that is used and whether the PP contains extended security requirements or not (see 10.2 and D.3.6).

The description of conformance claimed by the PP to other PPs means that the PP lists any other PPs to which conformance is being claimed to. The type of conformance being claimed is also identified. For an explanation of this, see 10.2.

The description of conformance of the PP to packages means that the PP lists the packages to which conformance is being claimed. For an explanation of this, see 10.2.

The references to the evaluation methods and/or activities means that the PP provides references to the evaluation method(s) and/or activities to be used during an evaluation based on a ST claiming conformance to the PP. These evaluation methods and activities may be included directly in the PP or may be found in a referenced supporting document. It is not necessary to reproduce the text of these evaluation methods and activities in the PP. See 10.2.

If evaluation method(s) and/or activities are included in the PP then the Conformance Statement shall also include a statement in the following form:

“This PP requires the use of evaluation methods and/or evaluation activities defined in <reference(s)>.”

Where <reference> is replaced by identification of the location of the evaluation methods and evaluation activities applicable to the PP.

NOTE 1 As outlined in clause 0, Evaluation Schemes may not approve the use of particular EMs/EAs.

The conformance type in the PP states how STs and/or other PPs shall conform to that PP. The PP author selects whether “exact”, “strict” or “demonstrable” conformance is required.

NOTE 2 See C.2.2.5 for the use of conformance claims in PP modules.

NOTE 3 See B.5.2 for the use of conformance claims in Direct Rationale PPs.

B.3.3.2 Exact conformance

If exact conformance is selected, the PP author shall, where applicable, specify the following information in the allowed-with statement in the conformance claims section of the PP:

- Other PPs that may be used, either by a ST based on this PP, or used in a PP-Configuration, with this PP;
- PP-Modules that may specify this PP as one of the PP-Module’s base PPs.

NOTE 1 If neither of the above options is exercised, then a ST can claim exact conformance to only the PP by itself.

NOTE 2 A PP cannot claim exact conformance to another PP.

B.3.4 Security problem definition (APE_SPD)

See 7.1 for information and requirements for the SPD. Including threats, assumptions and organizational security policies (OSPs).

B.3.5 Security objectives (APE_OBJ)

See 7.2 for information and requirements for the security objectives including security objectives for the TOE and security objectives for the operational environment.

NOTE In the case of Direct Rationale, security objectives for the TOE are not included.

B.3.6 Extended components definition (APE_ECD)

In many cases the security requirements in a PP are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3, see B.3.7. However, in some cases, there may be requirements in a PP that are not based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3. In these cases, new components, i.e. extended components, shall be defined, and the definition provided in the Extended Components Definition section. For more information on this, see 8.4.

NOTE This section is intended to contain only the extended components and not the extended requirements which are based on the extended components. The extended requirements are included in the security requirements section as described in B.3.7 and are then for all purposes treated identically to the requirements that are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3.

B.3.7 Security requirements (APE_REQ)

B.3.7.1 General

The security requirements consist of two groups of requirements:

a) *the security functional requirements* (SFRs): a translation of the security objectives for the TOE into a standardized language;

b) *the security assurance requirements* (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

These two groups are discussed in 7.3.

B.3.7.2 Including requirements in a PP

For a PP with strict conformance to another PP all the requirements in this PP shall be included, and additional requirements may be included in the conformant PP.

For a PP with demonstrable conformance to another PP all requirements in this PP shall be included, or a rationale explaining how they are otherwise met shall be provided in the conformant PP.

The following types of discretionary requirement may be included in PPs in all (exact, strict and demonstrable) conformance types:

If a PP contains optional requirements, a conformant PP may instantiate these requirements, being sure to include any required SPD-elements associated with those requirements. This may be done regardless of the conformance required by the PP. Omitting optional SFRs does not constitute "partial conformance" to a PP, and thus is allowed.

B.3.8 TOE summary specification (TSS)

Unlike a ST, a PP has no TOE summary specification.

B.4 Referring to other standards in a PP

In some cases, a PP author needs to refer to an external standard, such as a particular cryptographic standard or protocol. ISO/IEC 15408 (all parts) allows three ways of doing this:

a) As an organizational security policy (or part of it).

EXAMPLE 1

There exists a government standard defining how passwords have to be chosen, this may be stated as an organizational security policy in a PP. This may lead to an objective for the environment (e. g. if users of the TOE need to choose passwords accordingly), or it may lead to security objectives for the TOE and then to appropriate SFRs (likely of the FIA class), if the TOE generates passwords. In both cases the rationale of the PP author needs to make plausible that the security objectives for the TOE and the SFRs are suitable to fulfil the OSP. The evaluator will examine if this is in fact plausible (and may decide to look into the standard for this), if the OSP is implemented by SFRs, as explained below.

b) As a technical standard used in a refinement of a component or security requirement.

EXAMPLE 2

FCS_CKM.1.1 Refinement: The [selection: **TSF, TOE platform**] shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm

[selection:

— RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: [selection:

  – **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;**

  – **ANSI X9.31-1998, Section 4.1];**

— ECC schemes using "NIST curves" P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;

— FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1

].

If reference to only a certain part of a standard is desired, that part shall be unambiguously stated in the SFR refinement.

NOTE 1 The PP author is reminded that referring to a standard in SFRs can impose a significant burden on a developer developing a TOE that meets the PP (depending on the size and complexity of the standard and the assurance required), and that it can be more suitable to require alternative (non-CC related) ways to assess conformance to that standard.

B.5 Direct Rationale PPs

B.5.1 General

Writing a PP includes consideration of the STs that will be written with the PP as a basis. As noted in D.4, in some cases it is desired to write a PP that supports the specification of Direct Rationale STs.

The intention of the Direct Rationale PP is to minimize the level of indirection between the SPD, any security objectives for the operational environment, and the SFRs.

In some situations, it is appropriate to omit the definition of the TOE security objectives. In this case the SFRs enhanced with natural language descriptions and the objectives for the environment directly map the SPD.

A Direct Rationale PP consists of:

a) a PP introduction, consisting of a PP reference and a TOE overview;

b) the conformance claim;

c) security objectives for the operational environment;

d) the SFRs and the SARs (including the extended components definition) and the security requirements rationale (only if the dependencies are not satisfied).

The content of a Direct Rationale PP is shown in .

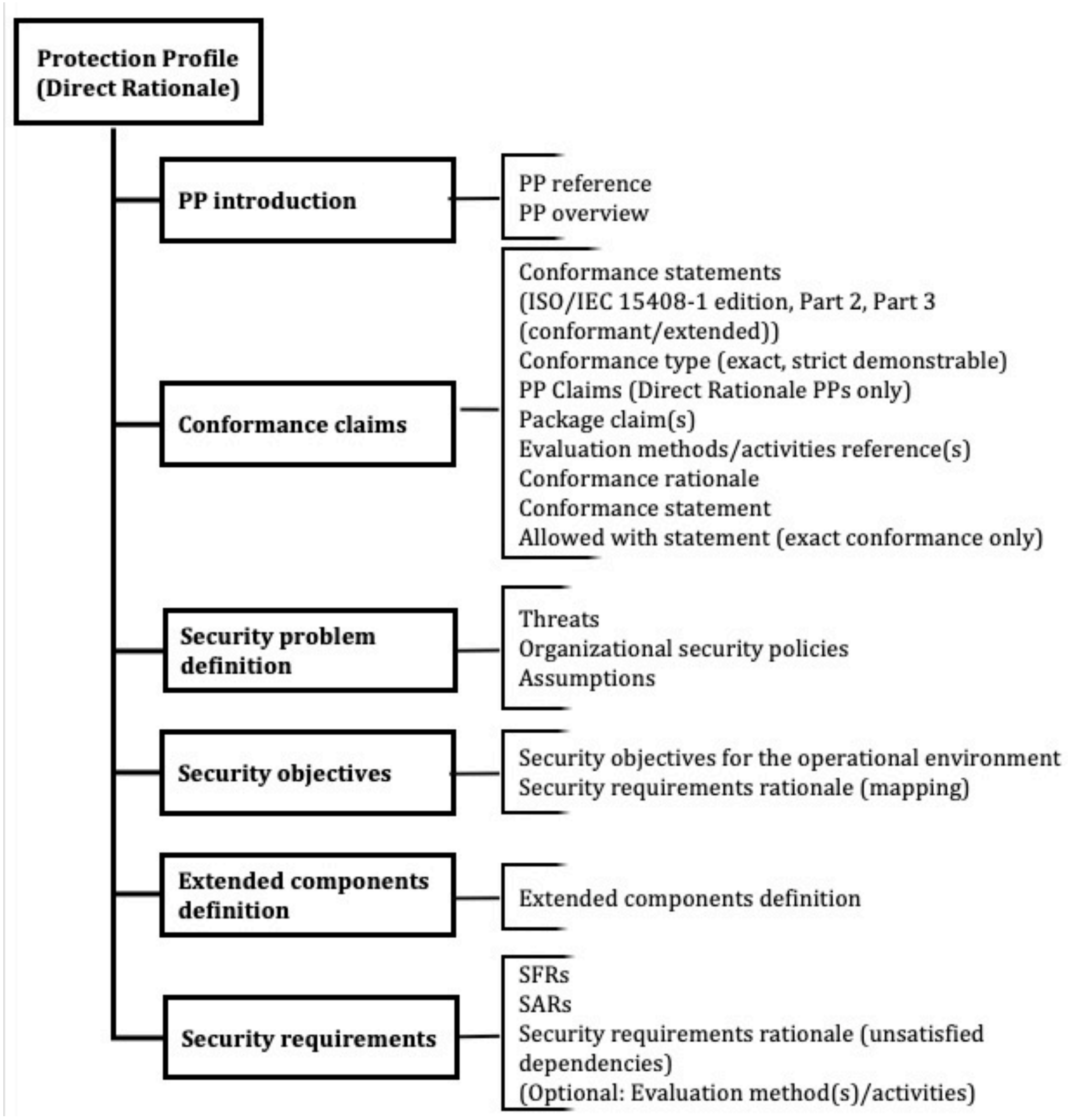

Protection Profile (Direct Rationale)
PP introduction
PP reference
PP overview
Conformance claims
Conformance statements
(ISO/IEC 15408-1 edition, Part 2, Part 3
(conformant/extended))
Conformance type (exact, strict demonstrable)
PP Claims (Direct Rationale PPs only)
Package claim(s)
Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
Allowed with statement (exact conformance only)
Security problem definition
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the operational environment
Security requirements rationale (mapping)
Extended components definition
Extended components definition
Security requirements
SFRs
SARs
Security requirements rationale (unsatisfied dependencies)
(Optional: Evaluation method(s)/activities)

Figure B.2 — Contents of a Direct Rational PP

B.5.2 Conformance claims (APE_CCL) for Direct Rationale PPs

A Direct Rationale PP shall only claim conformance to another Direct Rationale PP.

A regular PP may claim conformance with a Direct Rationale PP.

B.5.3 Security Problem Definition (APE_SPD) for Direct Rationale PPs

A Direct Rationale PP has the following differences when compared to a PP that contains security objectives for the TOE:

- security objectives for the TOE are not included. The security objectives for the operational environment shall still be described;
- a security objectives rationale is not included as there are no TOE security objectives in the PP;
- a Security Requirements rationale that directly maps the SFRs and any security objectives for the operational environment to the SPD-elements is included. It is recommended that this part of the security requirements rationale is located directly under each of the threats, OSPs and assumptions in the SPD section. As in regular PPs, the security requirements rationale also needs to justify any SFR dependencies that are not satisfied; this part of the rationale is typically located after the definition of the SFRs.
- there is a requirement to provide a natural language description of the SFRs and their relationship to security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

  EXAMPLE
  The following are examples of internal features:

  - Unavailability of residual data upon reallocation of a resource;
  - Hidden failure conditions of login/password-authentication;
  - Hidden biometric comparison score.

