COMMITTEE DRAFT **ISO/IEC 2nd CD 15408-1, revision**	Reference document: **SC 27 N18803**
Date: **2019-01-07**	Supersedes document N18700

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 technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for comments by: **2019-03-05** Please submit your comments via the online balloting application by the due date indicated.

ISO/IEC 2nd 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).

2nd CD Consideration

In accordance with Recommendation 14 (see SC 27 N18820 = WG 3 N1610) of the 57th SC 27/WG 3 meeting held in Gjøvik, Norway, 2018-09-30/10-04 the hereby attached document is being circulated for a 8-week 2nd CD letter ballot closing by

2019-03-05

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

No. of pages: 2 + 138

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 N18803

Date: 2018-12-21

ISO/IEC WD 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 exact conformance,
    - The removal of low assurance PPs and the introduction of direct rationale PPs,
    - The introduction of PP-Modules.

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 may 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.

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 are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines 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.

It provides guidelines for using ISO/IEC 15408-4 to derive evaluation methods and activities.

NOTE Such methods and activities may be included in Protection Profiles, Security Targets, or supporting documents.

It provides guidelines for using ISO/IEC 15408-5, pre-defined compliant packages of security functional or assurance requirements in Protection Profiles and Security Targets.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation, evaluation results are described. This document gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation method given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

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/

3.1 Terms and definitions in alphabetical order

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. The editors are working hard on grouping terms according to a hierarchy of concepts, but do not plan to present this until the next draft.

Experts are asked:

1) not to comment current order of terms

2) to contribute to the concept-based order of terms see ISO/IEC 22216, Annex C

While contributing to the Annex C, experts are asked to consider defining concepts as required by ADV_SPM, aligned with current terminology.

Furthermore, editors draw experts' attention to verb functioning as dual-use wording, in particular, these marked as <evaluation verb>. In Editors opinion, they should not exist as vocabulary entries. Instead of which an introductory subclause on specific usage of these word in evaluation context should be created.

Experts are asked to contribute.

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

3.2
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.

3.3

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.

3.4

activity

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

3.5

administrator

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

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

3.6

adverse action

action performed by a threat agent on an asset

3.X

application developer

entity developing an application running on the platform of a Composite TOE

3.7

asset

entity that the owner of the TOE presumably places value upon

3.8

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.

3.9

assurance

grounds for confidence that a TOE meets the SFRs

Editors' Note:

Two definitions ie. assurance package (3.10) and functional package (3.94) should be aligned with 3.126 (package)

3.10

assurance package

named set of security assurance requirements

EXAMPLE "EAL 3".

3.11

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).

3.12
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.

3.13
authentication data
information used to verify the claimed identity of a user

3.14
authorized user
TOE user who may, in accordance with the SFRs, perform an operation

3.15
base component
entity in a composed TOE, which has itself been the subject of an evaluation, providing services and resources to a dependent component

Editors' Note:

The notion of "base component" is used in both composition approaches: "composed evaluation" and "composite evaluation". The proposal is to keep the term component without any particular evaluation status, and use TOE when the component has been or requires evaluation. This is in line with the definition of "component TOE"

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

3.16
Base Protection Profile
Base PP
Protection Profile specified in a PP-Module used as a basis to build a Protection Profile Configuration

3.17
base TOE developer
entity developing the base TOE or sponsoring a base TOE evaluation

Editors' Note

The original definition by JIL is "platform developer". The equivalent term would be "base component".

It is not clear that defining the term "base component developer" is necessary.

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
base TOE
TOE comprising the independent component(s) of a layered composite TOE

3.21
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.

3.22
class
⟨taxonomy⟩ set of ISO/IEC 15408 families that share a common focus

3.23
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.

3.24
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

3.25
complete
property where all necessary parts of an entity have been provided

Note 1 to entry: In terms of documentation, this means that all relevant information is covered in the documentation, at such a level of detail that no further explanation is required at that level of abstraction.

3.26
component
⟨taxonomy⟩ smallest selectable set of elements on which requirements may be based

3.27
component TOE
successfully evaluated TOE that is part of another composed TOE

3.28
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

3.29
composed TOE
TOE comprised solely of two or more components that have been successfully evaluated

3.30
composite evaluation
evaluation of a composite TOE

3.31
composite product
product comprised of two or more components which can be organized in two layers: a layer of independent base component(s) and a layer of dependent components

Note 1 to entry: The composite evaluation can be applied as many times as necessary to a multi-component/multi-layered product, in an incremental approach.

Note 2 to entry: Usually, the layer consisted of base components has already been successfully evaluated.

3.32
composite product evaluation authority
evaluation authority monitoring the evaluation of the composite product

3.33
composite product evaluation sponsor
entity in charge of contracting the composite product evaluation

3.34

composite product evaluator

entity performing the composite product evaluation

3.35

composite product integrator

entity installing the dependent components on the base component(s)

3.36

composite TOE

TOE composed of a superposition of two layers

Note 1 to entry: This definition does not preclude products that use 3 layers, for example that include middleware.

Editors' Note:

The following alternate definition is proposed:

composite TOE = TOE composed of two or more components which can be organized in two layers: a layer of already evaluated autonomous base TOE(s) and a layer of dependent components

3.37

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]

3.38

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.

3.39

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.]

3.40

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

3.41

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

3.42

configuration management output

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

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

3.43

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.

3.44

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.

3.45

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.

3.46

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.

3.47

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

3.48

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.

3.49

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.

3.50

counter

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

3.51

covert channel

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

3.52

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.

3.53

demonstrable conformance

relation between an 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

3.54

demonstrate

<evaluation verb> provide a conclusion gained by an analysis which is less rigorous than a “proof”

3.55

dependency

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

3.56

dependent component

entity in a composed TOE, which is itself the subject of an evaluation, relying on the provision on services by a base component

Editors’ Note:

(see entry “base component”)

The notion of “dependent component” is used in both composition approaches: “composed evaluation” and “composite evaluation”. This definition should be used for “dependent TOE”.

The proposal is to keep the term component without any particular evaluation status, and use TOE when the component has been or requires evaluation. This is in line with the definition of "component TOE"

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

3.57
dependent TOE
entity in a composed TOE which is itself the subject of an evaluation, relying on the provision on services by one or more base components

Note 1 to entry: applies only to the "composed" evaluation approach (not to the composite approach).

3.58
dependent TOE developer
entity developing the dependent TOE of a composed TOE

3.59
describe
<evaluation verb> provide specific details of an entity

3.60
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

3.61
developer
organization responsible for the development of the TOE

3.62
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.

3.63
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.

3.64
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.

3.65
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 Security Objectives for the operational environment

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

Note 2 to entry: Direct rationale is an alternative method for specifying SFRs to the regular method of mapping via the SPD and the set of TOE Security Objectives.

3.66

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

3.67

element

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

3.68

encountered potential vulnerability

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

3.69

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.

3.70

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

3.71

evaluation

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

Editors' Note:

All terms related to 'evaluation' need to be aligned with section 3.8 (set of definitions taken out from ISO/IEC TR 18045). Experts are asked for contributions to this task, additionally see ISO/IEC 22216, Annex C

3.72

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 defined in ISO/IEC 15408-4.

3.73

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 that form an assurance package

3.74

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.

Editors' Note:

The following definitions are proposed to avoid circular definitions for evaluation authority and evaluation scheme:

evaluation authority

body operating an evaluation scheme

Note 1 to entry:

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

3.75
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

3.76
evaluation evidence
item used as a basis for establishing the verdict of an evaluation activity

3.77
evaluation method
set of one or more evaluation activities that are derived from ISO/IEC 18045 work units for application in a specific context

3.78
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 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: Evaluation scheme is usually established by an evaluation authority, which defines the evaluation environment, including criteria and methodology required to conduct IT security evaluations.

3.79
evaluation technical report
ETR
documentation of the overall verdict and its justification, produced by the evaluator, and submitted to an evaluation authority

3.80
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]

3.81
exact conformance
EC
hierarchical relationship between a PP and an ST where all the requirements in the ST are drawn only from the PP

Note 1 to entry: an ST is allowed to claim exact conformance to one or more PPs and/or PP configurations.

3.82
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.

3.83
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.

3.84
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.

3.85
exploitable vulnerability
weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE

3.86
extended security requirement
security requirement developed according to the rules given in ISO/IEC 15408 but that is not specified in any part of ISO/IEC 15408

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

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

3.87
external entity
user
human technical system or one of its components interacting with the TOE from outside of the TOE boundary

3.88
family
⟨taxonomy⟩ set of components that share a similar goal but differ in emphasis or rigour

3.89
formal
expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts

3.90
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.

3.91

functional package

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

3.92

guidance documentation

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

3.93

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

3.94

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.

3.95

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.

3.96

informal

expressed in natural language

3.97

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.

3.98

inter TSF transfer

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

3.99

interaction

general communication-based activity between entities

3.100

interface

means of communication with an entity

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

3.109
life-cycle definition
definition of the life-cycle model

3.110
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]

3.111
evaluation methodology
system of principles, procedures and processes applied to IT security evaluations

3.112
module
TOE-module
small architectural unit that can be characterized in terms of the properties discussed in TSF internals (ADV_INT)

3.113
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

3.114
multi-assurance evaluation
evaluation where the TOE is organized in parts, each part being associated with its own assurance package

3.115
non-bypassability
⟨of the TSF⟩ security architecture property whereby all SFR-related actions are mediated by the TSF

3.116
object
entity in the TOE, that contains or receives information, and upon which subjects perform operations

3.117
observation report
report written by the evaluator requesting a clarification or identifying a problem during the evaluation

3.118
operation
⟨on an ISO/IEC 15408 component⟩ modification or repetition of a component by assignment, iteration, refinement, or selection

3.119
operation
⟨on an object⟩ specific type of action performed by a subject on an object

3.120
operation
usage phase of the TOE including normal usage, administration, and maintenance of the TOE after delivery and preparation

3.121
operational environment
environment in which the TOE is operated, consisting of everything that is outside the TOE boundary

3.122
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.

3.123
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”.

3.124
oversight verdict
statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities

3.125
package
named set of either security assurance requirements or security functional requirements possibly including an SPD and Security Objectives derived from that SPD

Editors' Note:

The definitions "functional or security assurance package" were contributed by experts, but that definition is circular and have been amended by the Editors. Additionally, this definition should be integrated with the two ie. assurance package and functional one.

3.126
policy
set of rules, procedures, and guidelines

3.127
potential vulnerability
suspected, but not confirmed, weakness

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

3.128
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.

3.129
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.

3.130
Protection Profile configuration
PP-Configuration
Protection Profile composed of Base Protection Profile(s) and Protection Profile module(s)

3.131
Protection Profile
PP
implementation-independent statement of security needs for a TOE type

3.132
Protection Profile module
PP-Module
implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles

3.133
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.

3.134
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

3.135
refinement
addition of details to a security component

3.136
report
<evaluation verb> include evaluation results and supporting material in the evaluation technical report or an observation report

3.137
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

3.138
role
pre-defined set of rules establishing the allowed interactions between a user and the TOE

3.139
secret
information that shall be known only to authorized users and/or the TSF in order to enforce a specific SFP

3.140
secure state
state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs

3.141
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.

3.142
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

3.143
security function policy
SFP
set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs

3.144
security objective
statement of an intent to counter identified threats and/or satisfy identified organization security policies and/or assumptions

3.145
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.

3.146

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

3.146a

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

Editors' Note:

The definition of SFR should be split in two, for <general model PPs/STs> and for <direct rationale PPs/STs>.

For the direct rationale case:

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

For the general model:

"security requirement, which contributes to fulfil the TOE's Security Objectives as defined in the general model in a ST or PP

3.146a

security assurance requirement

SAR

security requirement, which refers to the conditions and processes such as specification, design, development, and delivery under which the TOE is developed and configured before being accepted by its final user

Editors' Note:

The definition is unclear (testing is missing, configuration is not a standardized operation). The proposal is to simplify it:

"security requirement, which refers to the conditions and processes for the development and delivery of the TOE. "

3.147

Security Target

ST

implementation-dependent statement of security requirements for a TOE based on a security problem definition

3.148

selection

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

3.149

selection-based Security Functional Requirement

selection-based SFR

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

3.150

semiformal

expressed in a restricted syntax language with defined semantics

3.1.51

SPD-element

threat, organizational security policy, or assumption

Editors' Note:

This term has been introduced as a result of using it in the clauses below in order to make the language more easily understood in the main clauses.

3.152

specify

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

3.153

strict conformance

hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST

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

3.154

sub-activity

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

Note 1 to entry: Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family.

3.155

sub-TSF (TSF part)

notion applied in multi-assurance evaluation to denote a portion of the TSF that provides a well-defined subset of security functionality, which corresponds to a set of SFRs that is closed by dependencies, objectives, and SPD elements

Note 1 to entry: a sub-TSF has the characteristics of a TSF.

Note 2 to entry: a sub-TSF is associated with its own set of SARs/assurance package in a multi-assurance PP-Configuration.

3.156

subject

entity in the TOE that performs operations on objects

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

Editors' Note:

The terms below have been introduced as a result of the action agreed at editing meeting

3.159

time to exposure

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

3.160

TOE resource

anything useable or consumable in the TOE

3.161
TOE security functionality
TSF
combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the correct enforcement of the SFRs

Editors' Note:

This definition needs adaptation to meet the needs of the sub-TSF notion (see 3.159)

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
perform an informal correspondence analysis in both directions between two entities with only a minimal level of rigour

3.164
trace
<evaluation verb> simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second

3.165
transfer outside of the TOE
TSF-mediated communication of data to entities not under the control of the TSF

3.166
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.

3.167
trusted channel
means by which a TSF and another trusted IT product can communicate with necessary confidence

3.168
trusted IT product
IT product, other than the TOE, which has its security functional requirements administratively coordinated with the TOE and which is assumed to enforce its security functional requirements correctly

EXAMPLE An IT product that has been separately evaluated.

Editor s' Note:

A trusted IT product has not necessarily been CC evaluated. Since the term "security functional requirements" has a specific meaning in CC, the definition must be reworked. The proposal is the following:

trusted IT product

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

EXAMPLE: An IT product that has been separately evaluated. CC evaluation is not mandated.

If no comments are received on this, the editors' proposal will be accepted and presented in the next draft.

3.169

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.

3.170

TSF data

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

3.171

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

3.172

TSF self-protection

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

3.173

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.

3.174

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.

3.175

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.

3.176

vulnerability

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

3.177

window of opportunity

period of time that an attacker has access to the TOE

3.178

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.

3.2 Hierarchy of concepts

Editors' Note:

Under development by the Editors

Note that ISO have stated that the terms must be presented using a hierarchy of concepts, and not in alphabetical order.

4 Abbreviated terms

Editors' Note:

Editors have removed abbreviations from the list that are presented in the clause 3 definitions

Editors still need to check all parts of 15408 and 18045 for abbreviations and update this list accordingly.

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

AP	Assurance Package
API	Application Programming Interface
CAP	Composed Assurance Package
DAC	Discretionary Access Control
DPA	Differential Power Analysis
DRBG	Deterministic Random Bit Generator
EA	Evaluation Activity
EMS	Electromagnetic spectrum
GUI	Graphical User Interface
HSM	Hardware Security Module
IC	Integrated Circuit
IOCTL	Input Output Control
IP	Internet Protocol
IT	Information Technology
MB	Mega Byte
OR	Observation Report
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SPA	Simple Power Analysis
TCP	Transmission Control Protocol

VPN	Virtual Private Network

5 Overview

5.1 General

This clause 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 3.1.

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. For example, ISO/IEC 18045 provides the baseline methodology for IT security evaluations performed in accordance with ISO/IEC 15408 (all parts). 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.

5.3 Target audience of ISO/IEC 15408 (all parts)

5.3.1 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 the following sub-clauses.

5.3.2 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 Protection Profile (PP), in which to express their security requirements in an unambiguous manner.

5.3.3 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 be based on one or more PPs to show that the ST conforms to 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.

5.3.4 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.

5.3.5 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 12.

5.3.6 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.

1539 Table 1 presents, for each of the audience groupings, how the parts of ISO/IEC 15408 are of interest.

1540 **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-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-Configurations, STs and composition. Shall use for the development of security specifications for TOEs, packages, PP-Modules and PP-Configurations.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Configurations, STs and composition. Shall use for the development of security specifications for packages, PPs and PP-Configurations.	Should use for background information, reference purposes, and for guidance on the structure of PPs, 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-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 PPs, PP-Modules and PP-Configurations Shall use when developing STs May use when formulating security functionality for IT products.	Shall use for when formulating statements of security functional components in PPs and PP-Configurations.	Shall use for reference when evaluating security functional components given in PPs and PP-Configurations or security functional requirements in STs.	May use for reference when reviewing security functional components given in PPs and PP-Configurations 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 PPs, PP-Modules and PP-Configurations. Shall use when developing STs May use when formulating or improving development processes.	Shall use for when formulating statements of security assurance components in PPs and PP-Configurations.	Shall use for reference when evaluating security functional components given in PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.	May use for reference when reviewing security functional components given in PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.
Part 4	Should use for reference and background information of any evaluation methods and activities derived from ISO/IEC 18045 applied to the evaluation of TOEs used in their risk-environment.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities derived from ISO/IEC 18045.	Shall use for reference purposes and for guidance in the structure of evaluation methods and activities derived from ISO/IEC 18045.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities derived from ISO/IEC 18045. Shall use when formulating specific evaluation methods and activities.	May use for reference purposes and for guidance in the structure of evaluation methods and activities derived from ISO/IEC 18045.
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 when developing PPs claiming conformance to pre-defined packages of security requirements.	Shall use for reference when evaluating PPs 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.

5.4 The Target of Evaluation (TOE)

5.4.1 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.

Further information on the TOE is given in Annex D.

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 large interface and/or number of components, multiple manufacturing/integration phases, field upgradeable products such as:

- A Local Area Network 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 Modules (HSM).

5.4.2 TOE Boundaries

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

A TOE may be a complete IT product (or products), a part of an IT product, or made up of various components. The Security Target 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*.

5.4.3 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.

5.4.4 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, such 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 may 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 of the general IT product, that may allow many configurations, and the guidance of 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 of 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.

5.4.5 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 Security Target 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.

EXAMPLE 1

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.

EXAMPLE 2

An example of an organizational security policy is a policy determining the intended usage of the TOE.

An example of a security objective for the operational environment is organizational key management for TOE cryptographic operation.

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

5.5 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 by completing security components provided in ISO/IEC 15408-3 is explained in 6.3.4.

The requirements and recommendations for the core constructs of packages, PPs, PP-Configurations and Security Targets, are explained in 8, 9, 10 and 11.

The requirements and recommendations for evaluation and evaluation results for TOEs, STs, PPs and PP-Configurations are found in 12.

Finally, the topic of composing assurance is found in 13.

6 General model

6.1 Background

This clause 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, which users of this document are obliged to consult, expand on the use of these concepts, and assume that the approach described 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. This clause assumes that the reader has knowledge of IT security and does not propose 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.