B.6 Optional Contents of a PP

PPs may include evaluation methods and/or activities that are derived from ISO/IEC 18405. Evaluation methods and/or activities that are associated with the PP are referenced in the conformance claims section of the PP. See subclause 10.2.

If the PP author decides to include any evaluation method(s) and/or activities in the PP then they shall be provided in the security requirements section with the relevant security requirement. Application notes, when appropriate, should be associated with the specific requirements.

Annex C
(Normative)

Specification of PP-Modules and PP-Configurations

C.1 Goal and structure of this Annex

The goal of this annex is to summarize the structure and expected content of PP-Modules and PP-Configurations.

NOTE 1 This annex does not define the requirements for evaluation of PP-Configurations. The PP-Configuration evaluation criteria are found in the ACE class given in ISO/IEC 15408-3.

C.2 Specification of PP-Modules

C.2.1 Using a PP-Module

A PP-Module is a security statement of a group of users or developers, regulators, administration, or any other entity that meets specific consumer needs. A PP-Module complements one or more PPs and optionally other PP-Modules, which are called collectively base PPs/PP-Modules, and allows consumers to refer to this statement, facilitates the evaluation against it and the comparison of conformant evaluated TOEs. A PP-Module can only be used within a PP-Configuration that includes those base PPs/PP-Modules.

NOTE A base PP is a PP that is required by a PP-Module. A base PP-Module is a PP-Module that is required by another PP-Module.

C.2.2 Mandatory Contents of a PP-Module

C.2.2.1 General

Figure C.1 shows the content of a PP-Module.

The content of a PP-Module is summarized below and explained in detail in C.2.2.2 to C.2.4. A PP-Module contains:

- an *Introduction* which identifies the PP-Module, identifies the base PPs/PP-Modules which it is based on and provides a description of the TOE within its environment that meets the descriptions underlying the base PPs/PP-Modules,
- a *Consistency rationale* that states the correspondence between the PP-Module and its base PPs/PP-Modules,
- a *Conformance claim* regarding the edition of ISO/IEC 15408 (all parts), the conformance statement and for the case of exact conformance the allowed-with statements,
- a *Security problem definition* with threats, assumptions, and organizational security policies,
- a *Security objectives section* presenting the solution to the security problem in terms of objectives for the TOE and its operational environment,
- an optional *Extended functional components* definition where new functional components not included in ISO/IEC 15408-2 are introduced,
- a *Security functional requirements* section with a standardized statement of the TOE security objectives,

Figure C.1 — Content of a PP-Module

- A *Security assurance requirement*s section, except in the exact conformance where the SARs are inherited from the base PPs.

C.2.2.2 PP-Module introduction

C.2.2.2.1 PP-Module reference

The PP-Module introduction provides a clear and unambiguous reference that allows identifying the PP-Module. A typical reference is made of the title of the PP-Module and the version of the document, the sponsors, and the publication date.

The PP-Module reference can be used to index the document in PP catalogues.

C.2.2.2.2 Identification of base PPs/PP-Modules

The PP-Module introduction identifies its base PPs/PP-Modules. The identification consists of a list of references.

A PP-Module that requires to be used with a set of base PPs/PP-Modules simultaneously, say $\{B_1 ..., B_n\}$, will provide an identification list of the following shape:

$$B_1 \dots \mathit{AND} \dots B_n \text{ with } n \geq 1$$

This set of PPs/PP-Modules must be closed, that is, for any PP-Module B_i, its own base PPs/PP-Modules must belong to the set $\{B_1 ... B_n\}$.

NOTE 1 This means that the set {B1 ..., B_n} either does not contain any PP-Module or that it contains at least one PP-Module which requires base PPs only but no other PP-Module.

A PP-Module may also allow alternative sets of base PPs/PP-Modules, say $\{S_1 ... S_k\}$; in this case, the identification list states:

$$S_1 \dots \mathit{OR} \dots S_k \text{ with } k \geq 1$$

The unfolded form of the identification of alternative sets of base PPs/PP-Modules is then:

$$(B_1 \dots \mathit{AND} \dots B_{n1}) \dots \text{OR} \dots (B_1 \dots \mathit{AND} \dots B_{nk}) \text{ with } k \geq 1 \text{ and ni} \geq 1$$

NOTE 1 A PP-Module that states an OR-ed list is equivalent to as many PP-Modules as elements S_i in the list. That is, an OR-ed list is a shortcut to avoid defining and maintaining similar PP-Modules for different usages.

C.2.2.2.3 TOE overview

The TOE overview of a PP-Module may complete the TOE overviews of the base PPs/PP-Modules, provided consistency between the PP-Module and its base PPs/PP-Modules is ensured:

- The TOE type of the PP-Module may either be the same as that of the base PPs/PP-Modules or may introduce specificities required to meet the purpose of the PP-Module.
- The PP-Module may introduce further usage and major security features in addition to those stated in the base PPs/PP-Modules.
- The PP-Module can specify particular non-TOE hardware, software and/or firmware compliant with the statement in the base PPs/PP-Modules.

In a PP-Module, the possibility of supplementing the TOE overview of the base PPs/PP-Modules has the same meaning as in a PP or ST that supplements the TOE overview of another PP to which they claim conformance.

The statement of the TOE overview in a PP-Module may be given by reference when it is the same as in its base PPs/PP-Modules, i.e. when there is no addition. The PP-Module may provide as many specific TOE overviews as alternative sets of base PPs/PP-Modules.

C.2.2.3 Consistency rationale

The PP-Module has to provide a consistency rationale with respect to its base PPs/PP-Modules.

If the PP-Module specifies alternative sets of base PPs/PP-Modules, the PP-Module shall provide as many consistency rationales as the number of alternative sets of base PPs/PP-Modules.

The consistency analysis shall be performed on the TOE type, the SPD, the objectives, and the security functional requirements. At the end, the goal is to demonstrate that a TOE can meet the TOE type descriptions provided in the base PP(s)/PP-Module(s) and in the PP-Module and satisfy all the security functional requirements specified in the PP-Module and its base PPs/PP-Modules The consistency rationale shall demonstrate that the unions of SPDs, objectives, and security functional requirements defined in the PP-Module and in its base PPs/PP-Modules do not lead to a contradiction.

The consistency rationale may use correspondence tables between SPD/objectives/SFRs together with textual justifications.

NOTE The consistency of the SFRs implies the consistency of the union of objectives and the union of SPDs provided that the PP-Module does not change the assumptions and objectives for the environment of the base PPs/PP-Modules.

C.2.2.4 Assurance rationale

A PP-Module of demonstrable or strict conformance type has to provide an assurance rationale.

The assurance rationale shall demonstrate the consistency of the applicable set of SARs (which may be inherited from its base PPs) with the SPD defined in the PP-Module. That is, that the assurance requirements and the threat model are not contradictory.

If the PP-Module does not inherit its set of SARs from its base PPs, then the assurance rationale shall demonstrate that the assurance requirements in the PP-Module and in its base PPs/PP-Modules are not contradictory with regard to the assets that are common to the PP-Module and its base PPs/PP-Modules.

C.2.2.5 Conformance claims and conformance statement

C.2.2.5.1 General

This section of a PP-Module shall be included for all PP-Modules and describes how the PP-Module conforms to:

- ISO/IEC 15408-2, ISO/IEC 15408-3, their editions, and any use of extended security requirements
- functional and assurance packages.

A PP-Module shall not claim conformance to any PP, other PP-Module, or PP-Configuration.

The PP-Module conformance statement identifies the required conformance type. Exact conformance is inherited from the base PPs and require that all the base PPs/PP-Modules are of exact conformance as well. The PP-Module conformance statement may also identify any evaluation methods and/or activities that are required to be used with it.

If evaluation methods and/or activities that have been derived from ISO/IEC 18045 are included in the PP-Module then the Conformance Statement may also include a statement in the following form:

"This PP-Module requires the use of evaluation methods and/or evaluation activities defined in <reference>."

Where <reference> is replaced by identification of the location of the evaluation methods and evaluation activities applicable to the PP-Module.

NOTE 1 Evaluation methods and/or evaluation activities can either be included in the PP-Module itself or included by reference to one or more separate documents describing them.

C.2.2.5.2 Exact conformance

In the case of exact conformance, the allowed-with statement also includes an identification of PPs and PP-Modules other than the PP-Module's set of base PPs/PP-Modules, that are allowed to be used in PP-Configurations with that PP-Module.

NOTE 1 All components in a PP-Configuration that requires exact conformance must also require exact conformance in their conformance statements.

NOTE 2 This maintains the exact conformance concept that the PP-Module authors have control over which other requirements can be specified in combination with the requirements specified in their PP-Module.

Figure C.2 shows how conformance claims and statements are inherited in the case of exact conformance.

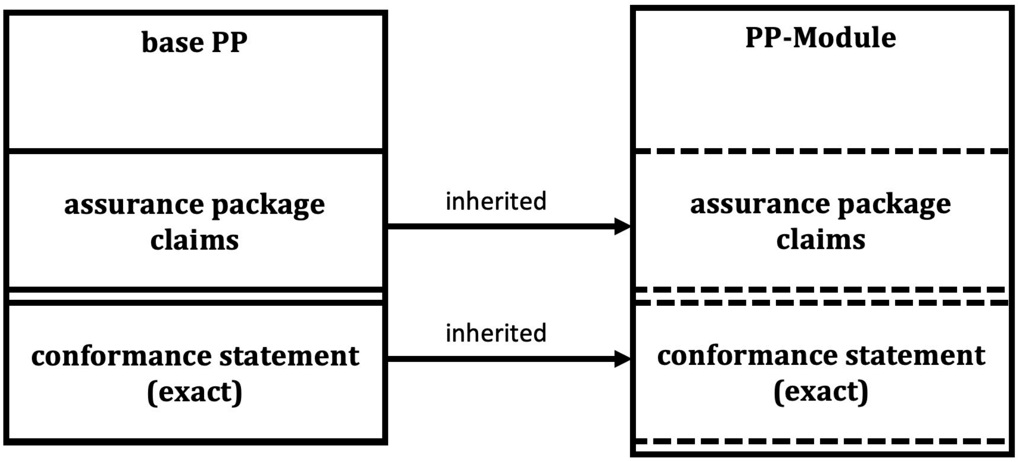


Figure C.2 — Inherited conformance claims and statement for exact conformance case

C.2.2.6 Security problem definition

This section defines the security problem addressed by the PP-Module. It can contain all types of SPD-elements, i.e. assumptions, threats, and organizational security policies.

A PP-Module defines the security problem in relationship with the security problem of the base PPs/PP-Modules and the definition of the TOE and its environment provided in the PP-Module's Introduction.

Each SPD-element could either come from a base PP/PP-Module or be entirely new. Let “E” be an SPD-element of the PP-Module, one of the following cases holds:

- “E” belongs to an identified base PP/PP-Module; a reference to the SPD-element is sufficient,
- “E” is a refinement of an SPD-element of a base PP/PP-Module,
- “E” is a new SPD-element, related to additional features of the TOE or its environment.

NOTE 1 The refined SPD-elements can be dealt with as new SPD-elements without any impact on the meaning of the SPD.

NOTE 2 In the same way that STs can, a PP-Module can introduce assumptions provided they cover aspects that are outside the scope of the base PPs/PP-Modules.

C.2.2.7 Security objectives

This section defines the security objectives for the TOE and for the TOE's operational environment.

A PP-Module defines new security objectives in context with the security objectives of the base PPs/PP-Modules.

Each Security Objective may either come from a base PP/PP-Module or be entirely new. Let “O” be an objective of the PP-Module, one of the following cases holds:

- “O” belongs to an identified base PP/PP-Module; a reference to the Security Objective is sufficient.
- “O” is a refinement of a security objective of a base PP/PP-Module,
- “O” is a new objective introduced by the PP-Module.

NOTE The refined objectives can be dealt with as new objectives without any impact on the meaning of the whole set of objectives.