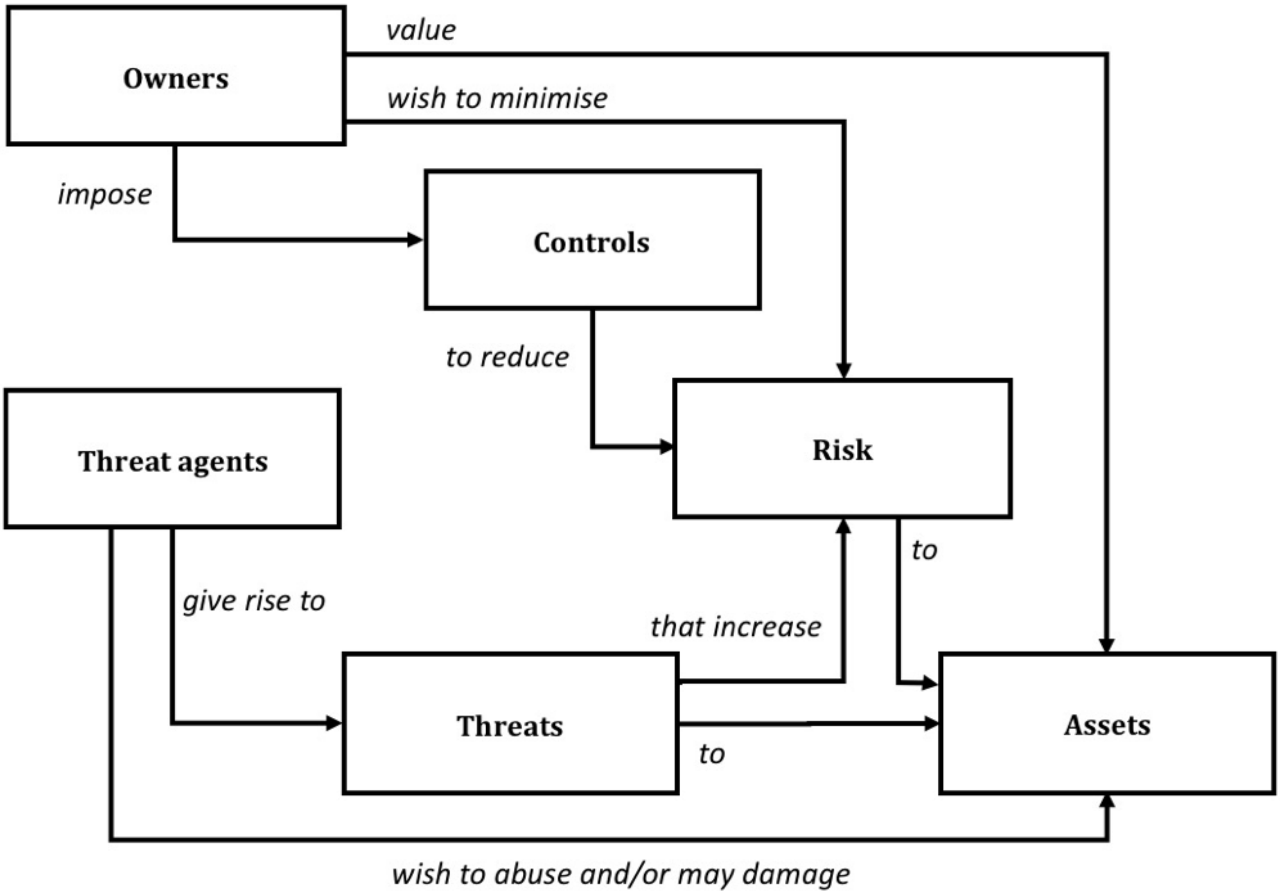


Figure 1 — Security concepts and relationships

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

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 potential for impairment of the assets such that the value of the assets to the owners would be reduced. 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 section.

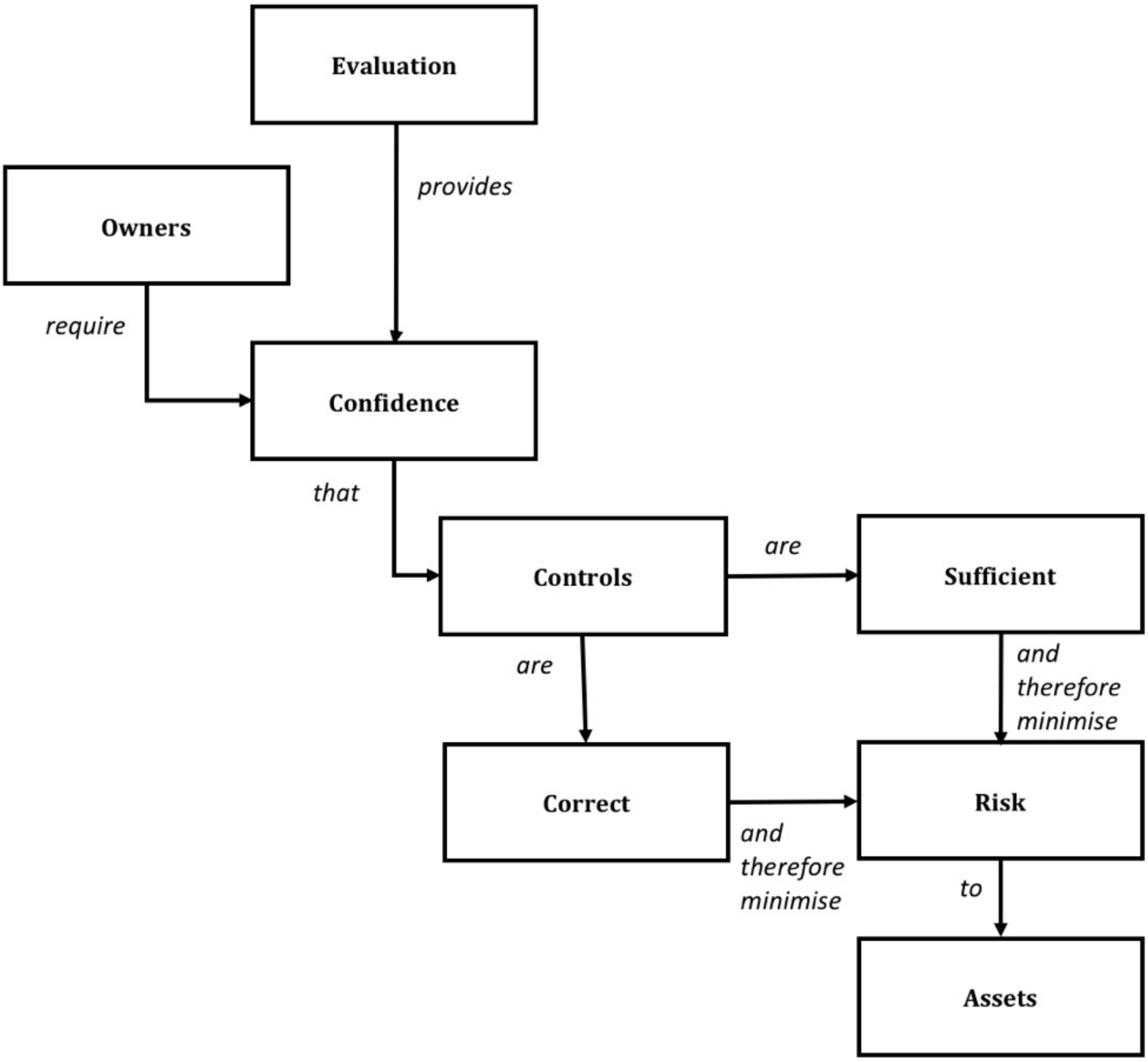


Figure 2 — Evaluation concepts and relationships

In an evaluation, the sufficiency of the security controls is analysed through a construct called the Security Target. In this subclause a simplified view on this construct is provided: a more detailed and complete description is found in Annex "A".

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, four constructs: STs, packages, Protection Profiles (PPs), and PP-Configurations are provided in the paradigm.

STs, PP-Modules, PPs and PP-Configurations shall specify a conformance type in support of the goals of PP and PP-Configuration authors.

This document specifies three conformance types; demonstrable, strict, and exact. Conformance types are described in detail in Annex F.

As this evaluation may need to meet varying assurance needs, the standard provides different tools, from predefined assurance levels (ISO/IEC 15408-5) to well-formed assurance components and packages (ISO/IEC 15408-3) and a companion evaluation methodology (ISO/IEC 18045), as well as a mechanism to define extended assurance components (ISO/IEC 15408-1).

6.3.2 Security Target

6.3.2.1 General

In this subclause a simplified view of the Security Target construct is provided: a more detailed and complete description is found in Annex D.

Core requirements for STs are found in clause 11 . ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs undergoing evaluation.

The Security Target (ST) is a key document that begins with describing the assets and the threats to those assets. The Security Target then describes the security controls (in the form of Security Objectives) and demonstrates that these security controls are sufficient to counter these threats: if the security controls do what they claim to do, the threats are countered.

The Security Target then divides these security controls in two groups:

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.

For the TOE (the IT security controls whose correctness will be assessed during the evaluation), the Security Target requires a further detailing of the Security Objectives for the TOE in Security Functional Requirements (SFRs). These SFRs are formulated in a standardized language (described in ISO/IEC 15408-2) to ensure exactness and facilitate comparability.

In summary, the Security Target 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 takes an alternative approach to specifying the SFR's is appropriate these STs are known as "Direct Rationale" STs and are explained in the clauses below.

A Security Target may be defined as standalone document for a specific TOE or may comply with one or more preexistent Protection Profile(s) or PP-Configurations and thereby reuse and specialize their generic definitions to the specific TOE. In the second case, the ST shall meet the conformance conditions given in the PPs.

The PP constructs and the related concepts of PP-Configurations are introduced in 9 and 10.

6.3.2.2 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 Security Target 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 exactness 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.

6.3.2.3 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 shall 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 General

Often sets of security requirements are commonly used, ISO/IEC 15408(all parts) also provides a mechanism for identifying sets of security requirements addressing particular TOE types and that share similar security problems. This document introduces three constructs for attaining this, packages, Protection Profiles and PP-Configurations. These are introduced below.

6.3.3.2 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 he conditions and processes such as specification, design, development, testing and delivery under which the TOE is developed and configured.

Core requirements for packages are found in 8, Annex A provides additional information about packages and 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.

6.3.3.3 Protection Profiles (PPs)

Protection Profiles (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 are found in 8.3, Annex B provides additional information about PPs and ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for PPs undergoing evaluation.

6.3.3.4 PP-Configurations

PP-Configurations build upon the concept of PP; introducing the notion of PP-Module which supplements one or more Base PP(s).

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

This concept is described in more detail in 10 and further guidance is provided in 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. The PP-Configuration describes which Base PPs and which PP-Modules are combined to instantiate an implied PP that includes the requirements given in the PP-Modules.

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

- Operating system PP,
- Operating system with Bluetooth,
- Operating system with Wireless client,
- Operating system with Bluetooth and wireless client.

- Mobile device,
- Mobile device with Bluetooth,
- Mobile device with Wireless client,
- Mobile device with Bluetooth and wireless client.

Note that in practice, STs instantiate the PP implied by the PP-Configuration. The implied PP may not be written.

6.3.4 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, while enforcing a global set of SARs/assurance package 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 Security Target 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 TOE 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 part can be associated with a subset of TOE components, for instance a TPM, a cryptographic library or a card reader.

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

- A device 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 device where some parts of the security functionality do not require the same high evaluation assurance as other more exposed parts of the device, for instance an internet gateway with support for personal area network protocols.
- A family of devices where some security functionality is shared across all the devices 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. The multi-assurance paradigm allows to combine the shared functionality and the use-case dependent functionality in as many multi-assurance PP-Configurations as needed.
- Multi-assurance is eventually relevant for products claiming conformance to different Protection Profiles 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 TSF part as usual since TSF parts are closed by dependencies, objectives, and SPD. The vulnerability analysis of each TSF part complies with the current definition of AVA_VAN which considers the whole TOE as the attack surface.

7 Tailoring security requirements

7.1 General

Security Targets specify the security requirements applicable to a TOE. Security functional requirements, and security assurance requirements may be drawn from security components which are a template for security requirements. The process of deriving a security requirement from a security component involves tailoring the components for the specific ST and is known as “completion”.

7.2 Operations

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

NOTE It is important to understand that a PP is intended to describe a TOE type whereas an ST describes a specific TOE. A PP can either be used as the basis for another PP, or as a basis for an ST.

When using operations, the PP/ST 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 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 PP/ST 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 annexes shall be consulted in order to determine when “None” would be a valid completion.

7.2.1 The iteration operation

The iteration operation may be performed on every component. The PP/ST 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(AES data encryption/decryption) and FCS.COP.1(Signature generation) is preferable to FCS.COP.1(a) and FCS.COP.1(b)

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.

7.2.2 The assignment operation

An assignment operation occurs where a given component contains an element with a parameter that may be set by the PP/ST 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 contains an assignment, a PP author shall do one of four things:

a) leave the assignment uncompleted;

EXAMPLE 1
The PP author could include FIA_AFL.1.2 in the PP.
"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 PP author could include FIA_AFL.1.2 "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 PP author could include FIA_AFL.1.1 in the PP
"The TSF shall detect when [assignment: positive integer between 4 and 9] unsuccessful authentication attempts occur ..."

In this case, the ST author could complete FIA_AFL.1.1 thus:
"The TSF shall detect when 7 unsuccessful authentication attempts occur ..."

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

EXAMPLE 4
The PP author could include FIA_AFL.1.2 in the PP
"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."

Whenever an element in an ST contains an assignment, an ST author shall complete that assignment, as indicated in b) above. Options a), c) and d) are not allowed for STs.

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, a PP author should provide a description of the set from which the elements of the set can 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.

7.2.3 The selection operation

7.2.3.1 General

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

Whenever an element in a PP contains a selection, the PP 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 contains a selection, an 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.

7.2.3.2 Selection-based security functional components and SFRs

A PP 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. The related selection-based components and/or SFRs shall be included in a PP/ST if:

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

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

EXAMPLE

Where the selection-based SFRs are included in an annex of the PP.

For the case that a PP author needs to leave a selection operation uncompleted, the PP 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 PP/ST 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/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 PP author shall remove any selection-based components and/or SFRs from the list that corresponds to the choices removed from the selection.

7.2.4 The refinement operation

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

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 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.

The only exception to this rule is that a PP/ST 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 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.

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

NOTE 1 A special case of refinement is an editorial refinement, where a small change is 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.

NOTE 2 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.

7.3 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. However, this does not preclude extended functional components having dependencies on assurance components or vice versa.

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 and 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 or ST contains a security requirement based on component A, the PP 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/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.).

7.4 Extended components

In ISO/IEC 15408, 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,

b) there are third party requirements that cannot be translated to SARs,

> EXAMPLE
>
> Laws and/or regulation regarding the evaluation of cryptography.

c) a security objective can be translated to SFRs, but only with great difficulty and/or complexity based on components in ISO/IEC 15408-2.

In these cases, the PP/ST 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 PP/ST author can 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.4.5 and in E.4.

8 Packages

8.1 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. Packages may be used in the construction of larger packages, PPs, PP-Modules and STs.

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

NOTE 3 Assurance packages cannot be used in the constriction of PP-Modules.

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

Further information on packages is given in Annex A.

8.2 Package types

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.

8.2.1 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 a security problem definition (SPD) or Security Objectives.

Assurance packages may be used within PPs and STs.

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.

8.2.2 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 a security problem definition (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

If a PP contains packages A, B, C and D, and if the following holds: Functional package A is included; functional package C depends on functional package B; and functional package D has no dependencies, then an ST can claim conformance to the PP in the following cases:

- the ST only uses functional package A from the PP
- the ST uses functional packages A and B
- the ST uses functional packages A, B and C
- the ST uses functional packages A and D
- the ST uses functional packages A, B, C, and D

The following combinations would not be allowed:

– the ST uses functional packages A and C since functional package C has a dependency on functional package B, which must be included if functional package C is claimed.

8.3 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 or ST that includes the package. This means that it is the responsibility of the PP or ST 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 7.3.

8.4 Evaluation method(s) and/or activities

Packages may include evaluation methods and/or activities that have been derived from ISO/IEC 18045 in accordance with the framework given in ISO/IEC 15408-4. Evaluation methods and/or activities that are associated with the package shall be referenced in the application notes section of the package. Evaluation methods and/or activities may be specified in the package associated with the relevant security requirements or provided in a separate document.

9 Protection Profiles

9.1 General

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

- as a template for many different STs to be used in different TOE evaluations;
- as a template for other PPs in order to further refine the TOE type.

NOTE A Base PP is a PP used in the PP-Configuration concept described in 10.

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

9.2 General conformance claims and conformance statements made by PPs

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 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.
- **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;

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, PP-Modules 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, the ST shall conform to the PP in an exact manner;
- **Strict conformance**: If the PP states that strict conformance is required, the PP/ST shall conform to the PP in either an exact or a strict manner;
- **Demonstrable conformance**: If the PP states that demonstrable conformance is required, the PP/ST shall conform to the PP in either an exact, strict, or demonstrable manner.

  NOTE 1 Restating this in other words, a PP/ST is only allowed to conform to a PP in a demonstrable manner if the PP explicitly allows this.

g) may also include a reference to any evaluation method(s) and activities derived from ISO/IEC 18045 in accordance with the framework given in ISO/IEC 15408-4.

- If evaluation methods and evaluation activities derived from ISO/IEC 18045 as described in ISO/IEC 15408-4 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 2 STs based on a PP that references evaluation methods and/or activities derived from ISO/IEC 15408-4 do not need to reproduce the text of the evaluation methods and/or activities. See 11.2.1 g)

NOTE 3 Either an 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.

9.2.1 Security problem definition

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

- all TOEs that meet the security problem definition in the PP/ST also meet the security problem definition in the PP;
- all operational environments that meet the security problem definition in the PP also meet the security problem definition in the PP/ST.

9.2.2 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.

9.3 Additional requirements for PPs common to strict and demonstrable conformance

9.3.1 Conformance claims and statements in the strict and demonstrable conformance cases

9.3.1.1 General

If an 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.

An 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.

9.3.2 Assurance requirements

A standard PP of demonstrable or strict conformance which complies with ISO/IEC 15408-3 (possibly extended) must define the set of SARs/assurance package that applies to the entire TOE.

- If the set of SARs/assurance package is an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference, then the same name should be used.

A PP may define a distinctive name for the sets of SARs/assurance packages that are globally and partially applicable.

9.3.3 Additional requirements specific to the strict conformance case

9.3.3.1 Requirements for the SPD in the strict conformance case

The PP/ST shall contain the security problem definition 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;

9.3.3.2 Requirements for the Security Objectives in the strict conformance case

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.

9.3.3.3 Requirements for the security requirements in the strict conformance case

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.

9.3.4 Additional requirements specific to the demonstrable conformance case

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.

9.4 Additional requirements for PPs with an exact conformance statement

9.4.1 General

Exact conformance is used to allow a Protection Profile (PP) author to control what an ST can 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 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. An ST (or PP-Module) can then include these optional SFRs (and any required SPD elements) in its set of requirements while maintaining its exact conformance claim.

A standard PP with exact conformance type shall not build upon any other PPs. A PP-Configuration with exact conformance shall not build upon PPs or PP-Modules with strict or demonstrable conformance type.

NOTE 1: Once a PP has been given exact conformance type, then it will never be possible to use them to build PPs with a different conformance claim. Additionally, it is impossible to claim conformance to both a strict conformance PP and an exact conformance PP, since it would mean adding requirements on top of the exact conformance PP, which explicitly prohibits this operation.

In the "simple" case where an 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, Objectives, SFRs, and SARs can be demonstrated during evaluation without the need to seek PP author input.

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

EXAMPLE

A complex case might be if a PP-Module wishes to the use a PP as its Base PP, or if an 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.