A PP-Module may introduce new objectives for the TOE operational environment only when they address aspects that are outside the scope of the base PPs/PP-Modules.

In the case where a PP-Module refines the TOE type, some security objectives for the environment of the base PPs/PP-Modules can become security objectives for the TOE in the PP-Module.

This section also defines the rationale between the SPD and the security objectives of the PP-Module, which consists of a mapping that traces the SPD of the PP-Module to their security objectives as well as a justification demonstrating that the tracing is effective, as specified in 7.2.5. Moreover, the mapping has to show not only that all the SPD-elements are covered but also that there is no useless security objective.

It can happen that some security objectives of the PP-Module cover also SPD-elements of the base PPs/PP-Modules that do not belong to the SPD of the PP-Module itself. This information is not required but may be provided in application notes.

C.2.2.8 Extended functional components definition

This section is identical to the PP and ST extended components section specified in Clause B.3.6.

C.2.2.9 Security requirements

C.2.2.10 General

The security requirements consist of two groups of requirements:

a) *the security functional requirements* (SFRs): a translation of the security objectives for the TOE into a standardized language;

b) *the security assurance requirements* (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

These two groups are discussed in 7.3.

C.2.2.11 Security functional requirements

This section defines the security functional requirements for the TOE in relationship with the set of TOE security objectives in the PP-Module and with the security functional requirements of the base PPs/PP-Modules.

Each security functional requirement may either come from a base PP/PP-Module or be entirely new. Let “R” be a security functional requirement of the PP-Module, one of the following cases holds:

- “R” belongs to an identified base PP/PP-Module; a reference to the requirement is sufficient,
- “R” is a refinement of an SFR in a base PPs/PP-Module,
- “R” is a new requirement introduced by the PP-Module.

NOTE The refined requirements can be dealt with as new ones without any impact on the meaning of the whole set of requirements.

This section also defines the rationale between the SFRs and the TOE security objectives of the PP-Module, which consists of a mapping that traces the SFRs to the TOE objectives of the PP-Module and a justification demonstrating that the tracing is effective, as specified in 7.2.5. Moreover, the mapping shall show not only that all the objectives for the TOE are covered but also that there is no useless security functional requirement.

It may happen that some SFRs of the PP-Module cover also TOE security objectives of the base PPs/PP-Modules that do not belong to the PP-Module itself. This information is not required but may be provided in application notes.

PP-Modules may define and include optional SFRs (and any required SPD elements) as previously specified for PPs in B.3.7.

C.2.2.12 Security assurance requirements

A PP-Module of strict or demonstrable conformance defines the set of SARs to be used in PP-Configurations that include this PP-Module. The assurance rationale described in C.2.2.4. ensures the consistency of this set of SARs with regard to the base PPs/PP-Modules.

A PP-Module of exact conformance inherits the set of SARs, including any assurance packages such as the pre-defined EALs, from its base PPs. The issue of ANDed base PPs with different EALs must be resolved and is dealt with in the same way that a PP conformant to all those PPs deals with the issue.

C.2.3 TOE summary specification (TSS)

Unlike a ST, a PP-Module has no TOE summary specification.

C.2.4 Direct Rationale PP-Modules

PP-Modules can be written with the intention that they be used with a Direct Rationale PP(s) as their base PP(s). In this case security objectives for the TOE are not included in the PP-Module and security objectives for the TOE's operational environment may be included.

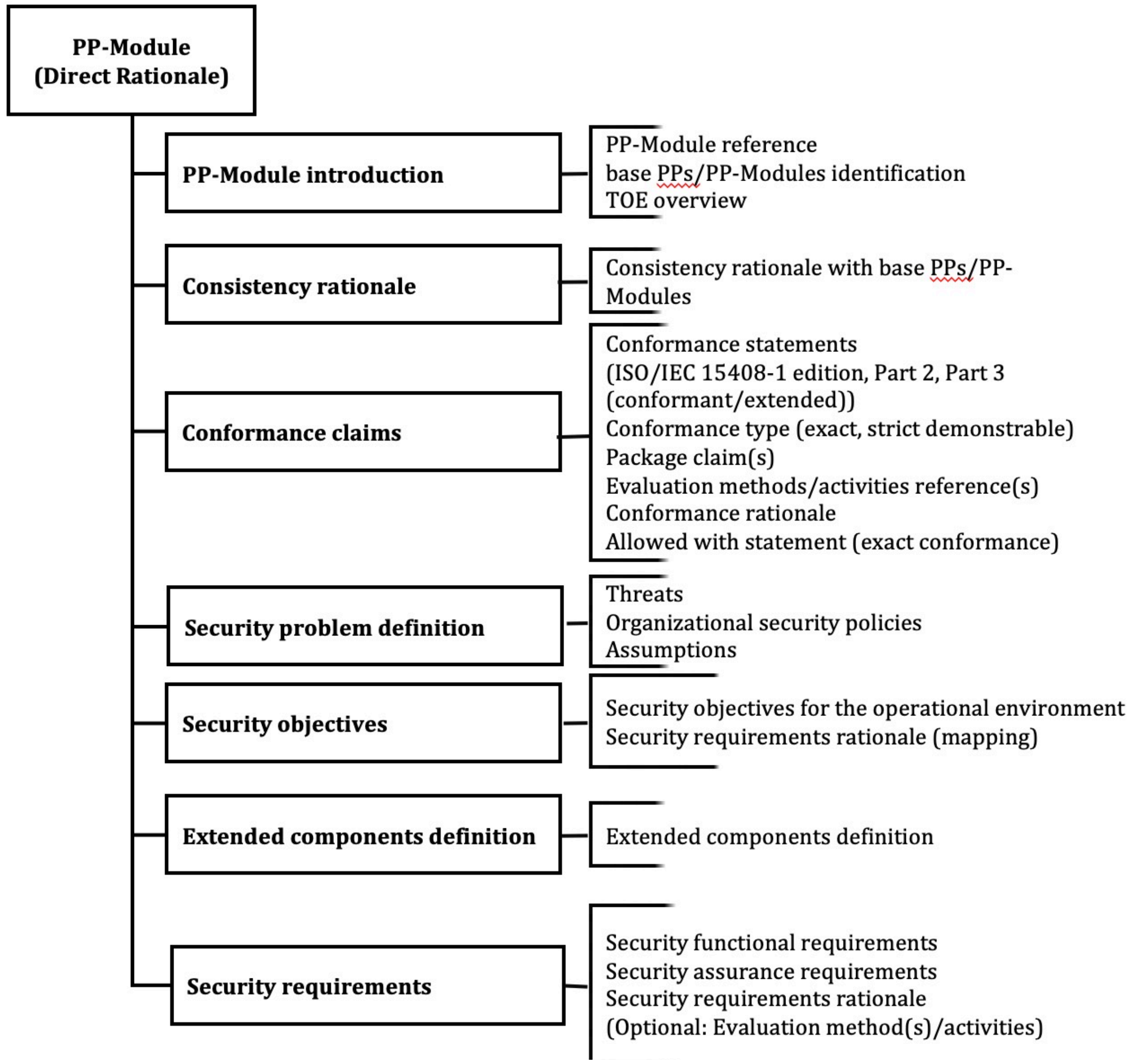

PP-Module (Direct Rationale)
PP-Module introduction
PP-Module reference
base PPs/PP-Modules identification
TOE overview
Consistency rationale
Consistency rationale with base PPs/PP-Modules
Conformance claims
Conformance statements
(ISO/IEC 15408-1 edition, Part 2, Part 3 (conformant/extended))
Conformance type (exact, strict demonstrable)
Package claim(s)
Evaluation methods/activities reference(s)
Conformance rationale
Allowed with statement (exact conformance)
Security problem definition
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the operational environment
Security requirements rationale (mapping)
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
(Optional: Evaluation method(s)/activities)

Figure C.3 — Direct Rationale PP-Module

The contents of a Direct Rationale PP-Module are shown in Figure C.3.

C.2.5 Guidance for inclusion of SPD-elements from a base PP/PP-Module

In order to limit the amount of information contained in the PP-Module, the PP-Module author applies the following rules:

Let E, O and R belong to the SPD, the security objectives, and the security functional requirements of a PP/PP-Module Q, respectively, with R mapped to O and O mapped to E.

Let M be a PP-Module and let Q be one of the base PP/PP-Module of M.

M has to satisfy the following condition: E, O, R, and the mappings between them should belong to M only if at least one of these elements is linked to a new element in M, that is

- Either there is a new SPD-element E' in M such that O is mapped to E', or
- There is a new objective O' in M such that O' is mapped to E' or R is mapped to O', or
- There is a new requirement R' in M such that R' is mapped to O.

That is, a PP-Module would not contain portions of base PPs/PP-Modules unless they are required to fulfil new needs. Here, refined elements are considered new.

C.2.6 Optional Contents of a PP-Module

PP-Modules may optionally include evaluation methods and/or activities that have been derived from ISO/IEC 18045. Evaluation methods and/or activities that are associated with the PP-Module are referenced in the conformance claims section. See 11.2.3.3.

If the PP-Module author decides to include any evaluation method(s) and/or activities in the PP-Module then they may be provided in the security requirement section with the relevant security requirement or in any other suitable section or external document. Application notes, when appropriate, should be associated with the specific requirements in the PP-Module.

C.3 Specification of PP-Configurations

C.3.1 Mandatory content of a PP-Configuration

C.3.1.1 General

The content of a PP-Configuration is summarized below in Figure C.4 and explained in detail in Annexes C.3.1.2 through C.3.1.7.

A PP-Configuration contains:

- a reference that uniquely identifies the PP-Configuration,
- a components statement that identifies the PPs and the PP-Modules composing the PP-Configuration, including all the base PPs/PP-Modules required to define a closed set of components,
- a conformance claim, that specifies the edition of ISO/IEC 15408, the claims to ISO/IEC 15408-2 and ISO/IEC 15408-3, the claims to assurance packages, and the conformance statement that defines whether the conformance of STs to this PP-Configuration has to be exact, strict, demonstrable, or a combination of strict and demonstrable inherited from its set of components, and any applicable evaluation methods and/or activities,
- a description of the TOE type,
- a description of the TSF organization in terms of the sub-TSFs defined by the PP-Configuration components,
- a SAR statement, specifying the set of the SAR that are applicable to the entire TOE. In a multi-assurance case, the SAR statement includes the sets of SARs that apply to the sub-TSFs defined in the PP-Configuration components. The SAR statement also includes the assurance rationale to ensure consistency between the PP-Configuration and its components.

NOTE An assurance package can be an EAL drawn from ISO/IEC 15408-5.

Figure C.4 — Content of a PP-Configuration

C.3.1.2 PP-Configuration reference

The PP-Configuration reference provides a clear and unambiguous identification, usually made of a title, version number, author, and the publication date.

The PP-Configuration reference can be used to index the document in catalogues.

C.3.1.3 Components statement

The PP-Configuration components statement identifies the PPs and the PP-Modules that compose the PP-Configuration.

The PP-Configuration components statement shall include the base PPs/PP-Modules required by the specified PP-Modules. If a PP-Module specifies alternative sets of base PPs/PP-Modules, only one of these sets shall be referred to in the PP-Configuration.

NOTE PP-Configurations do not directly claim conformance to functional packages, regardless of whether they are claimed by one of their components or not.

In the multi-assurance case, the PP-Configuration components statement shall provide the TSF organization in terms of the sub-TSFs defined by the components of the PP-Configuration.

C.3.1.4 TOE overview

The TOE overview of a PP-Configuration shall provide:

- The TOE type of the PP-Configuration, to be used by STs claiming conformance with the PP-Configuration.
- The expected usage and major security features of the TOE.
- The available non-TOE hardware, software and/or firmware (if applicable).

C.3.1.5 Consistency rationale

A PP-Configuration shall provide a consistency rationale to ensure the compatibility of the combination of components.

The consistency rationale shall demonstrate that the TOE overview is consistent with the TOE overview of the PP-Configuration components and that the unions of SPDs, objectives, and security functional requirements defined in these components do not lead to a contradiction.

The consistency rationale may use correspondence tables between SPD/objectives/SFRs together with textual justifications.

C.3.1.6 Conformance claim and conformance statement

C.3.1.6.1 ISO/IEC 15408-1 conformance claim

The edition of ISO/IEC 15408-1 and ISO/IEC 15408-3 applicable to the PP-Configuration;

NOTE The combination of different ISO/IEC 15408 editions in the PP-Configuration may be subject to compatibility issues, which must be addressed by the evaluation schemes

C.3.1.6.2 The conformance type

The conformance to this PP-Configuration by a ST shall be one of exact, strict, or demonstrable; or a combination of strict and demonstrable if the PP-Configuration contains components of both conformance types.

Any ST that claims conformance to a PP-Configuration shall conform to the conformance type required in the conformance statement of the PP-Configuration.

C.3.1.6.3 Assurance package conformance claim

The conformance claim may include an assurance package conformance claim describing any conformance of the PP-Configuration to an assurance package. More than one package may be claimed in a PP-Configuration.

C.3.1.6.4 Evaluation methods/activities references statement(s)

The PP-Configuration EM/EA references statement may specify the set of evaluation methods and/or activities that are applicable to the evaluation of the TOE specified in a ST based on the PP-Configuration.

A PP-Configuration may specify evaluation methods and/or activities in addition to those referenced in the PP-Configuration components.

NOTE In the case of strict or demonstrable conformance, it is not mandatory to declare every applicable EM/EA.

NOTE In the case of exact conformance, it is mandatory to declare every applicable EM/EA. See C.3.1.6.5 for restrictions on the specification of additional EM/EA in the case of exact conformance.

C.3.1.6.5 Additional requirements for exact conformance

If a PP-Configuration specifies exact conformance as its conformance type in its conformance statement then:

- If any one component in the PP-Configuration requires exact conformance, then all other components in the PP-Configuration shall also require exact conformance, and the conformance statement of the PP-Configuration shall specify exact conformance.
- All of the PP-Configuration components shall be allowed to be combined in their respective allowed-with statements. This is illustrated in Figure C.5.
- All components in the PP-Configuration shall allow all the other components in the PP-Configuration to be used together in the PP-Configuration in their respective allowed-with statement in the conformance claims section.

  NOTE A PP-Module does not need to include its own base PPs/PP-Modules in its allowed-with statement because they are implicitly allowed. An example is provided in Figure C.5..

- The EM/EA that are applied to a PP-Configuration shall be only those that are contained in the PP-Configuration's components; no additional evaluation methods/activities or modifications to the PP-Configuration components' evaluation methods/activities are allowed.

  EXAMPLE

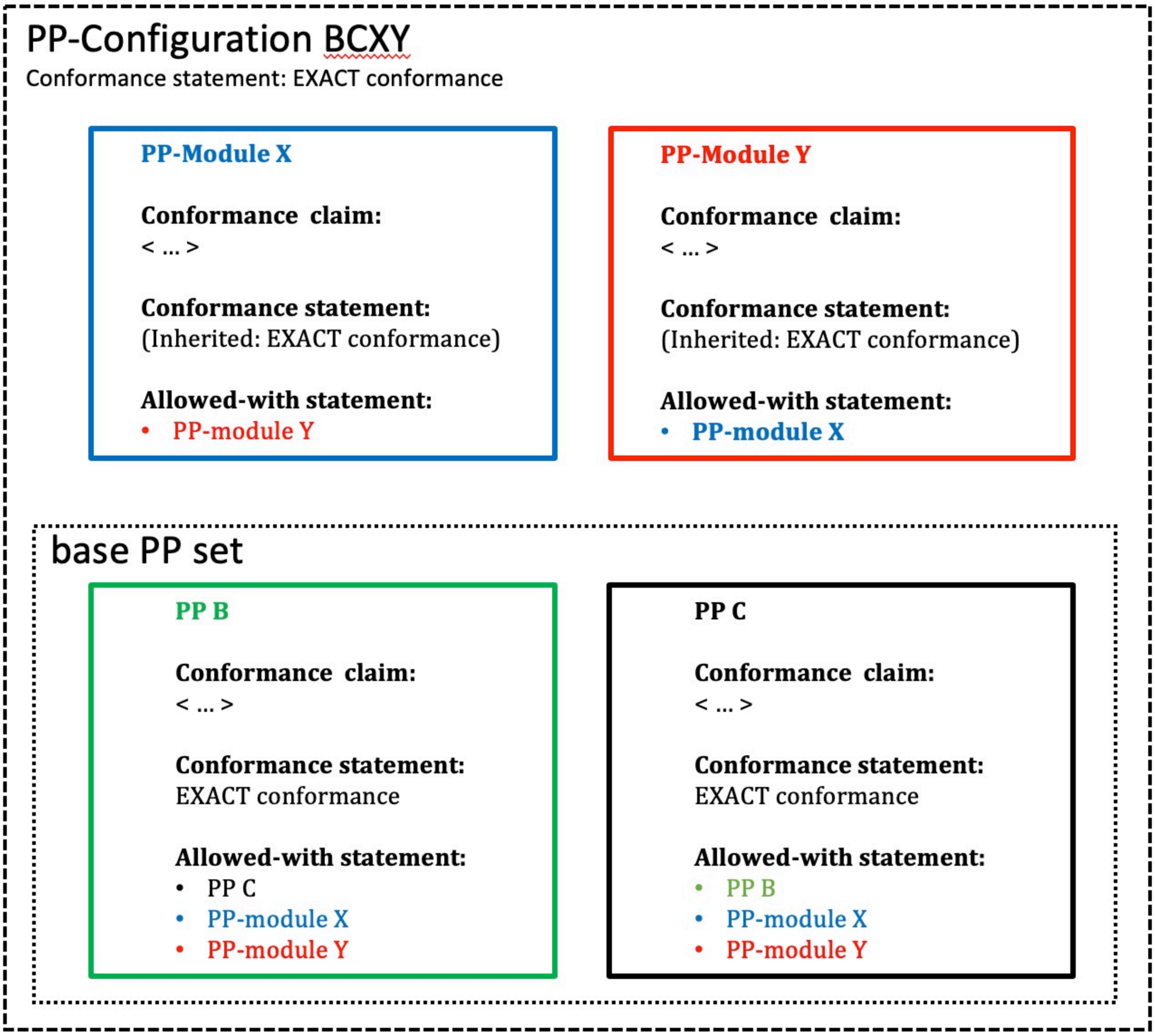


Figure C.5 — PP-Configuration and exact conformance

4719 A PP-Configuration requires exact conformance in its conformance statement because exact conformance is required in both base PPs, and is therefore inherited by the PP-Modules. PP-Modules X and Y both have an identical base PP set: PP B and PP C both of which require exact conformance. The following statements (shown in the diagram) must be true for this to be an evaluable PP-Configuration with a conformance statement of "exact conformance":

a) The PP-Modules inherit the conformance statement from their base PPs, so their conformance statement is exact conformance.

b) The PP-Configuration must require exact conformance since the PP-Modules require exact conformance.

c) PP B must specify in its conformance statement that it is allowed to be used with PP C, PP-Module X, and PP-Module Y.

d) PP C must specify in its conformance statement that it is allowed to be used with PP B, PP-Module X, and PP-Module Y.

e) PP-Module X must specify in its conformance statement that it is allowed to be used with PP-Module Y.

f) PP-Module Y must specify in its conformance statement that it is allowed to be used with PP-Module X.

C.3.1.7 SAR statement

The PP-Configuration SAR statement specifies the set of SARs applicable to the evaluation of a TOE specified by a ST that claims conformance to this PP-Configuration. In a multi-assurance case, when the PP-Configuration components carry different sets of SARs, the PP-Configuration must define the set of SARs that applies to each of the sub-TSF defined by these components.

The set of SARs that apply to the entire TOE, called global assurance package, is a superset of the common subset of SARs that apply to each of the PP-Configurations components.

In the PP-Configuration, the set of SARs that applies to each of the sub-TSF is either identical to the set of SARs defined in the corresponding PP-Configuration component or an augmentation of this set.

EXAMPLE

An example of a set of SARs is an EAL assurance package predefined in ISO/IEC 15408-5.

A PP-Configuration has to provide an assurance rationale to demonstrate the consistency of the applicable set of SARs with those defined in its components, in particular with regard to the common assets.

NOTE The assurance rationale of the PP-configuration must extend the analysis given in the PP-Modules to all the components of the PP-Configuration together. Usually this is done by unfolding the SPD-elements of the PP-Configuration components and analyzing the sets of SARs applicable to each asset.

Annex D
(Normative)

Specification of Security Targets and Direct Rationale STs

D.1 Goal and structure of this Annex

The goal of this annex is to summarize the structure and expected content of a ST.

As PPs and STs have a significant overlap, this annex focuses on the differences between PPs and STs. The material that is identical between STs and PPs is described in Annex B.

NOTE This annex does not define the requirements for the evaluation of STs. The ST evaluation criteria are found in the ASE class in ISO/IEC 15408-3.

This annex consists of four major parts:

a) *How to use a ST*. This is summarized in D.2. These subclauses describe how a ST should be used, and some of the questions that can be answered with a ST.

b) *What a ST must contain*. This is detailed in D.3. These subclauses describe the mandatory contents of the ST, the interrelationships between these contents, and provide examples.

c) *Claiming conformance with standards*. D.5 describes how a ST author can claim that the TOE meets a particular standard.

d) *Direct Rationale STs*. Direct Rationale STs are STs in which the SFRs and possibly to security objectives for the operational environment are mapped directly to the SPD-elements. Subclause D.4 is applicable to Direct Rationale STs.

D.2 Using a ST

D.2.1 How to use a ST

A typical ST fulfils two roles:

- Before and during the evaluation, the ST specifies “what is to be evaluated”. In this role, the ST serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. Technical correctness and completeness are major issues for this role. D.3.2 and D.3.5 describe how the ST is used in this role.

- After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST describes the exact security properties of the TOE in an abstract manner, and the potential consumer can rely on this description because the TOE has been evaluated to meet the ST. Ease of use and understandability are major issues for this role. D.2.3 describes how the ST is used in this role.

D.2.2 How not to use a ST

One role, among many, that a ST should not fulfil is:

- *a complete specification*: A ST is designed to be a security specification and not a complete specification. Unless security-relevant, properties such as interoperability, physical size, and weight, required voltage etc. should not be part of a ST. This means that in general a ST may be a part of a complete specification, but not a complete specification itself.

D.2.3 Questions that can be answered with a ST

After the evaluation, the ST specifies “what was evaluated”. In this role, the ST serves as a basis for agreement between the developer or re-seller of the TOE and the potential consumer of the TOE. The ST can therefore answer the following questions (and more):

a) *How can I find the ST/TOE that I need given the multitude of existing STs/TOEs?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

b) *Does this TOE fit in with my existing IT-infrastructure?* This question is addressed by the TOE overview, which identifies the major hardware/firmware/software elements needed to run the TOE;

c) *Does this TOE fit in with my existing operational environment?* This question is addressed by the security objectives for the operational environment, which identifies all constraints the TOE places on the operational environment in order to function;

d) *What does the TOE do (interested reader)?* This question is addressed by the TOE overview, which gives a brief (several paragraphs) summary of the TOE;

e) *What does the TOE do (potential consumer)?* This question is addressed by the TOE description, which gives a less brief (several pages) summary of the TOE;

f) *What does the TOE do (technical)?* This question is addressed by the TOE summary specification which provides a high-level description of the mechanisms the TOE uses;

g) *What does the TOE do (expert)?* This question is addressed by the SFRs which provide an abstract highly technical description, and the TOE summary specification which provide additional detail;

h) *Does the TOE address the problem as defined by my government/organization?* If your government/organization has defined packages and/or PPs and/or PP-Configurations to define this solution, then the answer can be found in the Conformance Claims section of the ST, which lists all packages, PPs and PP-Configurations that the ST conforms to;

i) *Does the TOE address my security problem (expert)?* What are the threats countered by the TOE? What organizational security policies does it enforce? What assumptions does it make about the operational environment? These questions are addressed by the security problem definition;

j) *How much trust can I place in the TOE?* This can be found in the SARs in the security requirements section, which provide the assurance requirements that were used to evaluate the TOE, and hence the trust that the evaluation provides in the correctness of the TOE.