9.4.2 Conformance claims and statements for PPs in the exact conformance case

If a PP requires exact conformance in its conformance statement then

a) the PP shall state which other PPs, base PPs, and PP-Modules are allowed to be combined with that PP, specifying which of these requirement packages are allowed to be claimed in conjunction with the PP by an ST;

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

c) all of the additional PPs, base PPs, and PP-Modules shall identify the PP in their respective conformance statements.

9.5 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 can be found in Annex A.

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 an 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.

9.6 Conformance statements and claims in the case of multiple PPs

9.6.1 General

ISO/IEC 15408 (all parts) allows both STs and PPs to claim conformance to multiple PPs. The case for an ST claiming conformance to multiple PPs is covered in 11. This subclause, 9.6 covers the case where a PP claims conformance to multiple PPs.

9.6.2 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 a PP on Smart Cards for Public Transport based on the Smart Card PP and a PP on Applet Loading. Finally, a developer could then construct an ST based on these Smart Cards for Public Transport PP.

9.6.3 Where exact conformance is specified

A PP shall not claim exact conformance to another PP or combination of PPs. The same effect may be achieved by creating PP-Configurations, where PP-Modules are used to specify additional functionality to one or more Base PPs.

10 PP-Configurations

10.1 General

To allow the definition of Protection Profiles that address a TOE's optional security features, this subclause introduces the concept of PPs constructed in a modular technique using three constructs: PP-Modules, Base PPs and PP-Configurations, and describes the way in which they may be used.

10.2 PP-Modules

10.2.1 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.

NOTE 1 In a Direct Rationale PP-Module, Security Objectives for the TOE are not included.

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.

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.

10.2.2 Requirements for PP-Modules

10.2.2.1 General

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

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

A PP-Module shall refer to a set of one or more Base PP(s), which constitutes the basis of the PP-Module. The PP-Module may refer to alternative sets of Base PPs. A PP-Module may refer to one or more Base PP-Modules as well, provided all their Base PPs are included.

A PP-Module may specify a particular TOE type and shall specify additional security functional requirements. A PP-Module may introduce new SPD-elements to the Base PPs and may also refine or interpret some of the SPD-elements of the Base PPs.

NOTE 1 In a Direct Rationale PP-Module, Security Objectives for the TOE are not included.

If the PP-Module refers to more than one Base PP, the set of Base PPs shall be identified in the PP-Module's configuration statement using "and" and "or" statements as described in B.13, in order to identify if they have to be used simultaneously for the evaluation and usage of the PP-Module.

NOTE 2 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 mandatory Base PPs.

A PP-Module that inherits exact conformance in its conformance statement is allowed to define optional SFRs and any SDP elements that are required to support these SFRs. An ST can then include these optional SFRs (and any required SPD elements) in its set of requirements (when claiming conformance to a PP-Configuration that includes the PP-Module) while maintaining its exact conformance claim.

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

Further information on PP-Modules is given in B.2.11.

10.2.2.2 PP-Module 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;

d) In the case of exact conformance, the Conformance Statement:

- shall state which other PPs (that are not in the PP-Module's set of Base-PPs), and PP-Modules are allowed to be used in PP-Configuration with that PP-Module;
- all of the additional PPs and PP-Modules referenced shall also require exact conformance; and
- the Base PPs for the PP-Module and all of the additional (non-Base) PPs and PP-Modules shall identify the PP-Module in their respective conformance statements.

NOTE 1 Conformance claims for security assurance packages are inherited from the PP-Module's Base PP(s).

NOTE 2 The conformance type; i.e. exact, strict, or demonstrable, is inherited from the PP-Module's Base PP(s).

NOTE 3 Base PPs for the PP-Module do not need to be specified in the PP-Modules' conformance statement.

A PP-Module must declare its **conformance type,** which must be one of demonstrable, strict, or exact:

- For demonstrable and strict conformance, there is no restriction on the conformance type of the PP-Module's base PPs/PP-Modules. The combination of demonstrable and strict conformance must be validated in the PP-Configuration evaluation.
- The combination of exact conformance with other types of conformance is not allowed.
- For exact conformance, the base PPs/PP-Modules must all declare exact conformance type.

NOTE 4 Such explicit declaration of demonstrable or strict conformance allows sponsors to make the most appropriate statement in each PP-Module.

10.2.2.3 PP-Module assurance requirements

A PP-Module of demonstrable or strict conformance must define the set of SARs/assurance package that applies to the TSF that is introduced in the PP-Module:

- If the set of SARs/assurance package is an (augmented) predefined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference, then the same name should be used.

A PP-Module may define a distinctive name for the sets of SARs/assurance packages that are globally and partially applicable.

A PP-Module of demonstrable or strict conformance must provide an assurance **rationale** that justifies:

- the consistency of the set of SARs/assurance package with regard to the threat model as defined in the SPD of the PP-Module,
- the consistency of the set of SARs/assurance package with all the sets of SARs/assurance package(s) defined in the base PPs/PP-Modules.

NOTE The PP-Module assurance rationale contributes to ensuring that the set of SARs/assurance package 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).

> Example
>
> The assurance rationale may explain, for instance, the relationship with predefined EALs.

For more information on the conformance statements and conformance claims for PP-Modules, see Annex B.

10.3 PP-Configurations

10.3.1 General

A PP-Configuration is a set of meta-data giving the specification for the construction of a PP using the concepts of Base PP, PP-Modules and a PP-Configuration. A PP-Configuration contains no SPD, Security Objectives, or security requirements.

A PP-Configuration is a way to build a PP out of a set of PPs and PP-Modules.

NOTE A Base PP is a PP that is intended to be used in combination with PP-Modules.

10.3.2 Requirements for a PP-Configuration

10.3.2.1 General

A PP-Configuration:

- may be used in context with the Direct Rationale approach described in B.2.10 and C.1.3. 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;
- 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 must define the **components list** that uniquely identifies all the PPs and PP-Modules that compose the PP-Configuration. A PP-Configuration must contain two or more components and one of the components must be a PP.

A PP-Configuration must define the TOE and its organization in terms of the sub-TSFs defined in its PPs and PP-Modules. A PP-Configuration contains exactly the SPD, security objectives, and SFRs defined in its PPs/PP-Modules; the specification of any additional element must be done through the PPs/PP-Modules.

NOTE 2 In the single-assurance evaluation approach, the sub-TSF organization is an option (i.e. it is acceptable to define one sub-TSF), which may facilitate the understanding of the TSF and possibility definition of the evaluation strategy. However, it does not impact the developer or evaluator activities (in the standard case where the PP-Configuration complies with ISO 15408-3 all the assurance requirements apply to the entire TOE and TSF).

NOTE 3 In the multi-assurance evaluation approach, the sub-TSF organization is mandatory. It allows ensuring that the different sets of SARs/assurance packages linked to those sub-TSFs are consistent and to apply the assurance requirements as required by each PP/PP-Module.

NOTE 4 For the simplest multi-assurance PP-Configuration, that is, for a PP-Configuration containing one PP and one PP-Module with different sets of SARs/assurance packages, the TSF organization is as follows: the global 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.

10.3.2.2 PP-Configuration components statement

A PP-Configuration carries a unique reference and

- shall identify all the components of the PP-Configuration in a components statement. The components statement shall contain two or more components, at least one of which is a PP.

  NOTE 1 These components include the selected Base PP(s), PP-Module(s) and any other PPs.

  NOTE 2 The components statement is further described in C.2.1.2

- shall not claim exact conformance to another PP-Configuration

  NOTE 3 If this is desired, the effect can be achieved by directly including all components in one PP-Configuration in the other PP-Configuration directly, where exact conformance can be checked and maintained.

- shall include the Base PP(s) of all the PP-Modules included in the PP-Configuration. If the PP-Module defines alternative sets of Base PPs then only one of these sets shall be used in a PP-Configuration;

– may select more PPs than the Base PPs of the PP-Modules;

NOTE 4 An instantiated PP-Configuration is analogous to a PP that includes all the SPD-elements from the Base PPs, the PP-Modules and any other PPs specified.

10.3.2.3 PP-Configuration 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 provide a **conformance statement** applicable to the ST/PPs that claim conformance to the PP-Configuration, as one of **exact, strict, or demonstrable**, that meet the conformance statements of the PPs and Base PP(s) in the components statement;

A PP-Configuration must declare the list of conformance types, which is inherited from the conformance types of its components (demonstrable, strict, or exact):

- A PP-Configuration where all its components share one conformance type must declare the same conformance type, i.e. demonstrable, strict, or exact conformance.
- Otherwise, the PP-Configuration must provide the list of demonstrable and strict conformance types inherited from each of its components. The compatibility of demonstrable and strict conformance must be validated in the ST evaluation.
- The combination of exact conformance with other types of conformance is not allowed.

10.3.2.4 PP-Configuration assurance requirements

A PP-Configuration consisting of demonstrable and/or strict conformance components must define the applicable SARs/assurance packages:

- The global set of SARs/assurance package that applies to the entire TOE. This can be an (augmented) predefined EAL (EAL1 to EAL7), an (augmented) assurance package defined in an applicable external reference or a set of SARs/assurance package that is defined within the PP-Configuration itself.
- For each TSF part, the applicable set of SARs/assurance package. This can be the same set of SARs/assurance package inherited from the PP or PP-Module defining the TSF part, or a larger set (augmentation) which requires the provision of a rationale.

A PP-Configuration may define a distinctive name for the sets of SARs/assurance packages that are globally and partially applicable.

A PP-Configuration consisting of demonstrable and/or strict conformance components must provide an assurance rationale for:

- the consistency of the global set of SARs/assurance package with regard to the threat models as defined in the SPDs of the component PPs and PP-Modules, and
- the consistency of the global set of SARs/assurance package and all the sets of SARs/assurance packages for the TOE parts with each other.

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/assurance packages that are different from predefined EALs and/or that contain extended SARs.

NOTE 2 In most cases, the global set of SARs/assurance package can be built as the common denominator of the sets of SARs/assurance packages that apply to the TSF parts. However, as it is the case with Security Targets in the general model, the PP-Configuration can declare additional or higher SARs than the common denominator. The evaluation of the PP-Configuration will ensure the consistency of the claim, similar to the general approach for compliance with two or more PPs defining different sets of SARs/assurance packages, and similar to the approach for multi-assurance Security Targets which can extend the sets of SARs/assurance packages defined in the associated PP-Configuration.

NOTE 3 The PP-Configuration cannot claim less assurance requirements as the global set of SARs/assurance package than those contained in the common denominator of SARs/assurance packages that apply to all the TSF parts.

NOTE 4 The PP-Configuration assurance rationale contributes to ensuring that the multiple sets of SARs/assurance packages do not undermine the security expected for the assets that are shared between the PPs and PP-Modules that compose the PP-Configuration. The PP-Configuration assurance rationale should rely on and/or reuse the PP-Modules' assurance rationales.

Figure 3 shows an example of multi-assurance PP-Configuration with one standard PP A and two PP-Modules X and Y The common denominator of the sets of SARs defined in A, X and Y is SARC, which has been chosen as global set of SARs for the entire TOE (the rules allow to augment this set). The multiple sets of SARs applicable to the sub-TSFs defined in A, X and Y are unchanged as well.

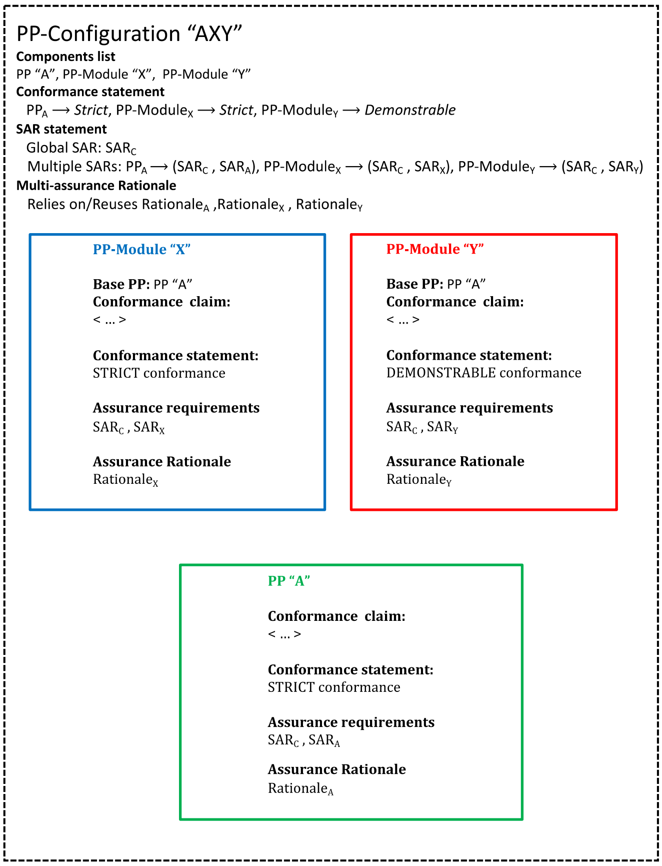


Figure 3 — Example of multi-assurance PP-configuration

10.3.2.5 PP-Configuration conformance statement in the exact conformance case

In the case that a PP-Configuration contains a PP or Base PP with an exact conformance statement then:

a) all PPs and Base PPs in the PP-configuration shall require exact conformance;

b) all PP-Configuration components shall allow each other to be allowed to be used together in their respective conformance statements.

NOTE 1 In the case of Base PPs for PP-Modules this is implicit. In all other cases this allowance must be explicitly stated.

NOTE 2 There are implications for conformance statements in PP-Modules in the exact conformance case that are covered in section C.1.2.3.

NOTE 3 Guidance on the conformance statement is given in B.5.

10.3.3 PP-Configuration SAR statement

- shall provide a SAR statement specifying the applicable set of assurance components or requirements.

> EXAMPLE
>
> A pre-defined EAL package from ISO/IEC 15408-5 or another assurance package.

11 Security Targets

11.1 General

An 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 by the TSF, the security objectives of the TOE, 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 that describe a security problem and security requirements for a TOE type that is relevant to the specific TOE.

An ST is typically produced by a developer and the audience for the ST includes evaluators, certifying bodies and end users of the evaluated TOE.

Further information about STs is found in Annex D.

11.2 Conformance claims

11.2.1 ST Conformance claims

The conformance claims of an 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** – An 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 –** An 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 an 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** – An 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** – An 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 an ST.

Packages to which conformance is claimed in PPs or PP-Configurations shall not be claimed by STs that claim conformance to those PPs or PP-Configurations.

NOTE 2 For exact conformance, any packages included are specified in the PPs or via a PP-Configuration. i.e. in the exact conformance case packages are inherited.

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

- **Package name Conformant** - An 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** – An 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;

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:

- An ST may claim conformance with one or more PP-Configurations when the conformance statement for the PP-Configuration is strict or demonstrable
- An ST shall not claim conformance to more than one PP-Configuration when the conformance statement is exact.
- A Direct Rationale ST shall only claim conformance to a PP-Configuration if that PP-Configuration uses the Direct Rationale approach.

g) If evaluation methods and/or evaluation activities are identified in the conformance statement of a PP or in the conformance statements of PP-Configuration components 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 based on a PP or PP-Configuration component that reference evaluation methods and/or activities derived from ISO/IEC 18045 in accordance with ISO/IEC 15408-4 do not need to reproduce the text of the evaluation methods and/or activities within the ST.

Evaluation methods and/or evaluation activities not included in a PP or PP-Configuration claimed by the ST shall not be included in an ST.

For more information on the conformance statements for STs see Annex D.

For more information on conformance types see Annex F.

11.2.2 Additional requirements for the SPD in the exact conformance case

An ST claiming exact conformance:

- shall contain the SPD of all PPs to which it is claiming exact conformance, including all SPD elements.

- shall not include any SPD-elements that are not present in the PPs to which it is claiming exact conformance.

NOTE An instantiated PP-Configuration can also be viewed as a PP. Hence any SPD found in PP-Modules and packages included in a PP-Configuration will be found in the instantiated PP-Configuration. See 10.3.

11.2.3 Additional requirements for the Security Objectives in the exact conformance case

An 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 An instantiated PP-Configuration can also be viewed as a PP that contains the Security Objectives found in the PP-Configuration components

11.2.4 Additional requirements for the security requirements in the exact conformance case

An ST shall contain all the SARs present in the PPs, and all the SFRs present in the PPs and PP-Modules, with the following exception:

- 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.

NOTE 1 This means that PP/ST authors cannot include additional or hierarchically higher security requirements.

NOTE 2 See 7.2.3.2and B.2.7 for further information in regard to selection-based SFRs.

NOTE 3 See Annex F for further information on PP conformance.

11.3 Multi-assurance Security Targets

A multi-assurance Security Target must organize the TSF in parts and claim a specific set of SARs/assurance package for each of the parts and a global set of SARs/assurance package for the entire TOE: this is achieved exclusively through the conformance to a multi-assurance PP-Configuration which defines the parts and the set of SARs/assurance packages.

A multi-assurance Security Target 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 standard 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/assurance packages as defined in the original PPs/PP-Modules.

A multi-assurance Security Target may claim the sets of SARs/assurance packages defined in the PP-Configuration, or may provide a rationale to claim “augmented” sets of SARs/assurance packages, similar to Security Targets in the general model.

NOTE In order to conform with two or more PPs that define different sets of SARs/assurance packages, a multi-assurance PP-Configuration composed of the PPs must be defined and claimed by the Security Target.

11.4 Using PP-Configurations in Security Targets

11.4.1 General

PP-Modules are used to build specific PP-Configurations on top of one or more Base PPs. Hence, PP-Modules shall only be used by STs as a constituent part of any claimed PP-Configurations.

PP-Configurations may be used by STs in a manner similar to that employed by Protection Profiles. An ST may claim conformity to a PP-Configuration. See 12.3 for a discussion of the evaluation of PP-Configurations.

NOTE 1 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 Security Target, prior to evaluating the ST conformance claim.

A Security Target may claim conformance with one or more PPs and PP-Configurations, thereby complying with their conformance types. The consistency of the combination of demonstrable and strict conformance must be validated in the ST evaluation.

The combination of exact conformance with other conformance types is not allowed, i.e. an ST cannot claim conformance to an exact PP/PP-Configuration and to a demonstrable or strict PP/PP-Configuration.

A Security Target that claims conformance with ISO/IEC 15408-3 (possibly extended) must define:

— the **global set of SARs/assurance package** that applies to the entire TOE. This can be an (augmented) predefined EAL (EAL1 to EAL7), an (augmented) assurance package defined in an applicable external reference, or a set of SARs/assurance package defined within the ST itself.

A Security Target that claims conformance with exactly one multi-assurance PP-Configuration may become a **multi-assurance Security Target** by additionally defining:

— for each TSF part, the applicable set of SARs/assurance package. This can be the same set of SARs/assurance package inherited from the PP-Configuration, or a larger set (augmentation) which requires the provision of a rationale.

A multi-assurance Security Target may define a distinctive name for the sets of SARs/assurance packages that are globally and partially applicable. This name should be consistent with the name given in the PP-Configuration (if a name is given).

A multi-assurance Security Target that extends the sets of SARs/assurance packages of the associated PP-Configuration must provide an assurance rationale that justifies the consistency of the extension.

A multi-assurance Security Target has to conform according to each and all of the individual conformance types that are identified in the multi-assurance PP-Configuration.

NOTE 2 A Security Target that claims conformance with more than one PP/PP-Configuration can only define a global set of SARs/assurance package that applies to the entire TOE. In such a case, the standard ASE rules for ensuring the consistency of the assurance requirements of the ST with regard to PPs/PP-Configurations apply.