D.3 Mandatory contents of a ST

D.3.1 General

There are two types of ST. Firstly the “regular” ST which is a ST that contains the full contents as described in D.3.3 through D.3.7.2. Secondly, in some cases a ST author may use a Direct Rationale ST which does not state the security objectives for the TOE. Direct Rationale STs, and the reasons and circumstances in which they are used are described in detail in D.4 All other parts of this Annex assume a ST with full contents.

Figure D.1 shows the contents of a ST that are given in ISO/IEC 15408- 3.

Figure D.1 may also be used as a structural outline of the ST, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it could be included in an appendix of the ST instead of in the security requirements section. The separate sections of a ST and the contents of those sections are briefly summarized below and explained in much more detail in D.3.3 through D.3.7.2. A ST contains:

a) *a ST introduction* containing three narrative descriptions of the TOE on different levels of abstraction;

b) *a conformance claim*, stating the ST's conformance to 15408-2 and 15408-3; showing whether the ST claims conformance to any PPs, PP-Configurations, and/or packages; and if so identifying the specific PPs, PP-Configurations, and/or packages, and the type of conformance claimed;

c) *a security problem definition*, showing threats, OSPs and assumptions;

d) *security objectives*, showing how the solution to the security problem is divided between security objectives for the TOE and security objectives for the operational environment of the TOE;

e) *extended components definitions* (optional), where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) may be defined. These new components are needed to define extended functional and extended assurance requirements;

f) *security requirements*, where a translation of the security objectives for the TOE into a standardized language is provided. This standardized language is in the form of SFRs. Additionally, this section defines the SARs;

g) *a TOE summary specification*, showing how the SFRs are implemented in the TOE.

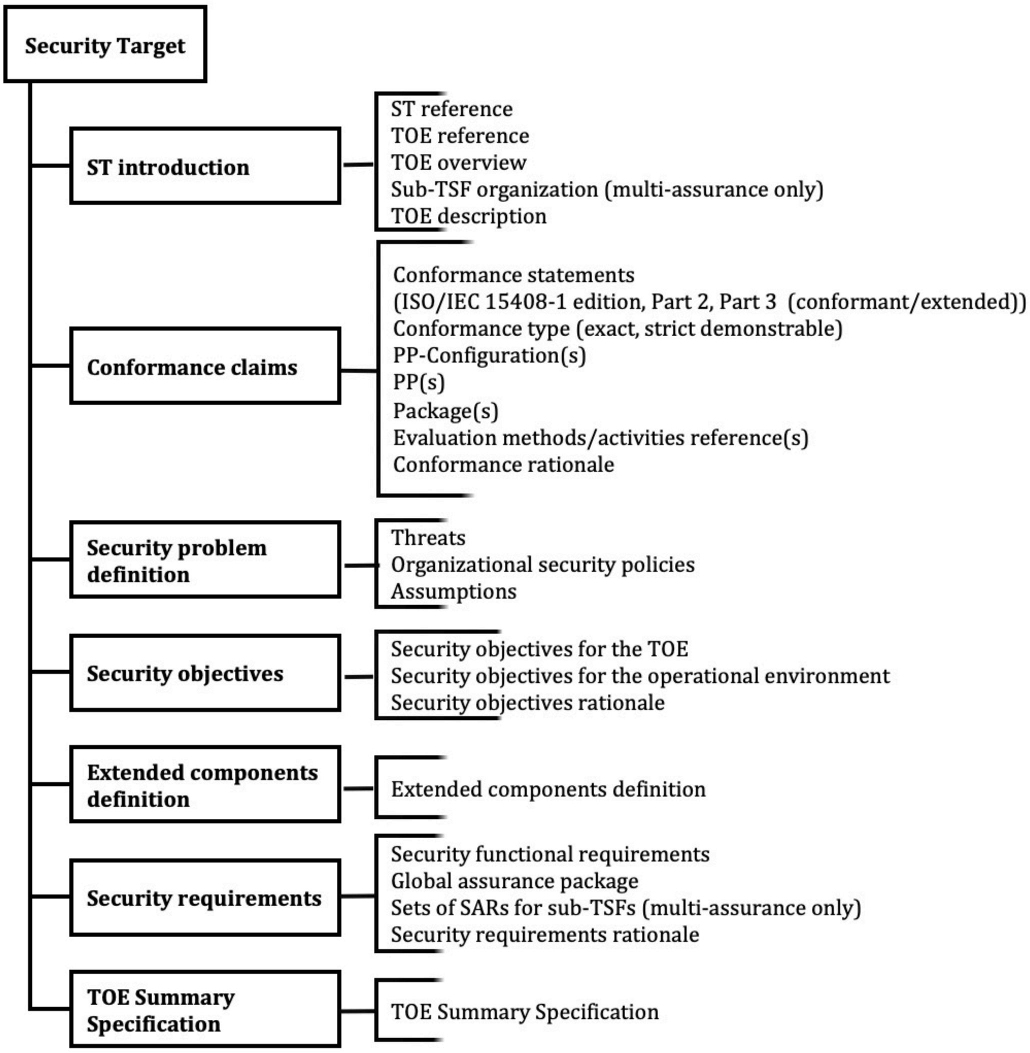

Security Target
ST introduction
ST reference
TOE reference
TOE overview
Sub-TSF organization (multi-assurance only)
TOE description
Conformance claims
Conformance statements
(ISO/IEC 15408-1 edition, Part 2, Part 3 (conformant/extended))
Conformance type (exact, strict demonstrable)
PP-Configuration(s)
PP(s)
Package(s)
Evaluation methods/activities reference(s)
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
Global assurance package
Sets of SARs for sub-TSFs (multi-assurance only)
Security requirements rationale
TOE Summary Specification
TOE Summary Specification

Figure D.1 — Contents of a ST

D.3.2 ST Introduction (ASE_INT)

The ST introduction describes the TOE in a narrative way on three levels of abstraction:

a) the ST reference and the TOE reference, which provide identification material for the ST and the TOE that the ST refers to;

b) the TOE overview, which briefly describes the TOE;

c) the TOE description, which describes the TOE in more detail.

D.3.2.1 ST reference and TOE reference

The ST reference and the TOE reference facilitate indexing and referencing the ST and TOE and their inclusion in catalogues.

A ST contains a clear ST reference that identifies that particular ST. A typical ST reference consists of title, version, sponsors, and publication date.

EXAMPLE 1

An example of a ST reference is "MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2017".

A ST also contains a TOE reference that identifies the TOE that claims conformance to the ST. A typical TOE reference consists of developer name, TOE name and TOE version number. A single TOE may be evaluated multiple times, for instance by different consumers of that TOE, and therefore have multiple STs associated with this this reference.

EXAMPLE 2

An example of a TOE reference is "MauveCorp MauveRAM Database v5.12".

If the TOE is constructed from one or more well-known products, it is allowed to reflect this in the TOE reference, by referring to the product name(s). However, this should not be used to mislead consumers: situations where major parts or security functionalities were not considered in the evaluation, yet the TOE reference does not reflect this are not allowed.

D.3.2.2 TOE overview

The TOE overview is aimed at potential consumers of a TOE who are looking through catalogs of evaluated TOEs/Products to find TOEs that meet their security needs, and are supported by their hardware, software, and firmware. The typical length of a TOE overview is several paragraphs.

To this end, the TOE overview briefly describes the usage of the TOE and its major security features, identifies the TOE type, and identifies any major non-TOE hardware/software/firmware required by the TOE.

In the case of a multi-assurance ST, the TOE overview also provides the TSF organization in terms of the sub-TSFs defined in the PP-Configuration the ST claims conformance to.

D.3.2.2.1 Usage and major security features of a TOE

The description of the usage and major security features of the TOE is intended to give a very general idea of what the TOE is capable of in terms of security, and what it can be used for in a security context. This section of the ST is written for (potential) TOE consumers, describing TOE usage and major security features in terms of business operations, using language that TOE consumers understand.

EXAMPLE

"The MauveCorp MauveRAM Database v5.12 is a multi-user database intended to be used in a networked environment. It allows 1024 users to be active simultaneously. It allows password/token and biometric authentication, protects against accidental data corruption, and can roll-back ten thousand transactions. Its audit features are highly configurable, so as to allow detailed audit to be performed for some users and transactions, while protecting the privacy of other users and transactions."

D.3.2.2.2 TOE type

The TOE overview identifies the type of TOE, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server and database, LAN, LAN with web server and database, etc.

In the case that the TOE is not of a readily available type, in which case a TOE type of "none" can be used.

The identification of the TOE type shall not be misleading for consumers.

EXAMPLE

Examples of misleading TOE types include:

- certain functionality can be expected of the TOE because of its TOE type, but the TOE does not have this functionality. Examples include:
  - an ATM-card type of TOE, which does not support any identification/authentication functionality;
  - a firewall type of TOE, which does not support protocols that are almost universally used;
  - a PKI-type of TOE, which has no certificate revocation functionality.
- the TOE can be expected to operate in certain operational environments because of its TOE type, but it cannot do so.:
  - a PC-operating system type of TOE, which is unable to function securely unless the PC has no network connection, floppy drive, and CD/DVD-player;
  - a firewall, which is unable to function securely unless all users that can connect through that firewall are benign.

D.3.2.2.3 Required non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs (notably software TOEs) rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the TOE overview is required to identify such non-TOE hardware, software and/or firmware. A complete and fully detailed identification of the additional hardware, software and/or firmware is not necessary, but the identification shall be complete and detailed enough for potential consumers to determine the major hardware, software and/or firmware needed to use the TOE.

EXAMPLE

Example hardware/software/firmware identifications are:

- a standard PC with a dual core 2.10 GHz or faster processor and 4GB or more RAM, running the Yaiza operating system for professionals, version 53.0 Update 6b, c, or 7, or version 54.0;
- a standard 64-bit server with a 2xQuad-Core core processor and 16GB or more RAM, running the Yaiza operating system, server edition version 7.0 Update 6d, and the WonderMagic 12.0 Graphics card with the 1.0 WM Driver Set;
- a CleverCard SB17067 integrated circuit;
- a CleverCard SB17067 integrated circuit running v12.0 of the QuickOS smart card operating system;
- the December 2019 installation of the LAN of the Director-General's Office of the Department of Traffic.

D.3.2.2.4 TSF organization in sub-TSFs in the multi-assurance case

A multi-assurance ST, i.e. a ST that claims conformance to a multi-assurance PP-Configuration and which defines multiple sets of SARs for the different sub-TSFs, shall inherit the organization of the TSF in sub-TSFs from the PP-Configuration.

The TOE overview describes such organization, possibly completed with details of the actual TOE.

D.3.2.3 TOE description

A TOE description is a narrative description of the TOE, likely to run to several pages. The TOE description provides evaluators and potential consumers with a general understanding of the security capabilities of the TOE, in more detail than was provided in the TOE overview. The TOE description may also be used to describe the wider application context into which the TOE will fit.

The TOE description discusses the physical scope of the TOE: a list of all hardware, firmware, software, and guidance parts that constitute the TOE. This list shall be described at a level of detail that is sufficient to give the reader a general understanding of those parts.

The TOE description shall also discuss the logical scope of the TOE, including the major TOE functions and provide a brief description of the security features (the TSF). The description provided shall be at a level of detail that is sufficient to give the reader a general understanding of those features. This description is expected to be in more detail than the major security features described in the TOE overview.