NOTE 3 A Security Target that claims conformance with one PP-Configuration which defines only one set of SARs/assurance package for the entire TOE and its parts cannot become a multi-assurance Security Target. 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 standard PP-Configuration must be defined and evaluated.

Figure 3 shows an example of multi-assurance Security Target that claims conformance to PP-Configuration “AXY” with one standard PP A and two PP-Modules X and Y. The sub-TSF structure consists of the three TSF defined in A, X and Y. The global set of SARs (SARC) and the multiple sets of SARs applicable to the sub-TSFs have been taken from the PP-Configuration without augmentation.

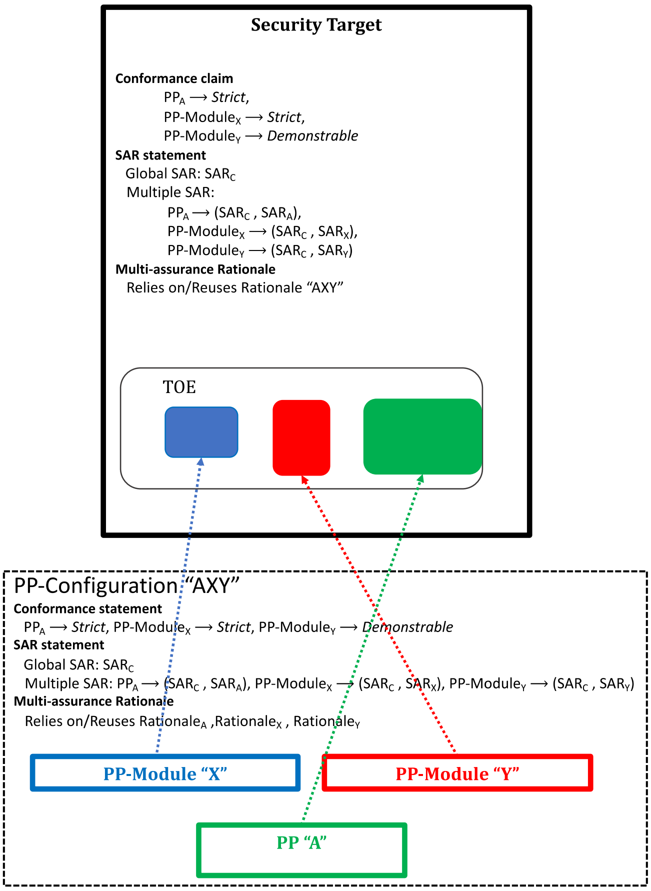

Security Target
Conformance claim
$PP_A \longrightarrow$ *Strict*,
$\text{PP-Module}_X \longrightarrow$ *Strict*,
$\text{PP-Module}_Y \longrightarrow$ *Demonstrable*
SAR statement
Global SAR: SAR_C
Multiple SAR:
$PP_A \longrightarrow (SAR_C , SAR_A)$,
$\text{PP-Module}_X \longrightarrow (SAR_C , SAR_X)$,
$\text{PP-Module}_Y \longrightarrow (SAR_C , SAR_Y)$
Multi-assurance Rationale
Relies on/Reuses Rationale "AXY"
TOE
PP-Configuration "AXY"
Conformance statement
$PP_A \longrightarrow$ *Strict*, $\text{PP-Module}_X \longrightarrow$ *Strict*, $\text{PP-Module}_Y \longrightarrow$ *Demonstrable*
SAR statement
Global SAR: SAR_C
Multiple SAR: $PP_A \longrightarrow (SAR_C , SAR_A)$, $\text{PP-Module}_X \longrightarrow (SAR_C , SAR_X)$, $\text{PP-Module}_Y \longrightarrow (SAR_C , SAR_Y)$
Multi-assurance Rationale
Relies on/Reuses Rationale_A ,Rationale_X , Rationale_Y
PP-Module "X"
PP-Module "Y"
PP "A"

Figure 3 — Example of multi-assurance Security Target

12 Evaluation and evaluation results

12.1 General

This clause 12 presents the expected results from PP, PP-Configuration and ST/TOE evaluations performed according to either ISO/IEC 18045, and/or evaluation methods developed using ISO/IEC 15408-4.

Evaluation should lead to 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 The use of evaluated PPs and PP-Configurations along with the use of well-defined evaluation methodologies is a necessary pre-condition for evaluation that leads to a result that provides a technical basis for the mutual recognition of evaluation results between evaluation authorities. Recognition criteria are out of the scope of this standard.

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 4 describes the various evaluations that are needed to provide confidence in the evaluation results for a TOE.

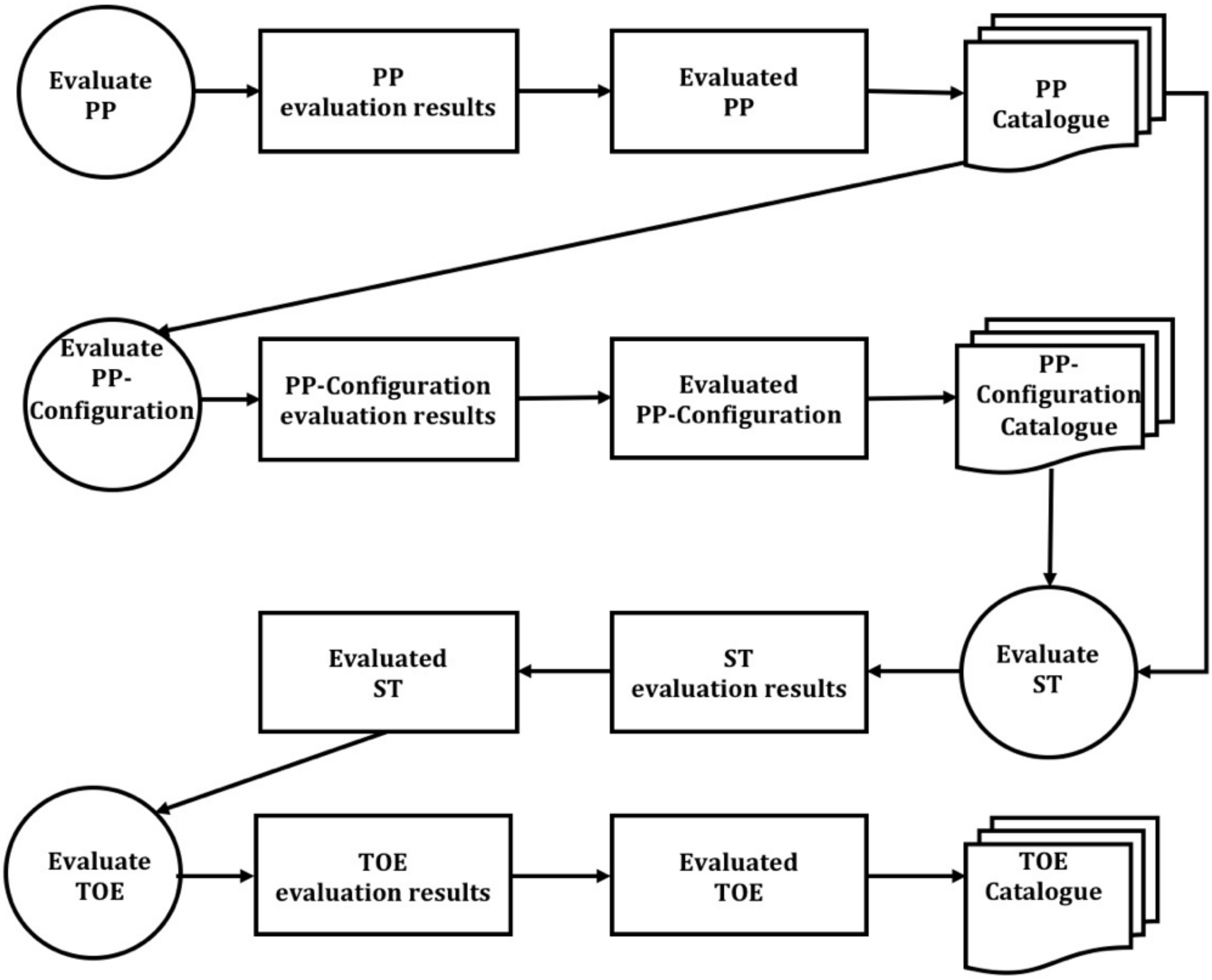


Figure 4 — Evaluation flow

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 12.3,

b) A PP-Configuration evaluation which is based on the ACE class given in ISO/IEC 15408-3, described in 12.3,

c) An ST evaluation which is based on the ASE class given in ISO/IEC 15408-3, described in 12.4, 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 12.4.

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, 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.

An 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.

12.2 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 ISO/IEC 19896-3 provides competency requirements for ISO/IEC 15408 evaluators which can be used to support conformity in the evaluation process.

For ISO/IEC 15408(all parts), the basic common evaluation methodology 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.

EXAMPLE

It may be necessary for PP authors to augment the basic common evaluation methodology with a method that includes technology-specific evaluation activities.

A certification process, which is outside the scope of ISO/IEC 15408(all parts), is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval, which can be publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.

12.3 Evaluation of PPs and PP-Configurations

Basing a PP or an 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 an ST or another PP.

The method of stating evaluation results for PPs and PP-Configurations is described in 12.7.

NOTE PP-Modules are not evaluated separately; they are evaluated in the course of evaluating the PP-Configuration that uses them.

12.4 Evaluation of STs

An 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 activities derived from ISO/IEC 18045 using the framework described by ISO/IEC 15408-4.

The method of stating ST evaluation results is described in 12.7. These results also identify any PP(s) and package(s) to which the ST claims conformance.

12.5 Evaluation of TOEs

A TOE evaluation determines that the correctness of the TOE against the criteria defined in the Security Target. 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 Security Target) to the evaluation evidence. The precise method to apply a specific SAR is determined by the evaluation methods and activities that are associated with the ST, either ISO/IEC 18405 or evaluation methods and activities derived from ISO/IEC 18045 using the ISO/IEC 15408-4 framework.

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 12.7.

12.6 Evaluation methods and activities

Basic 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 activities may be derived from ISO/IEC 18045 using the framework described in ISO/IEC 15408-4. Such methods and activities may be published either as an inclusion in PPs, PP-Modules and packages or as separate supporting documents.

12.7 Evaluation results

12.7.1 Results of a PP-Configuration evaluation

The results of a PP-Configuration evaluation shall also include a “conformance claim” in accordance with 10.3.

Once a PP-Configuration has been evaluated, an 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 an ST that claims conformity with the PP-Configuration. Otherwise the conformance claim is meaningless and the ST evaluation would fail in this aspect.

12.7.2 Results of a PP evaluation

The results of the PP evaluation shall also include a “Conformance Claim” in accordance with 8.3.

NOTE 1 ISO/IEC 15408-3 provides evaluation criteria for PPs in the APE class.

12.7.3 Results of an ST/TOE evaluation

Evaluation of the TOE shall therefore result in a pass/fail statement for the ST. If both the ST and the TOE evaluation have resulted in a pass statement, the underlying product can be eligible for inclusion in a catalogue.

The results of an ST evaluation shall also include a “Conformance Claim” as defined in 11.2.1.

The result of the TOE evaluation process is either:

- 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;
- 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.

NOTE 1 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.

NOTE 2 ISO/IEC 15408-3 provides evaluation criteria for STs in the ASE class.

12.7.3.1 Use of ST/TOE evaluation results

Once an 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 either one 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.

12.8 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/assurance packages does not undermine the expected security of the underlying assets, as defined in the SPDs of the component PPs and PP-Modules.

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 parts and the sets of SARs/assurance packages are consistent with the PP-Configuration.

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/assurance package and evaluating each of the TSF parts against the corresponding sets of SARs/assurance packages.

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 global TSF in terms of the sub-TSFs and the difference between the global set of SARs/assurance package and the multiple sets of SARs/assurance packages that apply to the sub-TSF.

The limitation of multi-assurance evaluation to products (and Security Targets) that comply with one multi-assurance PP-Configuration and the definition of the multi-assurance consistency rules in ACE limits the impact on the other assurance classes. The interpretation of the SARs applicable to a TSF part in a multi-assurance evaluation relies on the sub-TSF decomposition and is uniform for all assurance classes: "TOE" stands for "global TOE" and “TSF” stands for “sub-TSF”.

13 Composition of assurance

13.1 General

IT Products are almost always composed from several components. Some of which may be evaluated and some which are not.

EXAMPLE

evaluated software is composed with hardware to create an IT product.

Independent product components are often evaluated separately and the problem of composing the security assurance to determine the assurance of the entire product arises.

This clause 13, describes the concepts of composition techniques in 13.2. In 13.3 some methods by which security assurance in a composition scenario can be provided is given and in 13.4, how much can be re-used from the evaluation of individual components is provided. It also discusses the important considerations when re-using evaluation results.

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.

13.2 Composition techniques

13.2.1 Layered

In this type of layered composition, one component is built on top of another component, as pictured in Figure 5.

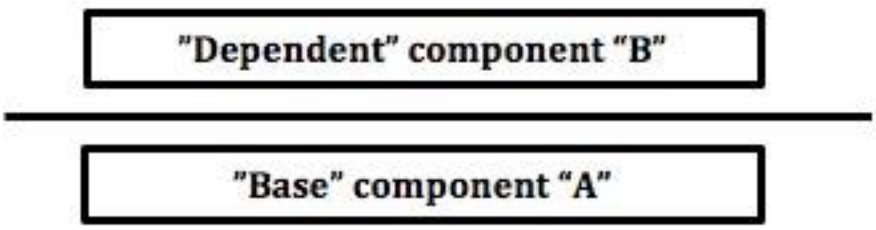


Figure 5 — Layered composition

The following assumptions are made in regard to the layered assurance 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 functions of the base component and not vice versa

Those performing such a composition should consider that:

- The dependent component can depend on functions not considered to be security functions in the evaluation of the base component. In particular, for
  - Hardware/software layering: Almost all instructions of the hardware are used to implement the security functions
  - Software layering: the dependent component layer can depend on some functions not considered in the evaluation of base component layer.

EXAMPLE

Two examples hereafter can be used to clarify the layered composition described in Figure 5. The first and main example comes from the smartcard domain, where an evaluation technique has been defined for layered composition. In this context, a smart card is built up with a combination of two parts: a hardware integrated circuit (IC) part and a software part often developed by different actors with specific objectives.

The software part of the smartcard may be layered itself consisting of an

- “Operating System layer” with possibly integrated applicative functions and an
- “Application layer” on top of it that may contain different applications.

All these software 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 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 functions of the application layer can be clearly broken down to the evaluated security functions of the base component. Where this is not possible, the dependent component implements the security functions itself.

13.2.2 Network, or bi-directional

In this type of composition, a component uses the specific functions of another component communicating via some communication channel. See Figure 6.

EXAMPLE 1

An application (component “A”) using the functions of an external LDAP server (component “B”)

The following assumptions are made in regard to the network, or bi-directional assurance 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 functions required to protect the communication channel.

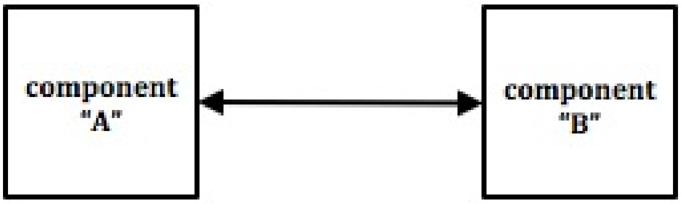


Figure 6 — Network composition

Those performing such a composition should consider that:

- Security functions 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 functions 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.

13.2.3 Embedded

In this type of composition, a component is used as part of a larger component or product. See Figure 7

EXAMPLE

A library or subsystem providing specific security functions as part of a larger product.

The following assumptions are made in regard to the embedded assurance composition model:

- There is usually no separation between the composed parts,
- Each part can influence the other via channels and interfaces other than the intended ones.

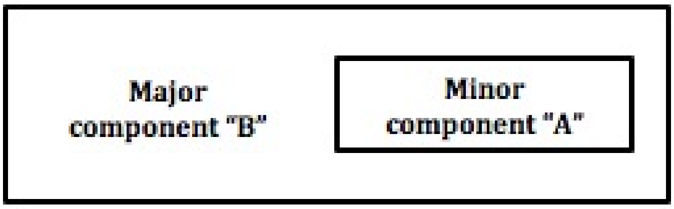


Figure 7 — Embedded composition

Those performing such a composition should consider that due to the lack of separation, components may:

- bypass security functions of the other components,
- modify the security functionality and security policy of other components and 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

13.3 Evaluation techniques for providing assurance in composition scenarios

13.3.1 General

Composed TOEs using the composition techniques described in 13.2 cannot always be successfully evaluated. To achieve reliable and repeatable evaluation results, a defined method of evaluating TOEs in a composition scenario is needed.

13.3.2 describes how the ACO class provided in ISO/IEC 15408-3 may be used, and 13.3.3 describes a technique for Composite product evaluation using a layered model.

13.3.2 Using the ACO class

The ACO class specified in ISO/IEC 15408-3, addresses a TOE composed of two TOEs, both of which have been separately evaluated, and that are composed using a layered technique. These TOEs can be described as a base TOE and a dependent TOE, Figure 8. An evaluation of the composed TOE consists of evaluating the interaction between both TOEs, reusing evaluation results from both the base TOE and the dependent TOE.

ISO/IEC 15408-5 provides pre-defined composed assurance packages (CAP) that may be used for rating the composed TOE's assurance. CAPs provide an alternative approach to obtaining higher levels of assurance for a composed TOE than application of the EALs above EAL1.

The ACO class is applicable up to Extended-Basic assurance level.

Figure 8 shows a typical scenario where the ACO class can be used for evaluating a composition.

Editors' Note:

The following figure corresponds to the definition of composed TOE, not to a typical scenario. A concrete example is welcome

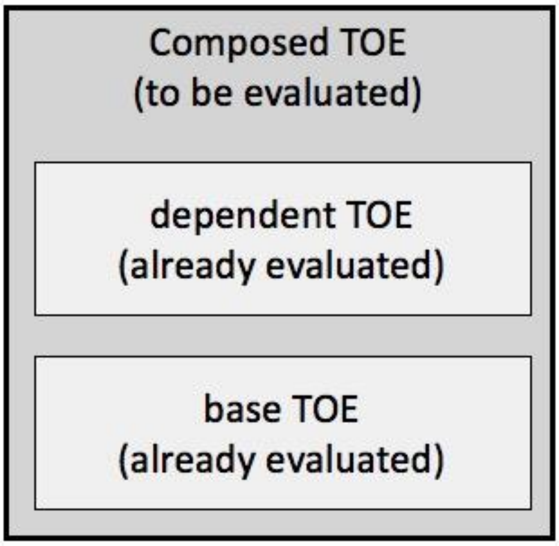


Figure 8 — Composed TOE evaluated using the ACO class

13.3.3 Composite product evaluation using a layered model

13.3.3.1 General

The composite product evaluation technique was devised to meet different types of objectives:

- independently perform one evaluation of a platform to address several applications and customers;
- create one or several applications to load on one or several certified platforms;
- install one or several applications onto one already certified platform to reduce the evaluation effort keeping a high level of confidence.

The evaluation technique describes a way to perform a transfer of knowledge and a reuse of evidence, in order to meet these objectives.

The COMP class specified in ISO/IEC 15408-3 provides evaluation criteria pertinent to TOEs using this layered model.

13.3.3.2 Objective

This method for composition of assurance applies to layered composite IT products that comprise one or more base TOE(s) evaluated independently and one or more dependent component(s). In the composite evaluation approach, the evaluation of the dependent component is performed within the evaluation of the composite product (that is, the composite TOE is made of the integration of the base TOE and the dependent component). Therefore, assurance level is claimed for and applies to the composite TOE as a whole and not to the dependent component alone.

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 TOE can claim any predefined EAL or well-defined assurance package, including resistance up to ‘high attack potential’ such as those 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 refinements to the existing assurance requirements for a composite TOE evaluation.

> EXAMPLE
>
> Examples of smart card devices requiring high-level assurance include banking (finance) and digital-signature applications.
>
> Smart cards and similar devices are built up with a combination of two parts: a hardware integrated circuit (IC) part and a software part often developed by different actors with specific objectives.
>
> The software part may be layered itself, consisting of an “Operating System layer” with possibly integrated applicative functions and an “Application layer” on top of it that may contain different applications.

13.3.3.3 Concept of composite TOE

A Composite TOE is composed of a base component and a supplementary layer. The base component is identified as “Platform TOE” in Figure 9 and will be identified as the ‘Platform’ in the remainder of this document. The supplementary layer is identified in Figure 9 as the ‘Application TOE’ and will be identified as the ‘Application’ in the remainder of this document.

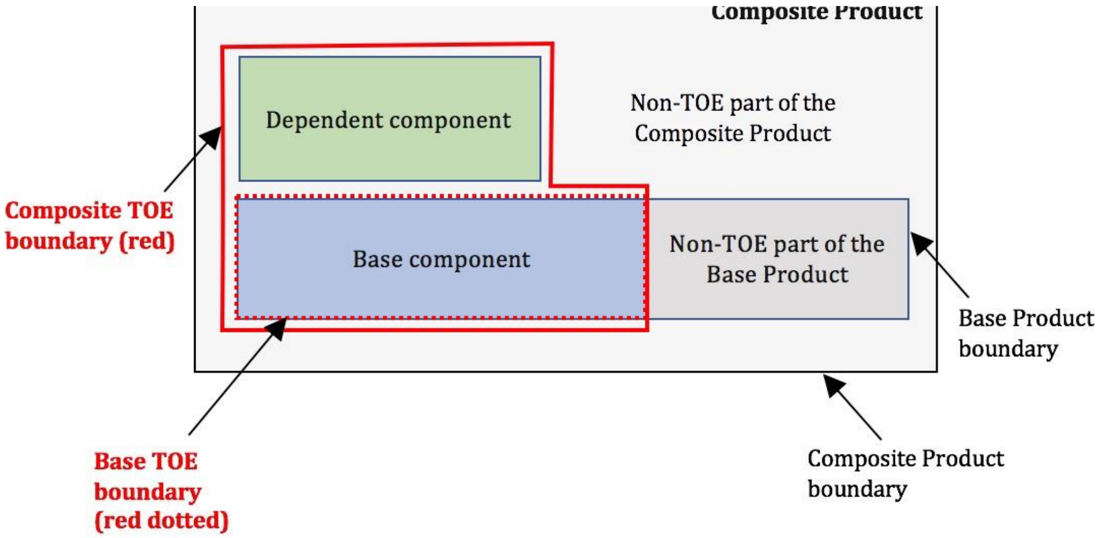
- The Platform is the underlying layer. This layer shall have already been evaluated. Therefore, it has a sponsor, a developer, an evaluator, and an evaluation authority;
- The Application is the supplementary layer that is dependent on the Platform. This layer shall also be evaluated.
- The Composite Product includes the Platform and the Application. The composite evaluation technique is intended to optimize the evaluation of this Composite Product;
- Non-TOE parts of the Composite Product, the Platform and the Application are considered part of the operational environment of the Composite Product TOE.

Several composition steps can follow each other. In other terms, the Platform can itself be a composite product.

Some rules apply when defining the Composite TOE:

- The application TOE cannot rely on platform functionalities that are outside the platform TOE, in the Non-TOE parts. This is depicted in grey layer ‘Non-TOE part of the Platform TOE’;
- The composite TOE is composed with a superset of the entire application TOE, and a superset of the minimum platform TOE functionalities required for the correct execution of the composite

Figure 9 — Composite TOE


Composite Product
Dependent component
Non-TOE part of the Composite Product
Base component
Non-TOE part of the Base Product
Composite TOE boundary (red)
Base Product boundary
Base TOE boundary (red dotted)
Composite Product boundary

product;

- The non-TOE subset of the application can use platform TOE functionalities. As usual, the composite evaluation needs to determine that this non-TOE application part is non-interfering with the application TOE – neither directly nor through the usage of the platform functionalities.

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 platform is equivalent or higher compared to the composite product evaluation level. Other cases will require dedicated techniques defined by evaluation authorities.

NOTE 3: In the case where both platform and application have already been evaluated using ISO/IEC 15408, a partial evaluation work may be performed regarding the results already obtained from previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

13.3.3.4 Roles

The Platform and the Application are all undergoing an evaluation. Therefore, both of them have a sponsor, a developer, an evaluator, and an evaluation authority.

The Composite TOE also undergoes an evaluation, and also has a sponsor, an evaluator, and an evaluation authority. Consequently:

- the Composite TOE sponsor is the entity in charge of contracting the composite TOE evaluation;
- the Composite TOE evaluation authority is the entity performing the composite TOE certification;
- the Composite TOE evaluator is the entity performing the composite TOE evaluation;
- The Application developer is the entity who develops the composite TOE security target;
- There is no Composite TOE developer in practice since the Composite TOE is resulting from the integration of the Application and the Platform. Instead, the composite evaluation technique defines additional evaluation activities for:
    - the Application developer and the Platform developer;
    - the Composite TOE Integrator. Entity installing the applications on the platform.

NOTE 1 As already mentioned, the Application may have undergone a separate evaluation, but the evaluator and evaluation authority of this previous evaluation are not considered here. Notably, the terms Application evaluator and Application evaluation authority do not refer to this previous evaluation.

NOTE 2 As in the general cases, some other 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 Platform developer may also be the Platform sponsor;
- The Platform evaluation authority may also be the Composite Product evaluation authority.

NOTE 3 The Composite Product Integrator is a different concept than the developer. While this integrator may, in some cases, also be one of the developers defined previously, this is not always true.

The following example illustrates the role of the Composite Product Integrator:

EXAMPLE 2:

- Native Smart cards: The ‘underlying platform’ is an integrated circuit and the Platform Developer is the integrated circuit (chip) manufacturer; the ‘application’ is a card operating system and its application(s) and the Application Developer is the developer of the smart card software and the application(s). In this case, the role of the Composite Product

Integrator is played by:

(i) the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by

(ii) 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 platform’ is the Java Card runtime Environment (Java Card RE) on chip and the Platform Developer is the card manufacturer/issuer; the ‘application’ is the Java Card applet and can be developed by the Application 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.

13.3.3.5 Actions elements and required information

To allow the evaluation of this Composite Product, the composite evaluation technique identifies two main sets of issues, leading to two sets of rules:

- The Composite Product might be insecure due to gaps in the definition, integration or test of the Platform and Application 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 Security Target;
  - The security mechanisms involved in the protection of these assets are those provided by the Platform and by the Application;
  - Some of the security mechanisms and security services provided by the Platform may require configuration, programming, or activation by the Application;
  - 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 Platform, as well as the evaluation of the Application and 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 must be selected in the Composite Product Security Target, and which information is required to allow a composite evaluation.

Table 2 — Information to be provided to the Application developer

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	Security target of the Platform Information (usually in the form of a guidance or user’s manual) related to the platform’s security mechanisms and security services that the application has to manage.	Platform developer
Composite design compliance (ADV_COMP)	Information (usually in the form of a guidance or user’s manual) related to the platform’s security mechanisms and security services that the application has to manage.	Platform developer

Table 3 — Information to be provided to the Composite Product evaluator and evaluation authority

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	Security target of the Platform Information related to the platform's security mechanisms and security services that the application has to manage.	Platform developer
	Security target of the Composite Product	Application developer
Integration of composition parts 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 platform and the application having been composed into the final composite product.	Composite Product Integrator
	Organizational evidence that components (Application or Platform) transmitted from an actor to another is securely received, accepted and parameterized.	Composite Product Integrator Platform developer Application developer
Composite design compliance (ADV_COMP)	Platform-related integration recommendations, typically including the user guidance.	Platform developer
	Evidence that the composite product meets the platform-related integration recommendations.	Composite Product Integrator
	Certification Report for the platform	Platform evaluation authority
Composite functional testing (ATE_COMP)	Composite product samples suitable for testing, that allow to load any Application	Composite Product Integrator
Composite vulnerability assessment (AVA_COMP)	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 platform, and explanation related to residual vulnerability linked to integration recommendations included in the user guidance.	Platform evaluator
	Certification Report for the platform	Platform evaluation authority

NOTE 1: In the case of composition, the term "developer" needs further clarification in order to distinguish the different actor involved. Here, the base TOE developer, the dependent TOE developer and the composite TOE integrator can be different entities. Similarly, for the terms "evaluator", "evaluation authority (evaluation scheme)" and "validator" further distinguishing of the different entities involved needs to be made.

NOTE 2: In the case where both base and dependent TOEs have already been evaluated, a reduced set of evaluation activities may be performed taking into account the evaluation results already obtained from the previous application evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

NOTE 3: The composite TOE evaluator may not need all the detailed results of the base and dependent TOEs evaluations. See subclause 13.4 for more detail on re-using evaluation results.

EXAMPLE

Smart Card

Smart card architecture is composed of a hardware platform (base TOE) and a software application (dependent TOE). In a Composite TOE evaluation, the platform is already evaluated, the application is evaluated and the results of the platform evaluation are reused. In this case, the platform is the base component, and the application is the dependent component.

The hardware platform has no 'strictly functional' properties related to the security of the composite TOE. It provides functionality supporting the protection of the composite product assets, but the composite product behaviour depends on the software application having to use, configure, and activate these security functions.

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 component TOEs does not lead to any exploitable vulnerability.

A smart card 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 TOE 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.

13.4 Requirements for evaluations using composition techniques

13.4.1 Re-use of evaluation results

When composing components into an IT product, it is possible that components have already been evaluated and that existing evaluation results could be reused. However, further evaluation of the TOE shall be performed to confirm the security assurance of the entire IT product.

If the evaluation results and evidence for TOE components are not available then they cannot be re-used.

The re-use of evaluation results and evaluation evidence is dependent upon:

- the assurance to be claimed for the TOE;

EXAMPLE 1

the evaluation assurance level.

- the type of composition performed;
- if security properties for the TOE are claimed or not.

EXAMPLE 2

Security properties include, but are not limited to:

- Separation;
- Information Flow Control;
- Fault tolerance.

- evaluation scheme policy.

13.4.2 Composition rationale

When composing an IT product from components, a composition rationale shall be provided. This includes analyses of the:

a) composition type (or types);

b) interfaces and dependencies of the functions;

c) composability of the security function policies, and organizational security policies;

d) preservation of security properties;

e) for the embedded type of composition, aspects of correctness.

13.4.2.1 Use of the ACO class

Part 3 of this standard, describes the ACO class which provides security assurance components that may be used in support of the evaluation of composed TOEs.

Part 5 of this standard, provides a family of pre-defined assurance packages for composition which provide packages (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.

13.4.2.2 Vulnerability analysis

The composed IT product shall have a vulnerability analysis, in accordance with the AVA class, performed on the composed IT product at a level commensurate with the required security assurance for the composed IT product. The vulnerability analysis is more difficult when security properties are claimed.

The vulnerability analysis shall be designed in consideration of the composition analysis.

13.4.2.3 Testing

Additional testing, using the ATE and IND classes given in ISO/IEC 15408-3, of the composed product shall be performed. It may be possible to re-use the testing evaluation results from the components, but additional tests for the composed product shall be designed and performed.

The testing shall be designed in consideration of the composition analysis.

Editors' Note:

In this CD2, the editors have re-numbered the annexes in order to present them in the same order as the main clauses in the normative part of the document.

It is hoped that this will aid the readers of the document in locating and understanding the information and guidance presented in the annexes.

Note that in CD1, Annex B presented information and guidance for PPs as well as PP-Configurations, while the normative clauses broke this into two sections. Hence, we now have split the annexes to follow this approach.

More information on verbal forms and the annex statuses are found in the latest directives at:

http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype

Annex A
(informative)

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 in implicit once a package is incorporated into a PP, PP-Module or ST.

A.2 Package families

A.2.1 General

Figure C.1 shows the structure of a package family. Each part is discussed in the following subclauses.

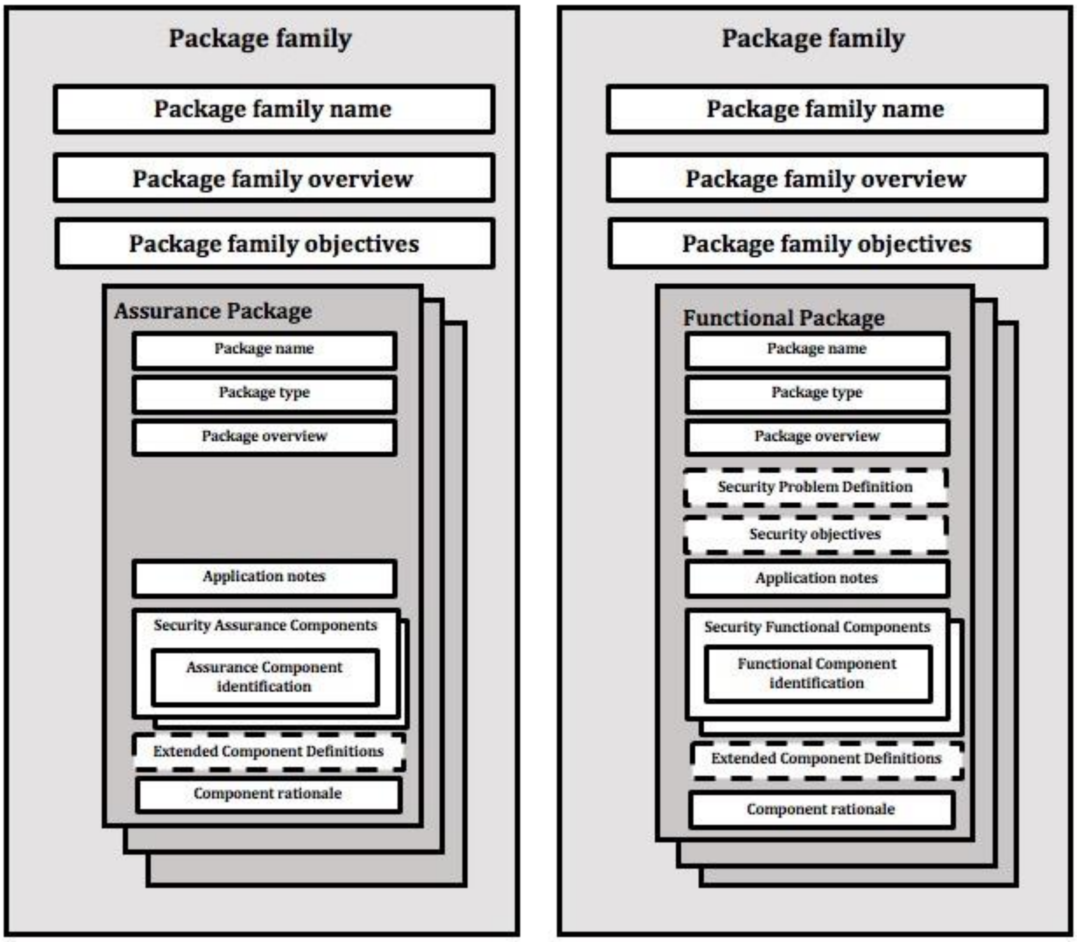


Figure A.1 — The structure of a package family with assurance or functional packages

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 can 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

If evaluation method(s) and/or activities, derived from ISO/IEC 18045 in accordance with the ISO/IEC 15408-4 framework are specified for use with the package then the application notes section is included and contains a reference to them. Evaluation method(s) and/or activities, derived from ISO/IEC 18045 in accordance with the ISO/IEC 15408-4 framework can either be specified associated with the security requirements in the package or in a separate supporting document.

For functional packages, any additional audit and management requirements relating to the SFRs included in the package are specified in the Application notes section.

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

Functional package can 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 can be provided in the application notes section of the functional package, and can 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 can be selection-based. See 7.2.3.2.

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 can include this section.

This section includes any SPD elements which describe the security problem addressed by the functional package.

In the case of a functional package used for direct rationale PPs/STs TOE Security Objectives are not included.

A.3.2.2 Security objectives (Functional Packages)

Assurance packages do not contain this section.

Functional packages can include this section.

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.

A.3.2.3 Application notes

The inclusion of application notes in a package is optional unless the package references evaluation methods/activities or, for functional packages additional audit and management requirements relating to the SFRs are specified. See A.3.1.4.

The application notes section can 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 can contain extended components. In this case, packages contain a section giving the extended component definitions.

A.3.2.5 Evaluation methods/activities

Packages can include evaluation methods and/or activities that have been derived from ISO/IEC 18045 in accordance with the framework given in ISO/IEC 15408-4. Evaluation methods and/or activities that are associated with the package are referenced in the application notes section of the package. See 8. Evaluation methods and/or activities can be included in the package associated with the relevant security requirements or provided in a separate document.

Annex B
(informative)

Specification of Protection Profiles

Editor's Note:

This annex is to be completed and updated in order to cover the multi-assurance paradigm once the corresponding multi-assurance text is stable.

B.1 Goal and structure of this Annex

The goal of this annex is to explain the Protection Profile (PP) concept and is supported by the documents given in the bibliography.

NOTE This annex does not define the requirements for evaluation of PPs and PP-Configurations. The PP and PP-Configuration evaluation criteria are found in the APE and ACE classes given in ISO/IEC 15408-3.

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 A.

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*
- *What a PP must contain*. This is summarized in B.2.2 and is described in more detail in B.2.2.1 to B.2.8. *These* clauses describe the mandatory contents of the PP, the interrelationships between these contents, and provide examples.
- *Claiming conformance with standards*. B.2.9 describes how a PP author can claim that the TOE is to meet a particular standard.
- *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.2.10.

b) *PP-Modules.* These are described in B.2.11.

c) *PP-Configurations.* These are described in C.2.

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. might 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 an 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 an ST for this purpose.

B.2.2 Mandatory Contents of a PP

There are two types of PP. Firstly the "regular" PP which is a PP that contains the full contents as described in in B.2.2.1 to B.2.8. 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.2.10. All other parts of this Annex assume a PP with full contents.

Figure B.1 portrays the content for a PP that is given in ISO/IEC 15408-3. Figure B.1 can 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.2.2.1 to B.2.8.

A PP contains:

a) a PP *introduction* containing a narrative description of the TOE type;

b) *conformance claims*, showing which edition of ISO/IEC 15408(all parts) is applicable, whether the PP claims conformance to any other PPs and/or packages, and if so, to which ones and the type of conformance claimed. The conformance claims section also provides reference to any evaluation method(s) and/or activities that have been derived from ISO/IEC 18045 in accordance with ISO/IEC 15408-4.