An important property of the physical and logical scopes is that they describe the TOE in such a way that there remains no doubt on whether a certain part or feature is in the TOE or whether this part or feature is outside the TOE. This is especially important when the TOE is integrated with and cannot be easily separated from non-TOE entities.

EXAMPLE 1

Examples where the TOE is integrated with non-TOE entities are:

- the TOE is a cryptographic co-processor of a smartcard IC, instead of the entire IC;
- the TOE is a smartcard IC, except for the cryptographic processor;
- the TOE is the Network Address Translation part of the MinuteGap Firewall v28.2.

In some cases, third-party components can present practical difficulties in obtaining evidence.

EXAMPLE 2

An example of where sufficient evidence for evaluation is not available from third-parties includes when source code, design documentation or test evidence cannot be made available to the developer of the TOE.

D.3.3 Conformance claims (ASE_CCL)

The conformance claims section of a ST describes how the ST conforms with ISO/IEC 15408 (all parts), packages, PPs, and PP-Configurations. It is identical to the conformance claims section for a PP described in B.3.3 with one exception, a ST does not have a conformance type since it is not allowed to claim conformance to another ST.

In the exact conformance scenario, a ST may conform to only one single-assurance PP-Configuration.

In the multi-assurance scenario, a ST shall conform to only one multi-assurance PP-Configuration.

D.3.4 Security problem definition (ASE_SPD)

The SPD section of a ST describes how the ST states the security problem that is to be addressed. It is identical to the SPD section for a PP described in B.3.4.

For a ST that conforms to PPs and/or PP-Configuration, the ST includes all the SPD elements defined in these PPs and PP-Configurations components. Remark that an assumption in a PP or PP-Configuration component may become an objective for the TOE in the ST.

D.3.5 Security objectives (ASE_OBJ)

This section of a ST is identical to the security objectives section of a PP as explained in B.3.5 and B.5.

For a ST that conforms to PPs and/or PP-Configuration, the ST includes all the objectives defined in these PPs and PP-Configurations components. Remark that objectives for the TOE operational environment in a PP or PP-Configuration component may become an objective for the TOE in the ST.

D.3.6 Extended Components Definition (ASE_ECD)

This section of a ST is identical to the extended components section of a PP as explained in B.3.6.

D.3.7 Security requirements (ASE_REQ)

D.3.7.1 Security Functional Requirements

D.3.7.1.1 General

This section of a ST is identical to the security requirements section of a PP as explained in B.3.7 with the exception that the specification of selection-based SFRs and optional requirements is not applicable in STs because all the SFRs must be fully instantiated.

For a ST that conforms to PPs and/or PP-Configuration, the ST includes all the SFRs defined in these PPs and PP-Configurations components.

D.3.7.1.2 Including requirements in STs

For STs with exact conformance to a PP all requirements in the PP shall be included. Requirements that are not found in the PP shall not be included in the ST.

For STs with strict conformance to a PP all requirements in a PP shall be included.

For STs with demonstrable conformance to a PP all requirements in a PP shall be included, or a rationale explaining how they are otherwise met shall be provided in the ST.

For STs with strict or demonstrable conformance to a PP, additional requirements not found in the PP may be included provided they support additional security objectives/cover additional threats.

For a STs claiming conformance to a PP-Configuration, the same rules as for conformance to a PP applies. In that case, the requirements are taken from the components of the PP-Configuration, i.e. its PPs and PP-Modules. If the PP-Configuration contains components that require different conformance type (strict and demonstrable only, because exact conformance cannot be combined with other types), the ST conforms to each of the components (PPs and PP-Modules) in the manner they require, either strict or demonstrable.

If the ST claims conformance to a PP or PP-Configuration, and the PP or the components of the PP-Configuration contain optional requirements, the ST may instantiate these requirements, being sure to include any required SPD-elements associated with those requirements. This may be done regardless of the conformance required by the PP or PP-Configuration. Omitting optional SFRs in a ST does not constitute “partial conformance” to a PP or PP-Configuration, and thus is allowed.

EXAMPLE 1

Example of the specification of external standards in SFRs and their evaluation:

> **FCS_CKM.1.1 Refinement:** The **TSF**[1] shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: **FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3**[2].

Conformance to the standard as part of the fulfilment of the SFR by the TOE is then assessed in one of the following ways:

- If an explicit Evaluation Activity has been defined for the SFR, then the evaluator actions in that Evaluation Activity are carried out;

[1] [selection: **TSF, TOE platform**]

[2] [selection:

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: [selection:
  - **FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;**
  - **ANSI X9.31-1998, Section 4.1];**
- ECC schemes using “NIST curves” P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1]

- If no explicit Evaluation Activity has been defined for the SFR then conformance is subsequently determined as if the full text of the standard is included as part of the SFR, applying the SARs that have been selected for the ST.

D.3.7.2 Security Assurance Requirements

The ST specifies the set of SARs applicable to the evaluation of a TOE.

If the ST conforms to a PP or PP-Configuration, then the set of SARs must be consistent with the PP or PP-Configuration.

If the ST conforms to a multi-assurance PP-Configuration, then

- either the ST applies a one set of SARs to the entire TOE and TSF (consistent with the global assurance package defined in the PP-Configuration). In this case, the TOE must be evaluated following the single-assurance approach,
- or the ST defines the global set of SARs that applies to the entire TOE and the sets of SARs that apply to each of the sub-TSF defined in the PP-Configuration (consistent with the sets of SARs defined in the PP-Configuration). In this case, the TOE must be evaluated following the multi-assurance approach.

A multi-assurance ST (and STs that augment the SARs of the PPs/PP-Configurations they conform to) must provide an assurance rationale to demonstrate the consistency of the sets of SARs.

D.3.8 TOE summary specification (ASE_TSS)

The objective for the TOE summary specification (TSS) is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification provides the general technical mechanisms that the TOE uses for this purpose. The level of detail of this description shall be sufficient to enable potential consumers to understand the general form and implementation of the TOE.

The statement of security requirements includes a natural language description, part of which describes how the SFRs combine together to provide security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

EXAMPLE 1:

The following are examples of internal features:

- Unavailability of residual data upon reallocation of a resource;
- Hidden failure conditions of login/password-authentication;
- Hidden biometric comparison score.

EXAMPLE 2:

If the TOE is an Internet PC and the SFRs contain FIA_UAU.1 to specify authentication, the TOE summary specification should indicate how this authentication is done: password, token, iris scanning etc. More information, like applicable standards that the TOE uses to meet SFRs, or more detailed descriptions may also be provided.

EXAMPLE 3:

The TOE summary specification may reference Technical standards, for instance: “The TOE provides cryptographic functionality to perform an AES encryption and decryption with 128, 192- or 256-bits keys to the embedded software. The AES algorithm conforms with ISO/IEC 18033-3:2010, 5.2.”

Note 1 The ST is an input to ADV, which means that ADV allows to point out inconsistencies between TSS and other specifications. However, there is no dedicated evaluation activity specified, which reflects the fact that the TSS provides an overview of the realization of the SFRs by the TOE but does not constitute an implementation specification.

NOTE 2 Since a Direct Rationale ST has no TOE summary specification, this option is not valid for Direct Rationale STs.

D.4 Direct Rationale STs

D.4.1 General

In some situations, it is appropriate to omit the definition of the TOE security objectives. In this case the Security Requirements rationale directly maps the SFRs and, where appropriate, security objectives for the operational environment, to the SPD.

The intention of the Direct Rationale ST is to minimize the level of indirection between the SPD, any security objectives for the operational environment, and the SFRs, based on an enhanced description of the SFRs.

The differences found in a Direct Rationale ST are in the conformance claims, security objectives and in the SPD sections. These are described in D.4.2 and D.4.3, below.

The content of a Direct Rationale ST is shown in Figure D.2.

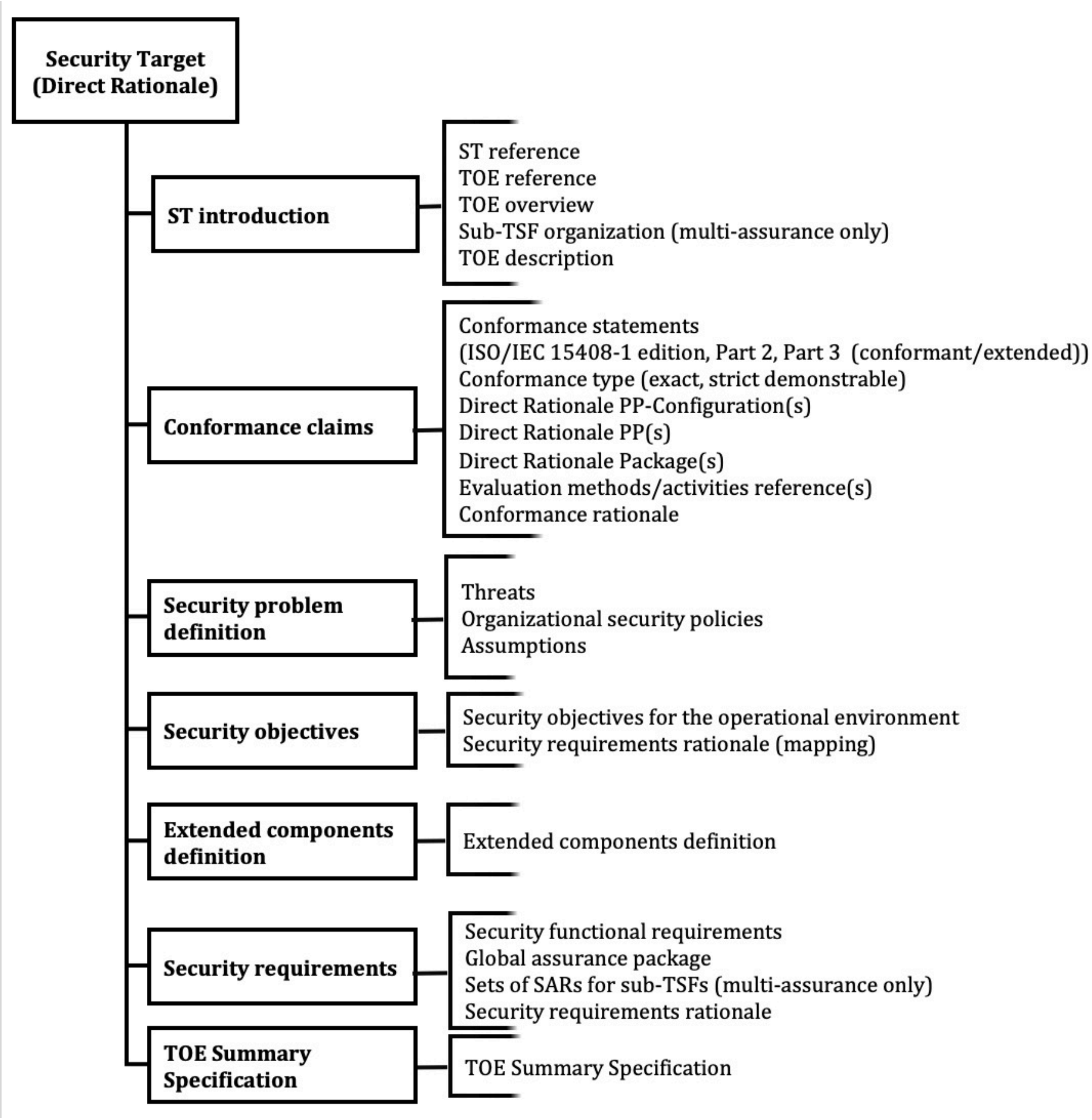

Security Target (Direct Rationale)
ST introduction
ST reference
TOE reference
TOE overview
Sub-TSF organization (multi-assurance only)
TOE description
Conformance claims
Conformance statements
(ISO/IEC 15408-1 edition, Part 2, Part 3 (conformant/extended))
Conformance type (exact, strict demonstrable)
Direct Rationale PP-Configuration(s)
Direct Rationale PP(s)
Direct Rationale Package(s)
Evaluation methods/activities reference(s)
Conformance rationale
Security problem definition
Threats
Organizational security policies
Assumptions
Security objectives
Security objectives for the operational environment
Security requirements rationale (mapping)
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Global assurance package
Sets of SARs for sub-TSFs (multi-assurance only)
Security requirements rationale
TOE Summary Specification
TOE Summary Specification

Figure D.2 — Contents of a Direct Rationale ST

D.4.2 Conformance claims (ASE_CCL) for Direct Rationale STs

A Direct Rationale ST shall only claim conformance to other Direct Rationale PPs (see 12.2 and Annex B).