NOTE 1 Any evaluation methods and/or activities may optionally be included in the PP, or in an associated supporting document.

c) The conformance claim also provides a conformance statement showing the type of conformance demanded of STs and other PPs derived from it;

NOTE 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;

d) a *security problem definition*, showing threats, OSPs and assumptions;

e) *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;

f) *extended components definition*, where new components (i.e. those not included in ISO/IEC 15408-2 or ISO/IEC 15408-3) can be defined. These new components are needed to define extended functional and extended assurance requirements;

g) *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;

There also exist Direct Rationale PPs, which have slightly different content; these are described in detail in B.2.10.. With this exception, all other parts of this Annex assume a PP with full contents.

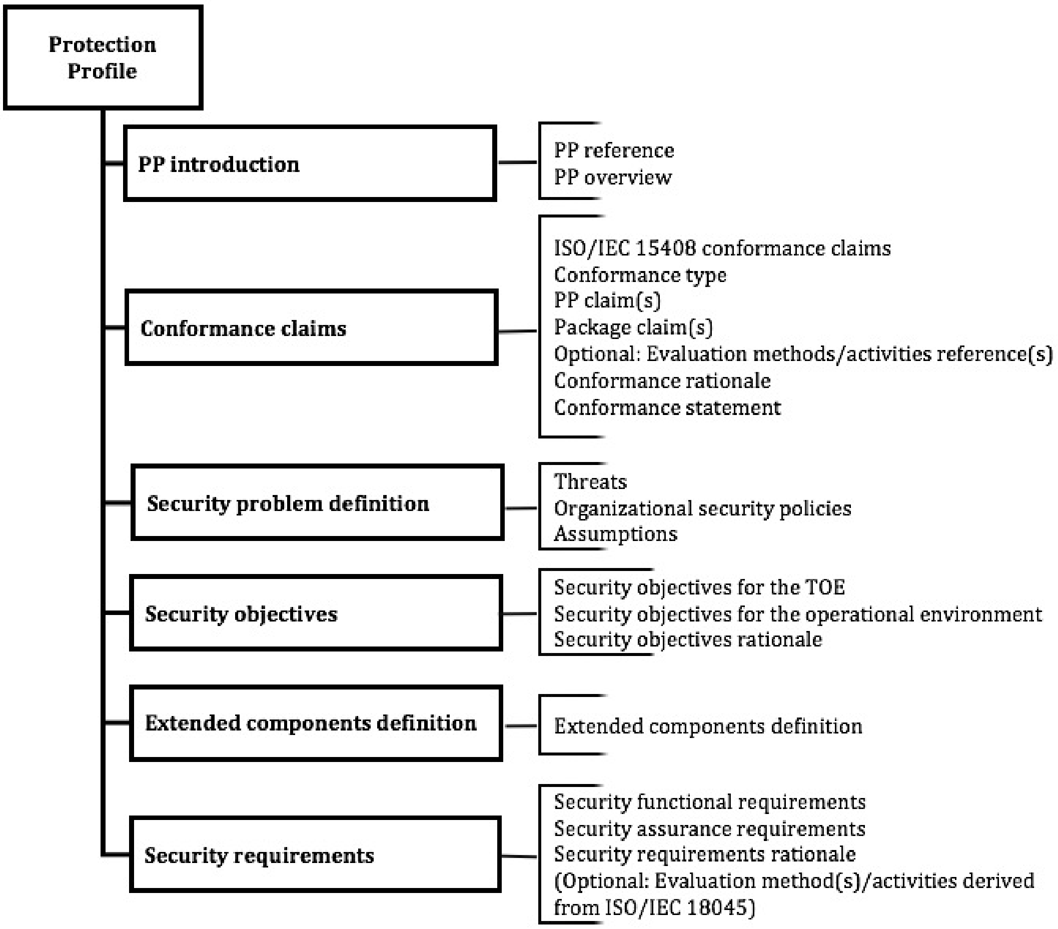

Protection Profile
PP introduction
PP reference
PP overview
Conformance claims
ISO/IEC 15408 conformance claims
Conformance type
PP claim(s)
Package claim(s)
Optional: Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
Security problem definition
Threats
Organizational 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 derived from ISO/IEC 18045)

Figure B.1 — Contents of a Protection Profile

B.2.2.1 PP introduction (APE_INT)

B.2.2.1.1 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.2.2.1.2 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 an ST, i.e. the entity responsible for its development, and the author of an ST 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 must 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 lists of PPs.

B.2.2.1.3 TOE overview

The TOE overview is aimed at potential consumers of a TOE who are looking through lists of evaluated products to find TOEs that can meet their security needs, and are supported by their hardware, software, and firmware.

The TOE overview is also aimed at developers who can use the PP in designing TOEs or in adapting existing products.

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 available to the TOE.

B.2.2.1.3.1 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, and what it can be used for. This section is written for TOE or potential TOE consumers, describing TOE usage and major security features in terms of business operations, using language that TOE consumers understand.

EXAMPLE

An example of this is “The Atlantean Navy CablePhone Encryptor is an encryption device that should allow confidential communication between ships across the Atlantean Navy CablePhone system. To this end it should allow at least 1024 different users and support at least 500 Mbps encryption speed. It should allow both bilateral communication between ships and broadcast across the entire network.”

B.2.2.1.3.2 TOE Type

The TOE overview identifies the general type of TOE, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server, mobile device, and database, etc.

B.2.2.1.3.3 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 TOE overview is required to identify the non-TOE hardware/software/firmware.

As a Protection Profile 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, (much) 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.2.3 Conformance claims and conformance statement (APE_CCL)

B.2.3.1 General

The conformance claims section of a PP describes how the PP conforms with ISO/IEC 15408 (all parts). other PPs, PP-Modules and with packages. It is identical to the conformance claims subclause for an ST described in D.4.2, with one exception, the conformance statement.

The conformance statement in the PP states how ST/PPs must conform to that PP. The PP author selects whether “exact”, “strict” or “demonstrable” conformance is required.

NOTE 1 See B.2.11 for the use of conformance claims in PP modules

NOTE 2 See B.2.10.2 for the use of conformance claims in Direct Rationale PPs

B.2.3.2 Exact conformance

If exact conformance is selected, the PP author also has the option of specifying the following information in the components statement:

- PPs that can be used, either by an ST or used in a PP-Configuration, with the PP;
- PP-Modules that can specify the PP as one of its Base PPs.

NOTE 1 See 8.3 (PPs) and 10 (PP-Configurations) for the requirements and Annex F for additional description in the exact conformance case.

B.2.4 Security problem definition (APE_SPD)

This subclause is identical to the security problem definition subclause of an ST as explained in D.4.3

B.2.5 Security objectives (APE_OBJ)

This subclause is identical to the Security Objectives subclause of an ST as explained in D.4.4. and D.4.9

B.2.6 Extended components definition (APE_ECD)

This subclause is identical to the extended components subclause of an ST as explained in A.8.

B.2.7 Security requirements (APE_REQ)

This subclause is identical to the security requirements subclause of an ST as explained in A.9. with the exception of

- the rules for completing operations as described in 7.2;
- the specification of selection-based SFRs as outlined below;
- the specification of optional requirements as outlined below.

A PP can identify a set of selection-based SFRs. In this case, the PP author additionally ensures that the PP clearly indicates the dependencies between a particular selection in a security functional component and/or SFR included in the PP and the associated selection-based SFR(s) that must be included if that selection is chosen by another PP/ST author. This is explained in 7.2.3.2.

The PP may define optional requirements in one of two categories. Each category shall be specified explicitly by the PP.

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

The first category of optional requirements is “purely” optional, in that the ST for a TOE is under no obligation to include the requirement, even if the TOE implements the functionality described by the requirement.

The second category of optional requirements is conditional in nature. If the TOE does not implement the functionality covered by the optional requirement, then the requirement is not included in the ST. However, if the TOE does implement the functionality, then it is to be included in the ST.

Additionally, optional requirements can be written in response to SPD elements that exist in the PP, or SPD elements that are specifically associated with the requirement. Such associations are identified in the PP. Direct rationale PPs will not have security objectives for optional requirements that have associated SPD elements, while non-Direct Rationale PPs will include security objectives for the associated SFRs and SPD elements.

The PP can define optional requirements in one of two categories. Each category is specified explicitly by the PP.

The first category of optional requirements is elective. Requirements in this category do not need to be included in an 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 must 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 PP, 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.

B.2.8 TOE summary specification

Unlike an ST, a PP has no TOE summary specification.

B.2.9 Referring to other standards in a PP

This subclause is identical to the subclause on standards for STs as described in A.12, with one exception: Since a Direct Rationale PP has no TOE summary specification, the third option is not valid for Direct Rationale PPs.

B.2.10 Direct Rationale PPs

B.2.10.1 General

Writing a PP includes consideration of the STs that will be written with the PP as a basis. As noted in D.4.9, 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, based on an enhanced description of the SFRs.

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 SPD and, where appropriate, Security Objectives for the operational environment.

Because of its directness and the additional description of SFRs in natural language, this type of PP makes it easier for end-users and risk owners to understand and use.

A Direct Rationale PP has the same relationship to a PP that contains Security Objectives for the TOE, as a Direct Rationale ST has to an ST that contains Security Objectives for the TOE. This means that 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 Figure B.2.

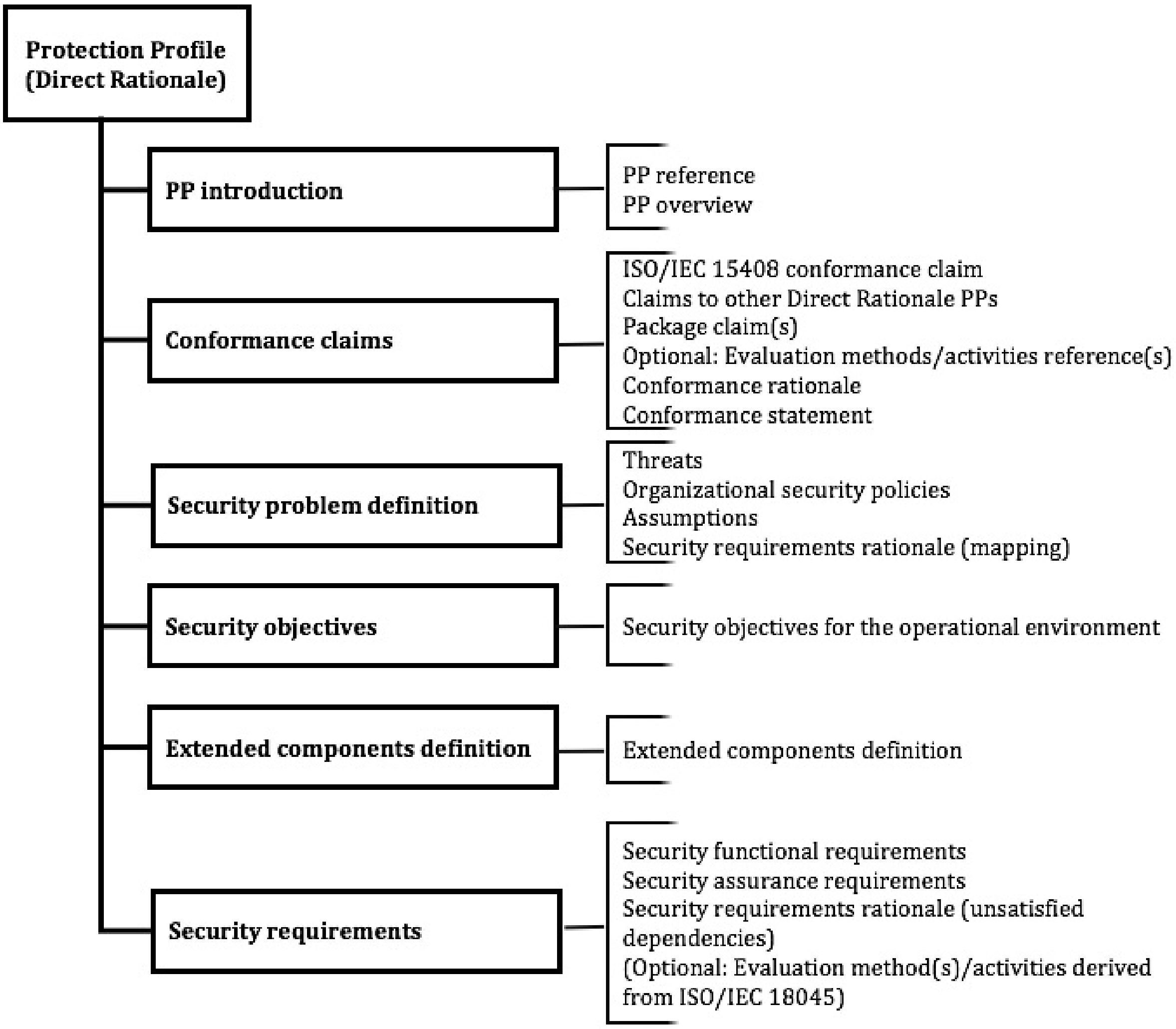

Protection Profile (Direct Rationale)
PP introduction
PP reference
PP overview
Conformance claims
ISO/IEC 15408 conformance claim
Claims to other Direct Rationale PPs
Package claim(s)
Optional: Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
Security problem definition
Threats
Organizational security policies
Assumptions
Security requirements rationale (mapping)
Security objectives
Security objectives for the operational environment
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale (unsatisfied dependencies)
(Optional: Evaluation method(s)/activities derived from ISO/IEC 18045)

Figure B.2 — Contents of a Direct Rationale PP

B.2.10.2 Conformance claims (ASE_CCL) for Direct Rationale PPs

A Direct Rationale PP can only claim conformance to another Direct Rationale PP (See 8.3 and B.5). A regular PP can claim conformance with a Direct Rationale PP.

B.2.10.3 Security Problem Definition (ASE_SPD) for Direct Rationale PPs

A Direct Rationale PP has the following differences when compared to an PP that contains Security Objectives for the TOE:

- Security Objectives for the TOE are not included. The Security Objectives for the operational environment must 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 SPD-elements to the SFRs and to any Security Objectives for the operational environment 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 PP that contain Security Objectives for the TOE, 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.2.11 Optional Contents of a PP

PPs can optionally include evaluation methods and/or activities that have been derived from ISO/IEC 18045 in accordance with the framework given in ISO/IEC 15408-4. Evaluation methods and/or activities that are associated with the PP are referenced in the conformance claims section of the PP. See 9.2.

If the PP author decides to include any evaluation method(s) and/or activities in the PP then they are included in the security requirements section associated with the relevant security requirement.

Annex C
(informative)

Specification of PP-Modules and PP-Configurations

Editor's Note:

This annex is to be completed and updated in order to cover the multi-assurance paradigm once the corresponding multi-assurance text is stable.

C.1 Specification of PP-Modules

C.1.1 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 Base PPs and allows consumers to refer to this statement, facilitates the evaluation against it and the comparison of conformant evaluated TOEs.

NOTE A Base PP is a PP that is intended to be used with one or more PP-Modules.

C.1.2 Mandatory Contents of a PP Module

Figure C.1 shows the content of a PP-Module.

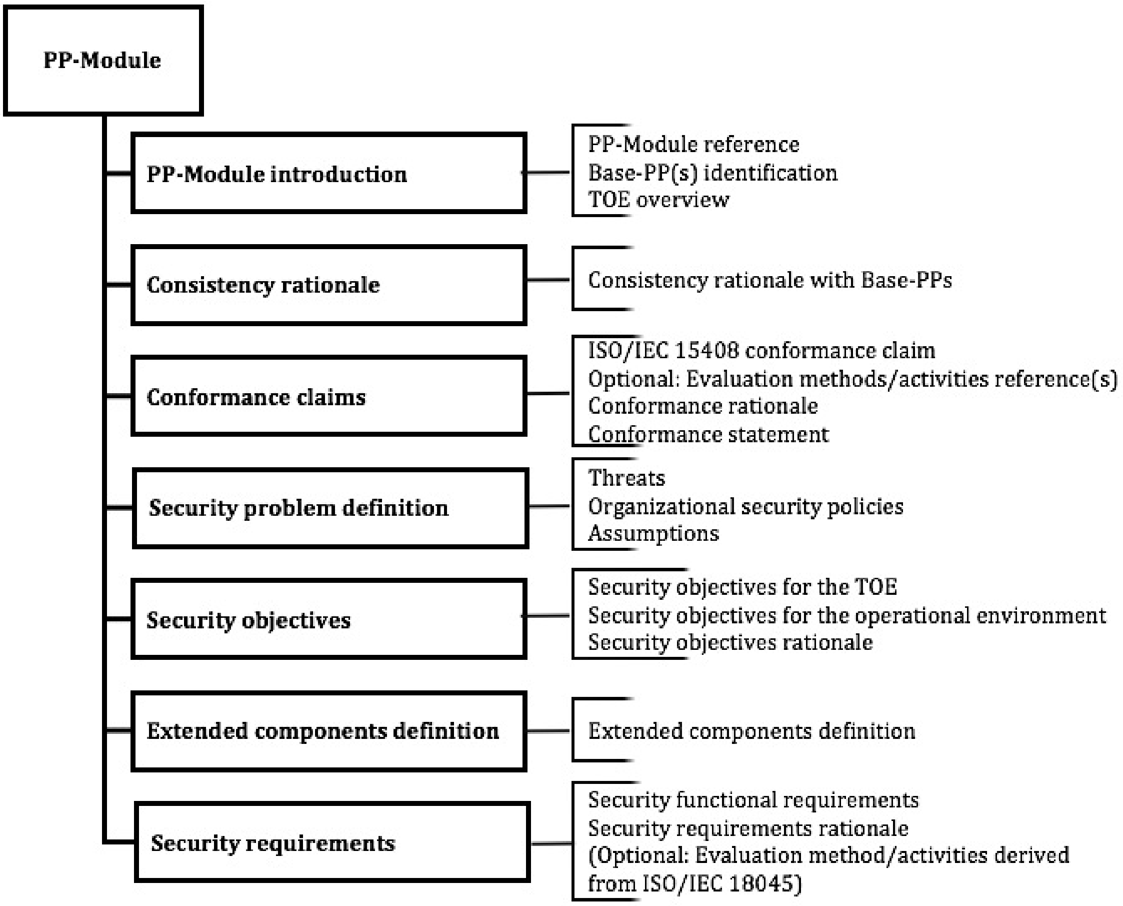

PP-Module
PP-Module introduction
PP-Module reference
Base-PP(s) identification
TOE overview
Consistency rationale
Consistency rationale with Base-PPs
Conformance claims
ISO/IEC 15408 conformance claim
Optional: Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
Security 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 requirements rationale
(Optional: Evaluation method/activities derived from ISO/IEC 18045)

Figure C.1 — Content of a PP-Module

The content of the PP-Module is summarized below and explained in detail in sections from C.1.2.1 to C.1.3. A PP-Module contains:

- an *Introduction* which identifies the PP-Module, identifies the Base PP(s) which it is based on and states the correspondence rationale, and provides a description of the TOE within its environment that meets the descriptions underlying the Base PPs,
- a *Consistency rationale* that states the correspondence between the Module and its Base PP(s),
- a *Conformance claim* regarding the edition of ISO/IEC 15408(all parts), the conformance statement and with any applicable inherited EAL,
- 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.

C.1.2.1 PP-Module introduction

C.1.2.1.1 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, its version, their sponsors, and the publication date.

The PP-Module reference can be used to index the document in Protection Profiles catalogues.

C.1.2.1.2 Base PP identification

The PP-Module introduction identifies the Base PPs that the PP-Module relies on. The identification consists of a list of Base PP references.