A Direct Rationale ST shall only claim conformance to a PP-Configuration that uses the Direct Rationale approach. (see 12.2)

D.4.3 Security Problem Definition (ASE_SPD) for Direct Rationale STs

D.4.3.1 General

A Direct Rationale ST has the following differences when compared to a ST that contains security objectives for the TOE:

- Security objectives for the TOE are not included.
- A security objectives rationale is not included as there are no TOE security objectives in the ST;
- A Security Requirements rationale that directly maps the SFRs and any security objectives for the operational environment to the SPD-elements is included. It is recommended that this part of the security requirements rationale is located directly under each of the threats, OSPs and assumptions in the SPD section. As in a ST that contain security objectives for the TOE, the security requirements rationale also needs to justify the absence of superfluous SFRs and any SFR dependencies that are not satisfied; this part of the rationale is typically located after the definition of the SFRs.
- There is a requirement, given in ISO/IEC 15408-3, to provide a natural language description of the SFRs and their relationship to security functionality in terms of the architecture that is visible (observable) to Administrators and other users, or in terms of internal features or properties.

D.4.3.2 Tracing between SFRs, security objectives and the security problem definition

The tracing between SFRs, security objectives and the SPD becomes more straightforward in a Direct Rationale ST.

Figure D.3 shows the more direct specification of the SFRs that is used in the Direct Rationale approach.

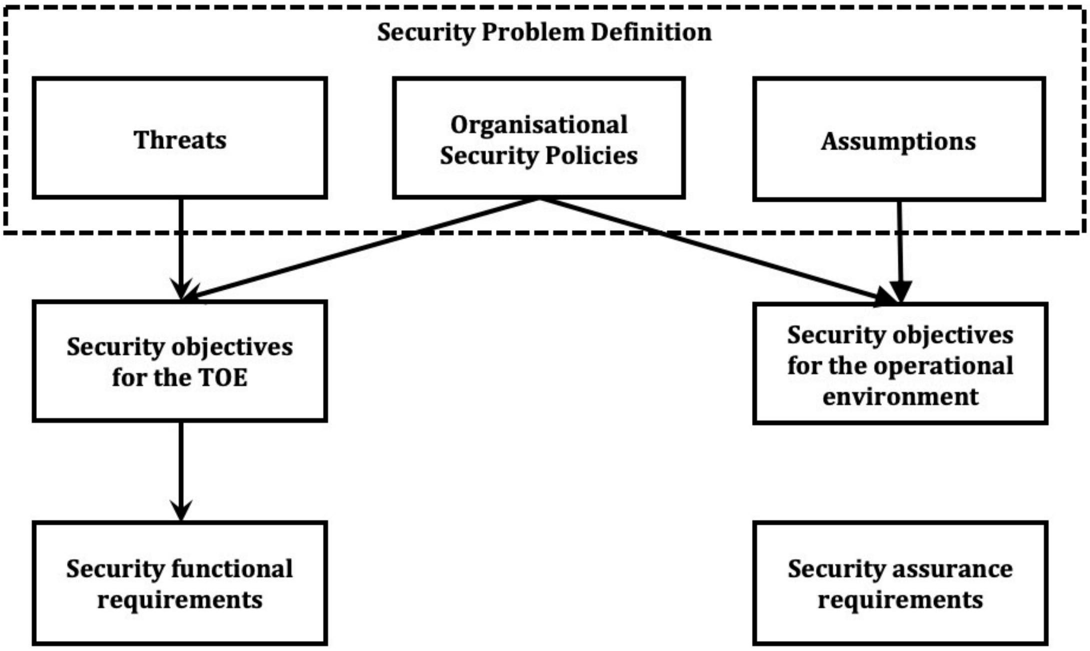

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure D.3 — Relations between the security problem definition, the security objectives, and the security requirements for Direct Rationale STs

D.5 Referring to other standards in a ST

Referring to standards in a ST is similar to the section on standards for PPs as described in B.4. Examples are given in clauses D.3.7.1.2 and D.3.7.2.

Annex E (Normative)

PP Conformance

E.1 General

A PP is intended to be used as a “template” for a ST. That is: the PP describes a set of user needs, while a ST that conforms to that PP describes a TOE that satisfies those needs.

ISO/IEC 15408 (all parts) does not allow any form of partial conformance, so if PP conformance is claimed, the ST shall conform to the referenced PP(s) or PP-Configuration.

NOTE 1 In the case of selection-based or optional SFRs, the inclusion or exclusion of these types of SFRs as outlined in 7.3.2.6 is not considered partial conformance and so is allowed.

ISO/IEC 15408 (all parts) defines three types of conformance: “demonstrable”, “strict” and “exact” where the type of conformance allowed is determined by the PP or PP-Configuration (and indirectly its PPs and PP-Modules). That is, the PP/PP-Configuration states, in accordance with B.3.3, what the allowed types of conformance for the derivative STs are.

As indicated in 10.3, if a PP/PP-Configuration specifies exact conformance, then a ST shall only claim exact conformance to that PP, and any other PP to which the ST claims conformance shall also require exact conformance. If the PP is included in a PP-Configuration (either by itself, or as a base PP to a PP-Module in that PP-Configuration), then the PP-Configuration itself and all other components of the PP-Configuration also require exact conformance.

The distinction between demonstrable, strict, and exact conformance when such conformance statements are contained in multiple PPs to which a ST is claiming conformance is applicable to each PP to which a ST may claim conformance on an individual basis. This may mean that the ST conforms strictly to some other PPs and demonstrably to other PPs.

A ST with exact conformance type shall claim conformance to a PP or PP-Configuration only if the PP/PP-Configuration is of exact conformance type and explicitly allows this.

A ST shall only claim demonstrable conformance to a PP or PP-Configuration if the PP/PP-Configuration explicitly allows this.

NOTE 2 Demonstrable conformance means that STs claiming conformance with the PP or PP-Configuration must offer a solution to the generic security problem described in the PP/PP-Configuration, but can do so in any way that is equivalent or more restrictive to that described in the PP/PP-Configuration. In principle that means that the ST can contain statements that vary from the PP/PP-Configuration, provided that overall the ST levies the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

It is also possible for a PP to be used as a template for another PP that specifies either strict or demonstrable conformance type. That is, PPs specifying either strict or demonstrable conformance can claim conformance to other PPs. This case is completely similar to that of a ST vs. a PP.

When the ST conforms with a PP-Configuration and this PP-Configuration is not of exact conformance, then the ST may be required to conform in a strict and in a demonstrable manner depending on the conformance types of the PP-Configuration components.

The conformance of a PP to a PP-Configuration is not allowed regardless of the conformance types.

E.2 Demonstrable conformance

Demonstrable conformance is orientated to the PP sponsor who requires evidence that the ST is a suitable solution to the generic security problem described in the PP.

Where there is a clear subset-superset type relation between PP and ST in the case of strict conformance, the relation is less clear-cut in the case of demonstrable conformance. STs claiming conformance to the PP shall offer a solution to the generic security problem described in the PP.

However, claiming conformance is allowed only in the case that the ST imposes the same, or more, restrictions on the TOE and the same, or less, restrictions on the operational environment of the TOE.

E.3 Strict conformance

Strict conformance is oriented to the PP sponsor who requires evidence that the requirements in the PP are met, that the ST is an instantiation of the PP, though the ST could be broader than the PP. In essence, the ST specifies that the TOE does at least the same as in the PP, while the operational environment does at most the same as in the PP.

EXAMPLE

A typical example of the use of strict conformance is in selection-based purchasing where an IT product's security requirements are expected to match those specified in the PP.

A ST instantiating strict conformance to a PP can still introduce additional restrictions to those given in the PP.

E.4 Exact conformance

E.4.1 General

Exact conformance is oriented to the PP sponsor who requires evidence that the requirements in the PP are met, and that the ST is an instantiation of exactly those security requirements (SFRs) without including additional functionality. In essence, the ST specifies that the TOE does what is required by the PP without making additional claims.

If “exact” conformance is selected, the PP author also has the option of specifying the following information:

a) Other PPs to which a ST may claim conformance in combination with the subject PP and still maintain exact conformance;

b) PP-Modules that may be specified with the PP in a PP-Configuration and still maintain exact conformance.

NOTE 1 This can be achieved either by using the PP as a base PP, or by inclusion in the PP-Configuration with a different base PP.

ISO/IEC 15408 (all parts) allows STs to claim exact conformance to multiple PPs as long as all PPs require exact conformance in their conformance statement, and allow the claim with the other PPs specified. ISO/IEC 15408 (all parts) allows STs to claim exact conformance to a PP-Configuration as long as the PP-Configuration requires exact conformance and the STs do not claim conformance to any other PP or PP-Configuration.

ISO/IEC 15408 (all parts) also allows PPs to claim conformance to one or more PPs. However, in the case where the PP being claimed requires exact conformance the potential to circumvent the intent of exact conformance becomes apparent. This is because requirements could be added that the exact conformance PP’s authors would not find appropriate for use with the claimed PP. Therefore, if a PP requires exact conformance, another PP shall not claim any type of conformance to that PP. This restriction gives the exact conformance PP author more control over the functionality and assurance provided for conformant STs than either strict or demonstrable conformance does.

EXAMPLE 1

If a ST can claim conformance to PP A (which requires exact conformance) and to PP B (which requires demonstrable conformance) at the same time, this would pull in SFRs which PP A’s author did not explicitly approve to be used in combination with PP A’s functionality when a ST claims conformance to PP A.

As indicated above, it is allowed for a ST to claim exact conformance with multiple exact conformance PPs. Also, a PP-Configuration is allowed to include multiple components (PPs, base PPs, and PP-Modules) that require exact conformance. In order to allow PP authors to maintain control of which PP-Configuration components may be claimed along with their PP, the conformance statement in the PP, described in B.2.3, may also include a statement specifying which PPs a ST author may simultaneously claim conformance to with the subject PP. All identified PPs shall require exact conformance in their conformance statement and shall also list the subject PPs, and all other PPs being claimed, in their conformance statement. The same construct is used for PP-Modules and base PPs (although base PPs are indistinguishable PPs that are not designated as base PPs in this aspect). Example 2 is provided to clarify the concept of a ST claiming conformance to multiple PPs.

EXAMPLE 2

For the ST example, suppose PP B's authors wanted to allow STs to claim conformance to PP "B" and also to allow conformance claims to it in combination with PP "C". This situation is pictured in Figure E.1.