The PP-Module could require that it be used with a set of Base PPs simultaneously, say {PP_1 ..., PP_n}; the identification list states:

$$PP_1 \ AND \ldots AND \ PP_n \text{ with } n \geq 1$$

Alternatively, the PP-Module could allow it’s use with alternative sets of Base PPs, say {S_1 ..., S_k}; the identification list states:

$$S_1 \ OR \ \ldots \ OR \ S_k \text{ with } k \geq 1$$

The general form of the Base PP identification is then:

$$(PP_{1,1} \ AND \ \ldots \ PP_{1,n_1}) \ OR \ \ldots OR \ (PP_{k,1} \ AND \ \ldots \ PP_{k,n_k}) \ with \ n_k \ \geq 1, k \geq 1$$

NOTE 1 A PP-Module that states a list with an "OR" can be replaced by as many PP-Modules as elements in the list. That is, the list with an "OR" is a means to avoid managing similar PP-Modules for different usages, which does not introduce any complexity to the security specification itself.

NOTE 2 A Base PP with an exact conformance statement is not allowed to be combined with Base PPs with other types of conformance in a PP-Module.

C.1.2.1.3 TOE overview

The TOE overview of the PP-Module can complete the TOE overviews of the Base PPs, provided the supplements do not contradict the Base PPs:

- The TOE type of the PP-Module can be the same as that of the Base PPs or introduce specificities that meet the purpose of the PP-Module.
- The PP-Module can introduce further usage and major security features in addition to those stated in the Base PPs.

- The PP-Module can specify particular non-TOE hardware, software and/or firmware compliant with the statement in the Base PPs.

In a PP-Module, the possibility of supplementing the TOE overview of one or more of the Base PPs has the same meaning as in a Base PP or ST that supplements the TOE overview of a Base PP to which they claim conformance.

The statement of the TOE overview in a PP-Module is necessary whenever the TOE overview of the Base PPs present different characteristics that need to be consolidated.

The PP-Module can provide as many specific TOE overviews as alternative sets of Base PPs.

C.1.2.2 Consistency rationale

The PP-Module has to provide a consistency rationale with respect to its Base PPs.

If the PP-Module specifies alternative sets of Base PPs, the PP-Module must provide as many conformance claims as the number of alternative sets of Base PPs.

If the PP-Module specifies alternative sets of Base PPs, the PP-Module must provide as many consistency rationales as the number of alternative sets of Base PPs.

The consistency analysis must 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) and in the PP-Module and that the TOE can satisfy all security functional requirements specified in the Base PPs and the PP-Module.

The consistency rationale must demonstrate that the unions of the SPD, the objectives, and the security functional requirements from the Base PPs and from the PP-Module do not lead to a contradiction.

The consistency rationale can use correspondence tables between SPD/objectives/SFRs in the PP-Module and SPD/objectives/SFRs in the Base PPs together with textual justifications whenever needed.

NOTE The consistency at the SFR level 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- PP(s).

C.1.2.3 Conformance claims and conformance statement

C.1.2.3.1 General

This section of a PP-Module must be included for all PP-Modules and describes how the PP-Module conforms to:

- ISO/IEC 15408-2, its edition, and any use of extended security requirements
- functional packages.

A PP-Module cannot claim conformance to any PP, PP-Module, or PP-Configuration.

The PP-Module conformance statement also identifies any evaluation methods and evaluation activities (as described in ISO/IEC 15408-4) that are required to be used with it.

NOTE A PP-Module inherits the set of security assurance requirements, 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 an ST conformant to all those PPs deals with the issue.

C.1.2.3.2 The conformance statement

The conformance statement must be stated in a PP-Module. A PP-Module does not claim conformance to any PP, PP-Module, or PP-Configuration. However, a PP-Module inherits the conformance statement, exact, strict, or demonstrable, from its Base PPs. The issue of two or more Base PPs with different conformance statements must be resolved and is dealt with in the same way that an ST conformant to all those PPs deals with the issue.

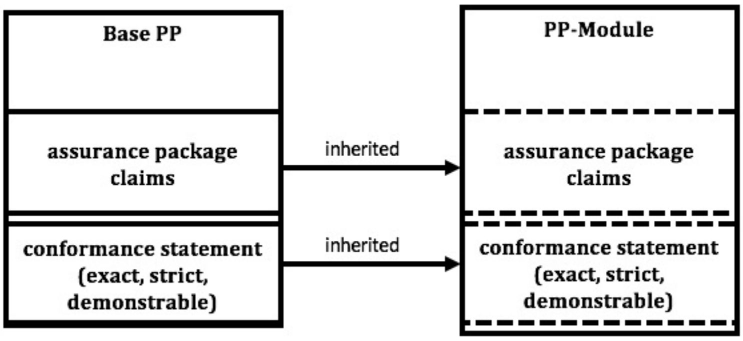

Base PP
assurance package claims
conformance statement (exact, strict, demonstrable)
inherited
inherited
PP-Module
assurance package claims
conformance statement (exact, strict, demonstrable)

Figure C.2 — General case for inherited conformance claims and statement

If evaluation methods and evaluation activities (as described in ISO/IEC 15408-4) are included in 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>."

Where <reference> is replaced by identification of the location of the evaluation methods and evaluation activities applicable to the PP-Module.

NOTE 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.1.2.3.2.1 Exact conformance

In the case of exact conformance, the conformance statement also includes an identification of PPs other than the PP-Module's set of Base-PPs, and 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.

C.1.2.4 Security problem definition

This section defines the security problem addressed by the PP-Module. It can contain the SPD-elements assumptions, threats, and organizational security policies.

A PP-Module defines the security problem in relationship with the security problem of the Base PPs 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 or be entirely new. Let E be an SPD-element of a PP-Module, one of the following cases holds:

- E belongs to an identified Base PP; the PP-Module can only contain a reference to the SPD-element in the Base PP,
- E results from the refinement of an SPD-element of a Base PP,
- E is a new SPD-element introduced by the PP-Module, related to additional features of the TOE or its environment.

NOTE 1 The interpreted / 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.

C.1.2.5 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 PP(s).

Each Security Objective can either come from a Base PP or be entirely new. Let O be an objective of a PP-Module, one of the following cases holds:

- O belongs to an identified Base PP; the PP-Module can only contain a reference to the Security Objective in the Base PP.
- O is a result of the refinement of a security objective of a Base PP,
- 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 can introduce new objectives for the TOE operational environment only when they address aspects that are outside the scope of the Base PPs.

In the case where a PP-Module refines the TOE type, some Security Objectives for the environment of the Base PPs 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 section B.7. 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 that do not belong to the SPD of the PP-Module itself. This information is not required but can be provided in application notes.

C.1.2.6 Extended functional components definition

This section is identical to the standard PP and ST extended components section specified in section A.8, applied to functional components only.

C.1.2.7 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.

Each security functional requirement can either come from a Base PP or be entirely new. Let R be a security functional requirement of a PP-Module, one of the following cases holds:

- R belongs to an identified Base PP; the PP-Module can only contain a reference to the requirement in the Base PP,
- R results from the refinement of an SFR of a Base PPs,
- 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 TOE objectives of the PP-Module to one or more SFRs and a justification demonstrating that the tracing is effective, as specified in section B.9. Moreover, the mapping must fulfil the conditions specified in section B.14.10 and has to show not only that all the objectives for the TOE are covered but also that there is no useless security functional requirement.

It can happen that some SFRs of the PP-Module cover also TOE Security Objectives of the Base PPs that do not belong to the PP-Module itself. This information is not required but can be provided in application notes.

PP-Modules can define and include optional SFRs (and any required SPD elements) as previously specified for PPs in B.2.7.

C.1.3 Direct Rationale PP-Modules

PP-Modules can be written with the intention that they be used with a Direct Rational 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 can be included.

The contents of a Direct Rationale PP-Module are shown in figure B.5.

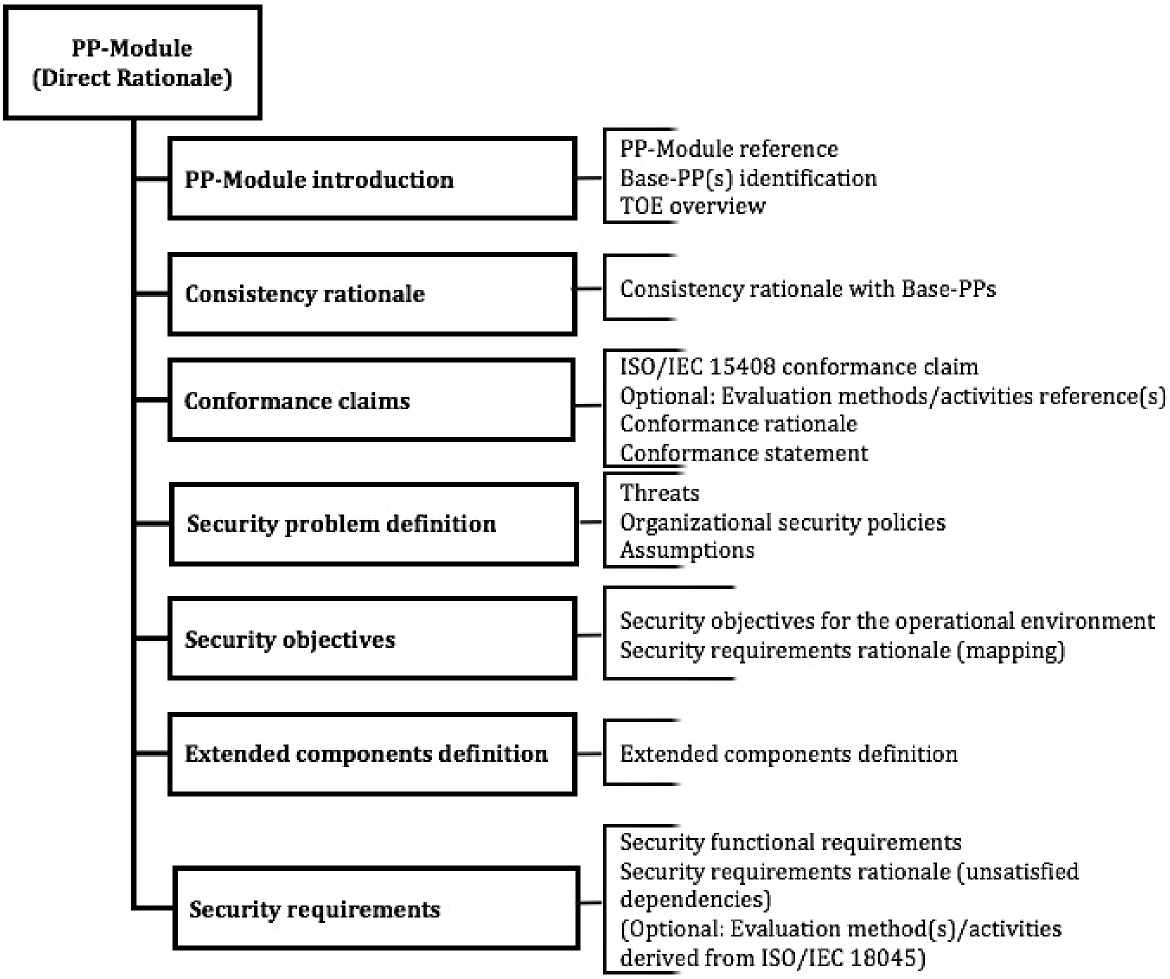

PP-Module
(Direct Rationale)
PP-Module introduction
PP-Module reference
Base-PP(s) identification
TOE overview
Consistency rationale
Consistency rationale with Base-PPs
Conformance claims
ISO/IEC 15408 conformance claim
Optional: Evaluation methods/activities reference(s)
Conformance rationale
Conformance statement
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 requirements rationale (unsatisfied dependencies)
(Optional: Evaluation method(s)/activities derived from ISO/IEC 18045)

Figure C.3 — Direct Rationale PP-Module

C.1.4 Guidance for inclusion of SPD-elements from a Base PP

In order to limit the amount of information contained in the PP-Module, the PP-Module editors apply the following rules:

Let E, O and R belong to the SPD, the Security Objectives, and the security functional requirements of a Protection Profile Q, respectively, with E mapped to O and O mapped to R.

Let P be a PP-Module and let Q be one of the Base PPs of P. P has to satisfy the following condition:

E, O, R, and the mappings between them can belong to P only if at least one of these SPD-elements is linked to a new SPD-element in P, that is

- Either there is a new SPD-element E' in the SPD of P such that E' is mapped to O, or
- There is a new objective O' in P such that E is mapped to O' or O' is mapped to R, or
- There is a new requirement R' in P such that O is mapped to R'.

That is, a PP-Module would not contain portions of Base PPs unless they are required to fulfil new needs. Here, refined SPD-elements are considered new.

C.1.5 Optional Contents of a PP-Module

PP-Modules can optionally include evaluation methods and/or activities that have been derived from ISO/IEC 18045 in accordance with the framework given in ISO/IEC 15408-4. Evaluation methods and/or activities that are associated with the PP are referenced in the conformance claims section of the PP-Module. See 10.2.2.2.

If the PP-Module author decides to include any evaluation method(s) and/or activities in the PP-Module then they are included in the security requirements section associated with the relevant security requirement.

C.2 Specification of PP-Configurations

C.2.1 Mandatory content of a PP-Configuration

The content of a PP-Configuration is summarized below in Figure B.6 and explained in detail in Annexes C.2.1.1 through C.2.1.4. A PP-Configuration contains:

- a PP-Configuration reference that uniquely identifies the PP-Configuration,
- a Components statement that identifies the PPs, Base PPs and the PP-Modules composing the PP-Configuration,
- a Conformance statement, that specifies the edition of ISO/IEC 15408, the conformance claims to ISO/IEC 15408-2 and ISO/IEC 15408-3 and whether the conformance of STs to this PP-Configuration has to be exact, strict, or demonstrable.
- A SAR statement, specifying the SAR package, or a list of the security assurance components selected that are applicable to the PP-Configuration.

NOTE An SAR package can be an EAL drawn from ISO/IEC 15408-5.

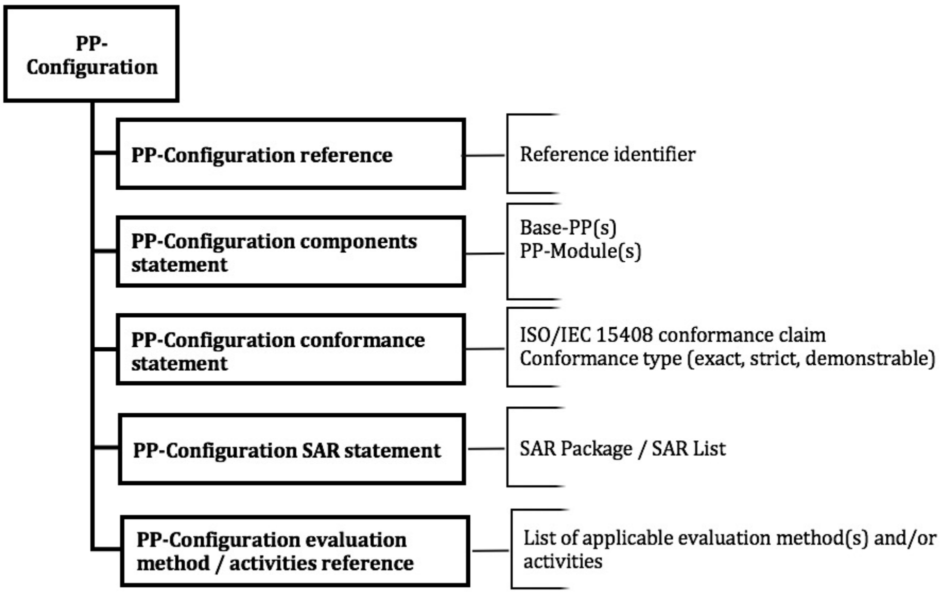

PP-Configuration
PP-Configuration reference
Reference identifier
PP-Configuration components statement
Base-PP(s)
PP-Module(s)
PP-Configuration conformance statement
ISO/IEC 15408 conformance claim
Conformance type (exact, strict, demonstrable)
PP-Configuration SAR statement
SAR Package / SAR List
PP-Configuration evaluation method / activities reference
List of applicable evaluation method(s) and/or activities

Figure C.4 — Content of a PP-Configuration

C.2.1.1 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.2.1.2 PP-Configuration components statement

The PP-Configuration components statement identifies the Base PPs and the PP-Modules that compose the PP-Configuration.

The PP-Configuration components statement must include the Base PPs required in the PP-Modules. If a PP-Module specifies alternative sets of Base PPs, only one of these sets must be referred to in the PP-Configuration.

C.2.1.3 PP-Configuration conformance statement

C.2.1.3.1 General

All PPs, Base-PPs and PP-Modules in the PP-Configuration must allow all other PPs, Base-PPs and PP-Modules to be combined in their respective conformance statements.

NOTE A PP-Module does not need to include its own Base PPs in its conformance statement because they are implicitly allowed.

The PP-Configuration conformance statement specifies whether the conformance to this PP-Configuration by an ST is one of exact, strict, or demonstrable.

C.2.1.3.2 Exact conformance

If one Base PP in the PP-Configuration has an exact conformance statement, then all Base PPs, and therefore all the PP-Module(s) in the PP-Configuration must also have exact conformance statements. Further, all PPs and PP-Modules in the PP-Configuration must explicitly include all the other components of the targeted PP-Configuration either as a base PP or in their “allowed with” statement. This is illustrated in Figure C.5

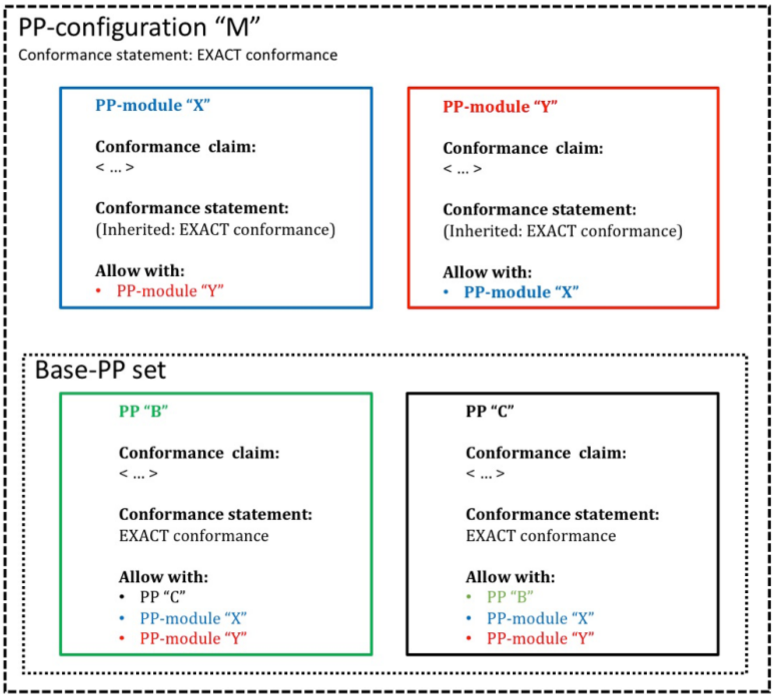


Figure C.5 — PP-Configuration and exact conformance

EXAMPLE

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.

Any ST that claims conformance to the PP-Configuration will conform to the conformance type required in the conformance statement of the PP-Configuration.

C.2.1.4 PP-Configuration SAR statement

The SAR statement specifies the set of SARs applicable to any product evaluation with a ST that claims conformance to this PP-Configuration.