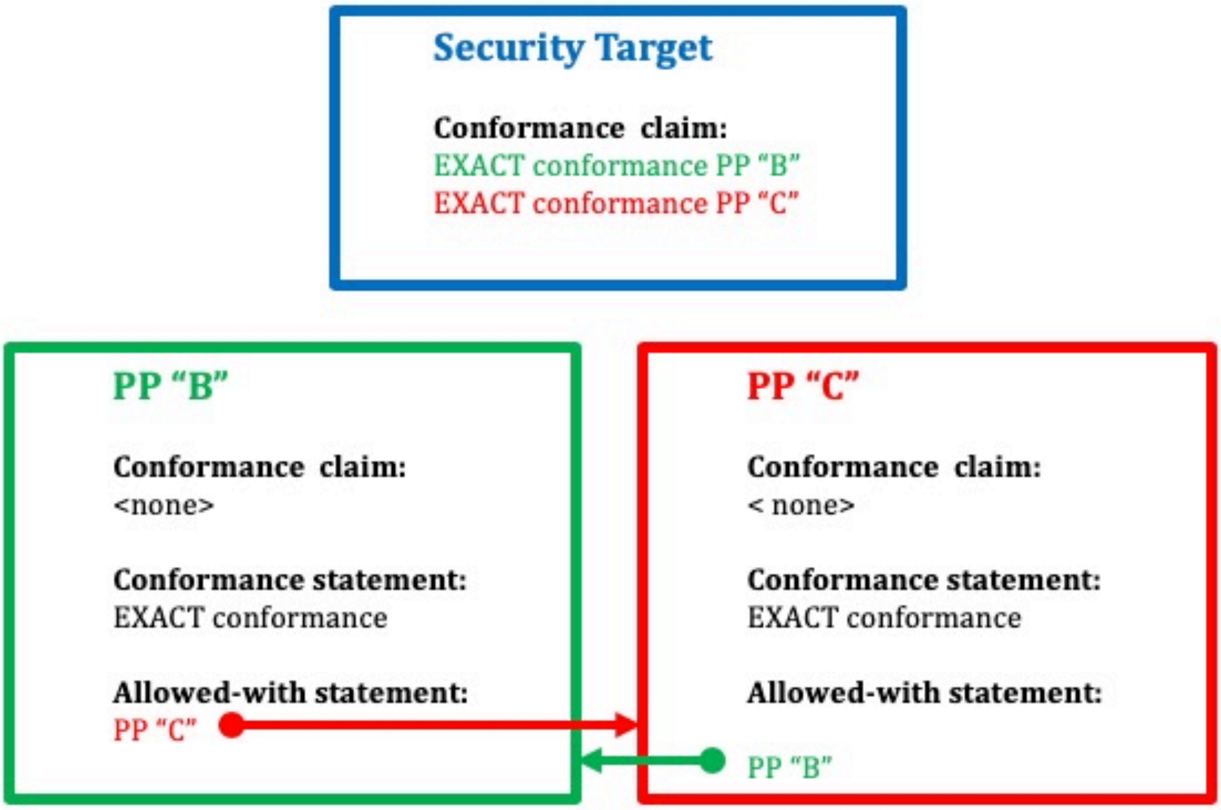


Figure E.1 — Exact conformance of a ST to multiple PPs

Then the following would have to be true:

a) Both PP B and PP C would have to specify exact conformance in their conformance statement.

b) PP B would list PP C as allowed with PP B in its allowed-with statement.

c) PP C would list PP B as allowed with PP C in its allowed-with statement.

If any of these statements did not hold, then the ST could not claim exact conformance to PPs B and C.

This concept also extends to PP-Modules and PP-Configurations. A PP-Module shall identify a set of base PPs/PP-Modules; if one of the identified base PPs/PP-Modules has a conformance statement of exact conformance, then all of the base PPs/PP-Modules specified by the PP-Module shall also have conformance statements specifying exact conformance. Further, in order to ensure that the PP-Modules are allowed for use with the base PP/PP-Module, each base PP/PP-Module specifies in its conformance statement the PP-Modules that are allowed to specify it as a base PP/PP-Modules for use in a PP-Configuration.

NOTE 3 The reverse is not true; a PP-Module does not need to specify any of its base PPs/PP-Modules in the Allowed-with statement because it has implicitly done so by defining the PP/PP-Module as a base PP/PP-Module.

A PP-Module also specifies which other PP-Modules or PPs that are not already included as one of the PP-Module's base PPs/PP-Modules, can be used in combination with it in a PP-Configuration.

EXAMPLE 3

Figure E.2 describes a case for exact conformance involving both PPs and PP-Modules.

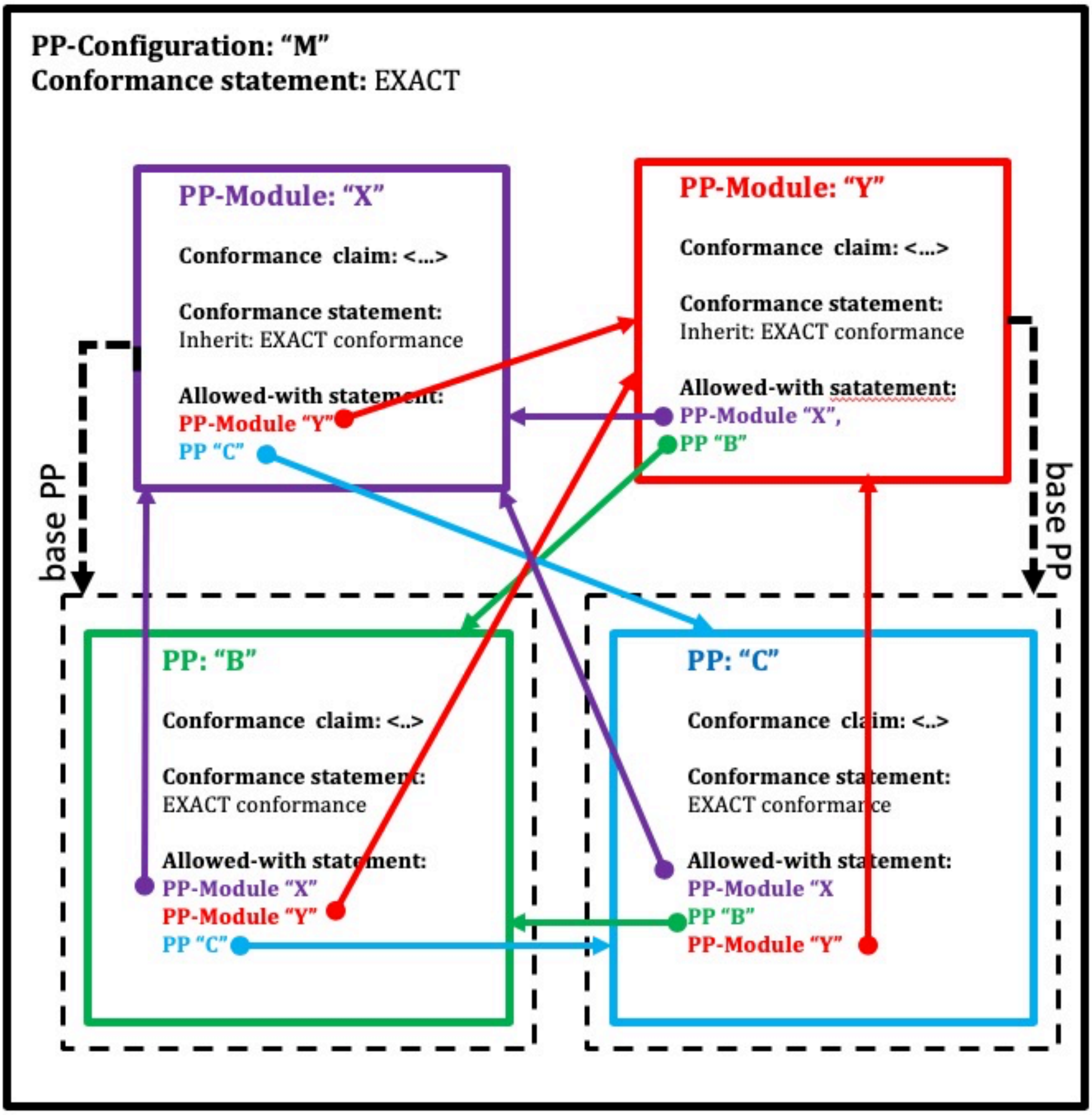


Figure E.2 — Exact conformance with a PP-Configuration including multiple PPs and PP-Modules

E.4.2 Exact conformance FAQs / Cheat-sheet

Table E.4 gives a summary of frequently asked questions about the exact conformance case.

Table E.4 — Exact Conformance Summary

PP-Configurations	**Clause**	**Allowed/Required?**
Can be used in multi-assurance – modular PP-Configuration?	Figure 5	No
Can be used in single assurance – modular PP-Configuration?	Figure 5	Yes
Can mix EC with strict/demonstrable conformance types	10.6.1	No
Other EC PPs allowed in EC PP-Configuration		Yes
EC PP		
Optional/Selection-based SFRs in EC PP	12.4.1	Yes
Additional SPD elements associated with optional SFRs		Yes
EC PP claim conformance to another EC PP? (Chained)	10.6.1 10.4.6 10.8.3 B.3.2.2	No
Other EC PPs allowed in EC PP-Configuration		Yes
PP build upon strict or demonstrable PP?		No
Can be used in strict or demonstrable PP-Configuration?		No
States which other EC PPs are “Allowed-with”		Yes
States which other EC PP-Modules are “Allowed-with”	11.2.3.3 d)	Yes
EC PP-Modules		
Optional/Selection-based SFRs in EC PP-Module	11.2.3.3	Yes
EC PP-Module allowed none base PPs	11.2.3.3 d)	Yes
States other EC PPs and PP-Modules are allowed-with	11.2.3.3 d)	Yes
All Allowed-with items also EC	11.2.3.3 d)	Yes
EC functional Packages		
Optional/Selection-based SFRs allowed in EC functional Package		Yes
Functional packages can be augmented in the ST		No
Are claimed in a ST conformance claim	12.2.1 d)	No
EC STs		
Contains the SPD of all EC PPs, and/or PP-Configuration	12.4.3	Yes

components		
Additional or hierarchically higher security requirements?	12.4.4	No
Includes only those selection-based requirements that have been selected	12.4.4	Yes
Can be used with Direct Rationale approach		No

Bibliography

This bibliography contains references to further material and standards useful to the readers of ISO/IEC 15408 (all parts). For undated references the reader is recommended to refer to the latest edition of the referenced document.

ISO/IEC standards and guidance

[1] ISO/IEC 8367, *Information technology — Security techniques — Cryptographic algorithms and security mechanisms conformance testing*

[2] ISO/IEC 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*

[3] ISO/IEC 15446, *Information technology — Security techniques — Guidance for the production of Protection Profiles and ST s*

[4] ISO/IEC TR 18018:2010, *Information technology — Systems and software engineering — Guide for configuration management tool capabilities*

[5] ISO/IEC TR 18031:2011, *Information technology — Security techniques — Random bit generation*

[6] ISO/IEC 19608, *Information technology — Security techniques — Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*

[7] ISO/IEC 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems, and applications*

[8] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[9] ISO/IEC 19791, *Information technology — Security techniques — Security assessment of operational systems*

[10] ISO/IEC 19896-1, *IT Security techniques — Competence requirements for information security testers and evaluators: Part 1: Introduction, concepts, and general requirements*

[11] ISO/IEC 19896-3, *IT Security techniques — Competence requirements for information security testers and evaluators: Part 3: Knowledge, skills, and effectiveness requirements for ISO/IEC 15408 evaluators*

[12] ISO/IEC 20004, *Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045*

[13] DRAFT ISO/IEC TR 22216, *Information technology — Security techniques — Introductory guidance on evaluation for IT security*

Editors' Note:

Note that while in draft, this companion document to 15408/18045 revision 4 aims to provide a useful overview of changes to the ISO revision audience and is updated in step with the ISO/IEC 15408/18045 revision

The editors expect that ISO/IEC 22216 will be published concurrently with this standard

[14] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[15] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[16] ISO/IEC 27034, *Information technology — Security techniques — Application security*

Other standards and guidance

[16] CCDB. *Composite product evaluation for Smart Cards and similar devices,* April 2012, V1.2
Available at http://www.commoncriteriaportal.org/files/supdocs/CCDB-2012-04-001.pdf

Catalogues of PPs and evaluated products

[17] Common Criteria portal: Certified Products, available at http://www.commoncriteriaportal.org/products/

[18] Common Criteria portal: Protection Profiles, available at http://www.commoncriteriaportal.org/pps/

[19] Common Criteria portal: Collaborative Protection Profiles, available at http://www.commoncriteriaportal.org/pps/?cpp=1