EXAMPLE

An example of a set of SARs is an EAL predefined in ISO/IEC 15408-5

C.2.1.5 PP-Configuration Evaluation methods/activities references

The PP-Configuration Evaluation methods/activities references statement specifies the set of evaluation methods and/or activities that are applicable to the instantiated PP-Configuration.

A PP-Configuration may specify evaluation methods and/or activities in addition to those referenced in the PP-Configuration components.

C.2.2 Using a PP-Configuration

PP-Configurations address the specific needs of groups of users, consumers, organizations, etc.

An instantiated PP-Configuration can be used in the same way as a standard Protection Profile, as explained in section C.2.4.

C.2.3 Evaluation of a PP-Configuration

PP-Configurations can be evaluated using the ACE class given in ISO/IEC 15408-3.

C.2.4 Interpretation of PP-Configuration as a PP

C.2.4.1 General

Once evaluated, the instantiation of a PP-Configuration can be refined and used in the same way as a PP. This sub-clause, C.2.4, explains how to combine the content of the PP-Module(s), Base PP(s) and PPs of a PP-Configuration so as to interpret it as a single PP.

The consistency analysis performed during a PP-Configuration's evaluation ensures that the combination is valid.

C.2.4.2 TOE type

The TOE type of the PP is constituted from the TOE type of the PPs and or Base PP(s) with any additions introduced by the TOE types of the PP-Module(s).

The evaluation of an instantiated PP-Configuration ensures that it forms a consistent TOE type.

C.2.4.3 Conformance claims and conformance statement

C.2.4.3.1 General

The conformance claims of the PP instantiated from a PP-Configuration must contain:

- The edition of ISO/IEC 15408 (all parts), and if ISO/IEC 15408-2 and ISO/IEC 15408-3 have been extended or not;
- If evaluation methods and evaluation activities derived from ISO/IEC 18045 as described in ISO/IEC 15408-4 are associated with the instantiated PP, then these must be referenced by the instantiated PP;
- The conformance to any other PP(s) or PP-Modules whose conformance is claimed in PP(s) of the PP-Configuration;
- The conformance to SAR packages/lists, including any pre-defined EALs, from the PPs of the PP-Configuration;
- The conformance to functional packages from the Base PPs and any PP-Modules.

NOTE 1 The issue of two or more PPs with different conformance statements has to be dealt with in the same way that an ST conformant to all those PPs would.

NOTE 2 The issue of two or more PPs with different SAR packages such as EALs has to be dealt with just as in an ST conformant to all those PPs would, i.e. the PP must claim the minimum set of SARs (such as an EAL) of all the included PPs).

NOTE 3 The issue of two or more PPs with different functional packages has to be dealt in the same way that an ST conformant to all those PPs would.

C.2.4.3.2 Exact Conformance

If a PP-Module inherits a conformance claim from a set of Base PPs of exact conformance, then the PP-Module can list in its conformance statement a set of other PPs that are not its own Base PPs and PP-Modules. These other PPs are allowed to be specified in a PP-Configuration, in combination with the Base PPs, with that PP-Module. The PP-Module's own Base PPs for that PP-Configuration are inherently allowed and do not need to be specified in the conformance statement.

A PP with an exact conformance statement is not allowed to be combined with PPs with other types of conformance.

NOTE 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.

C.2.4.4 Security problem definition

The SPD of the PP contains the union of the SPD-elements from the PPs, Base PP(s) and PP-Module(s) of the PP-Configuration.

C.2.4.5 Security Objectives

The Security Objectives of the PP contains the union of the Security Objectives from the PPs, Base PP(s) and PP-Module(s) of the PP-Configuration.

NOTE For PP-Configurations following a Direct Rationale approach, then the Security Objectives would not contain any Security Objectives for the TOE.

C.2.4.6 Extended functional components definition

The extended functional components definition section of the PP contains all of the extended functional components / SFRs from the PPs, Base PP(s) and PP-Module(s) of the PP-Configuration.

C.2.4.7 Security functional requirements

The set of security functional components and/or SFRs of the PP contains:

- all the security functional components and/or SFRs from the PP-Module(s) of the PP-Configuration.
- all the security functional components and/or SFRs from the PPs and Base PP(s) except those which are refined in the PP-Module(s). This can include selection-based SFRs from the Base PP(s).

- all the security functional components and/or SFRs from functional packages claimed in the PP-Configuration.

Any optional SFRs (and associated SPD elements) in any PP-Configuration component that are allowed to be claimed by an ST.

The consistency analysis performed during a PP-Configuration's evaluation ensures that this set of SFRs is valid.

Annex D
(informative)

Specification of Security Targets and Direct Rationale STs

Editor's Note:

This annex is to be completed and updated in order to cover the multi-assurance paradigm once the corresponding multi-assurance text is stable.

D.1 Goal and structure of this Annex

The goal of this annex is to explain the Security Target (ST) concept and is supported by the documents given in the bibliography.

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 an ST*. This is summarized in A.2 and A.3. These sections describe how an ST should be used, and some of the questions that can be answered with an ST.

b) *What an ST must contain*. This is summarized in A.4 and is described in more detail in A.5 - A.11. These sections describe the mandatory contents of the ST, the interrelationships between these contents, and provide examples.

c) *Claiming conformance with standards*. A.12 describes how an ST author can claim that the TOE meets a particular standard.

d) *Direct Rationale STs*. Direct Rationale STs are STs in which the SPD-elements are mapped directly to the SFRs, and possibly to Security Objectives for the operational environment. A.4 through A.12 are applicable to Direct Rationale STs with the differences given in A.13.

D.2 Using an ST

D.2.1 How to use an 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. A.7 describes 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. A.11 describes how the ST is used in this role.

D.2.2 How not to use an ST

One role, among many, that an ST should not fulfil is:

- *a complete specification*: An ST 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 an ST. This means that in general an ST may be a part of a complete specification, but not a complete specification itself.

D.3 Questions that can be answered with an 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 to define this solution, then the answer can be found in the Conformance Claims section of the ST, which lists all packages and PPs 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.4 Mandatory contents of an ST

There are two types of ST. Firstly the “regular” ST which is an ST that contains the full contents as described in A.5 through A.12. Secondly, in some cases an ST author can use a Direct Rationale ST which has different contents compared to STs that contain Security Objectives for the TOE. Direct Rationale STs, and the reasons and circumstances in which they are used are described in detail in A.13 All other parts of this Annex assume an ST with full contents.

Figure D.1 — Contents of an ST, portrays the contents of an ST that are given in ISO/IEC 15408- 3. Figure A.1 can 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 an ST and the contents of those sections are briefly summarized below and explained in much more detail in A.5 to A.12. An ST contains:

NOTE In Direct Rationale STs no Security Objectives for the TOE are included: See D.4.9.

a) *an 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.

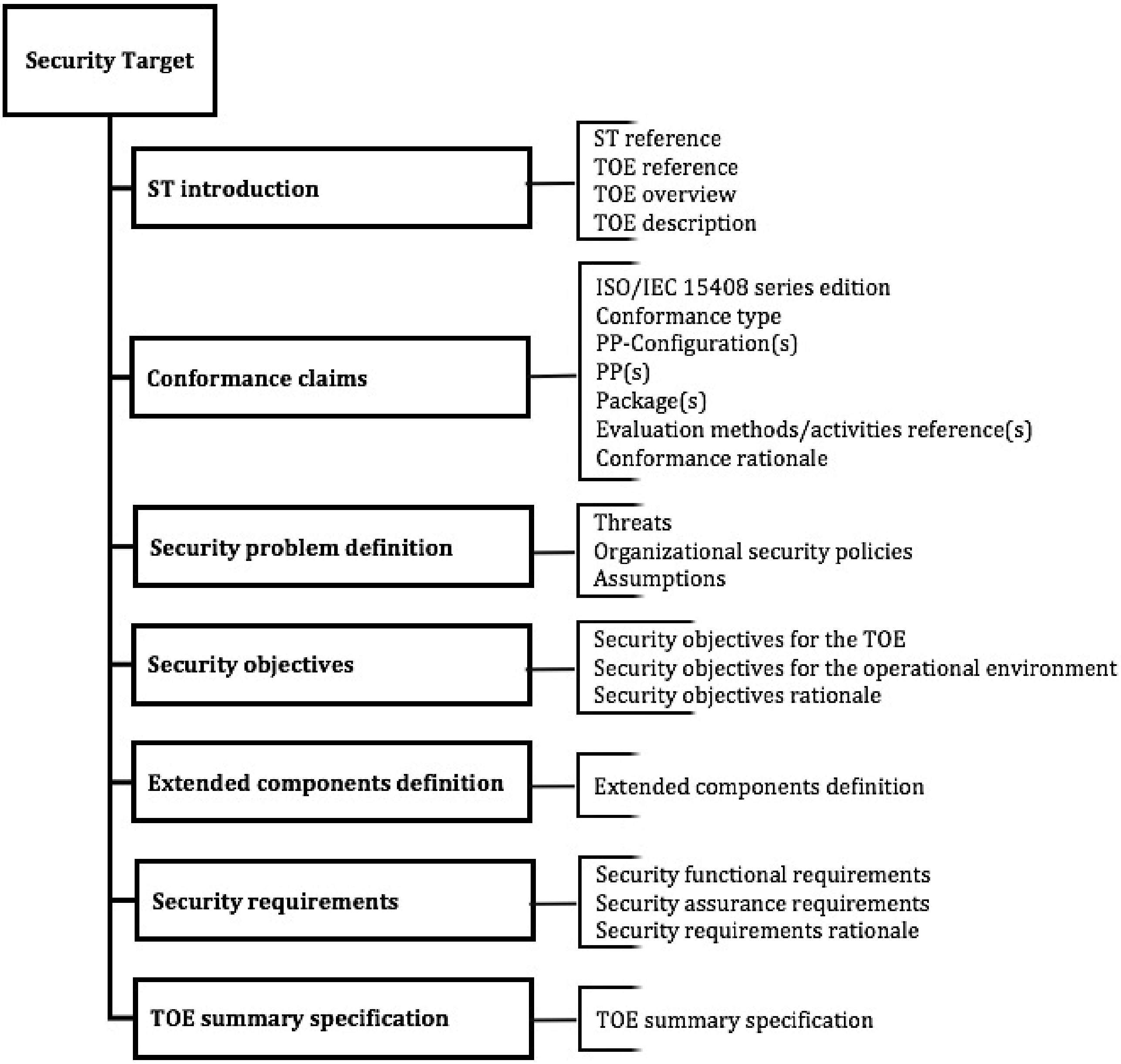

Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
ISO/IEC 15408 series edition
Conformance type
PP-Configuration(s)
PP(s)
Package(s)
Evaluation methods/activities reference(s)
Conformance rationale
Security problem definition
Threats
Organizational 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
Security assurance requirements
Security requirements rationale
TOE summary specification
TOE summary specification

Figure D.1 — Contents of an ST

D.4.1 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.4.1.1 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.

An ST contains a clear ST reference that identifies that particular ST. A typical ST reference consists of title, version, sponsors, and publication date.

NOTE Here a distinction is made between the sponsor of an ST, i.e. the entity responsible for its development, and the author of an ST which is the entity responsible for its production.

> EXAMPLE 1
>
> An example of an ST reference is "MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2017".

An 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. As a single TOE may be evaluated multiple times, for instance by different consumers of that TOE, and therefore have multiple STs, this reference may not be unique.

> 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.4.1.2 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 can 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.

D.4.1.2.1 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 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.4.1.2.2 TOE type

The TOE overview identifies the general 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.

It can be the case that the TOE is not of a readily available type, in which case “none” would be acceptable.

In some cases, a TOE type can mislead consumers. This is to be avoided by ST authors.

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 TOE, which does not support any identification/authentication functionality;
    - a firewall type TOE, which does not support protocols that are almost universally used;
    - a PKI-type 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 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.4.1.2.3 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 must 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.4.1.3 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 can 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 must be described at a level of detail that is sufficient to give the reader a general understanding of those parts.

The TOE description must also discuss the logical scope of the TOE, including the major TOE functions and provide a brief description of the security features of the TSF in the context of these functional features. The description provided must 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

Examples where the TOE is integrated with non-TOE entities are:

- the TOE is a cryptographic co-processor of a smart card IC, instead of the entire IC;
- the TOE is a smart card 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

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.4.2 Conformance claims (ASE_CCL)

This section of an ST describes how the ST conforms with:

- The edition of ISO/IEC 15408(all parts) used;
- ISO/IEC 15408-2 and ISO/IEC 15408-3;
- Protection Profiles (if any);
- PP-Configuration(s) (if any);
- Packages (if any);
- Evaluation methods/activities derived from ISO/IEC 18045 (if any).

The description of how the ST conforms to ISO/IEC 15408(all parts) consists of two items: the edition of ISO/IEC 15408 that is used and whether the ST contains extended security requirements or not (see 11.2. and D.4.5).

The description of conformance claimed by the ST to Protection Profiles and PP-Configurations means that the ST lists the PPs, and any PP-Configurations to which conformance is being claimed to. The type of conformance being claimed is also identified. For an explanation of this, see 11.2.

NOTE In the exact conformance scenario, an ST conforms to only one PP-Configuration.

The description of conformance of the ST to packages means that the ST lists the packages to which conformance is being claimed. For an explanation of this, see 11.2.

The description of the evaluation methods and activities derived from ISO/IEC 18045 in accordance with ISO/IEC 15408-4 means that the ST provides references to the documents specifying the evaluation method(s) and/or activities to be used during an evaluation based on the ST. These evaluation methods and activities may be included in a PP, PP-Module or package claimed by the ST, or may be found in an associated supporting document. It is not necessary to reproduce the text of these evaluation methods and activities in the ST. See 11.2.1.

D.4.3 Security problem definition (ASE_SPD)

D.4.3.1 Introduction

The security problem definition defines the security problem that is to be addressed. The security problem definition is, as far as ISO/IEC 15408 is concerned, axiomatic. That is, the process of deriving the security problem definition falls outside the scope of ISO/IEC 15408.

NOTE 1 The usefulness of the results of an evaluation strongly depends on the ST, and the usefulness of the ST strongly depends on the quality of the security problem definition. It is therefore often worthwhile to spend significant resources and use well-defined processes and analyses to derive a good security problem definition.

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

D.4.3.2 Threats

This section of the security problem definition shows 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 are actions performed by a threat agent on an asset. These actions influence one or more properties of an asset from which that asset derives its value.

Threat agents can be described as individual entities, but in some cases, it can 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;
- someone on the Internet listening in on confidential electronic communication.

D.4.3.3 Organizational security policies (OSPs)

This section of the security problem definition shows 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 by an actual or hypothetical organization 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.

D.4.3.4 Assumptions

This section of the security problem definition shows 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 not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

EXAMPLE

Examples of assumptions are:

- 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.

D.4.4 Security objectives (ASE_OBJ)

D.4.4.1 General

The Security Objectives are a concise and abstract statement of the intended solution to the problem defined by the security problem definition. The role of the Security Objectives is threefold:

- provide a high-level, natural language solution of the problem;
- divide this solution into two part-wise solutions, that reflect that different entities each have to address a part of the problem;
- demonstrate that these part-wise solutions form a complete solution to the problem.

D.4.4.2 High-level solution

The Security Objectives consist of a set of short and clear 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.

D.4.4.3 Part-wise solutions

In an 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. This reflects that these part-wise solutions are to be provided by two different entities: the TOE, and the operational environment.

D.4.4.3.1 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 must achieve in order to solve its part of the problem.

NOTE In Direct Rationale STs Security Objectives for the TOE are not included: See D.4.9.

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 ST.

If the TOE is physically distributed, it can be better to subdivide the ST section containing the Security Objectives for the TOE into several subsections to reflect this.

D.4.4.3.2 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 must achieve.

EXAMPLE

Examples of Security Objectives for the operational environment are:

- The operational environment shall provide a workstation with the OS Inux 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 could be better to subdivide the ST 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 must include that the third-party component works as intended.

D.4.4.4 Relation between Security Objectives and the security problem definition

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 STs a Security Objectives Rationale is not included: See D.4.9.

> 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".

D.4.4.4.1 Tracing between Security Objectives and the security problem definition

The tracing shows how the Security Objectives trace back to the threats, OSPs and assumptions as described in the security problem definition (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 D.2.

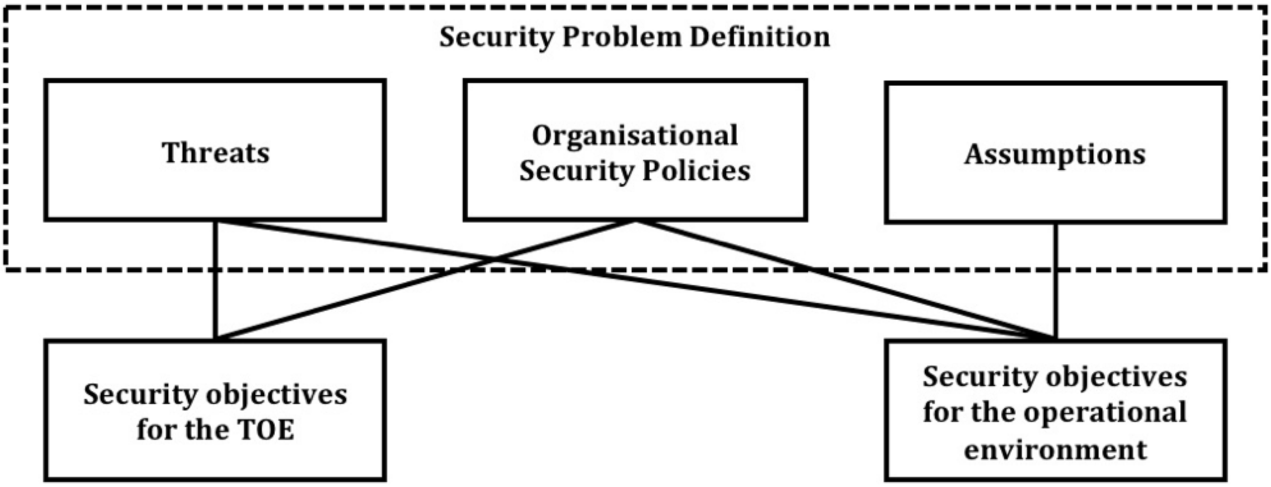

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment

Figure D.2 — Tracings between Security Objectives and the SPD

Multiple Security Objectives can trace to the same threat, indicating that the combination of those Security Objectives counters that threat. A similar argument holds for OSPs and assumptions.

D.4.4.4.2 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 can be much simpler.

D.4.4.4.3 On countering threats

Countering a threat does not necessarily mean removing that threat, it can 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;
  EXAMPLE 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.

D.4.4.5 Security Objectives: conclusion

Based on the Security Objectives and the Security Objectives rationale, the following conclusion can be 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.

D.4.5 Extended Components Definition (ASE_ECD)

In many cases the security requirements in an ST are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3, see D.4.6. However, in some cases, there might be requirements in an ST 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, must be defined, and the definition provided in the Extended Components Definition section of the ST. For more information on this, see E.4

NOTE This section of an ST is intended to contain only the extended components and not the extended requirements which are based on the extended components. The extended requirements can be included in the security requirements section of the ST as described in D.4.6 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.

D.4.6 Security requirements (ASE_REQ)

D.4.6.1 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 the following two subclauses:

D.4.6.2 Security functional requirements (SFRs)

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 must be completely addressed) and be independent of any specific technical solution (implementation). ISO/IEC 15408 requires this translation into a standardized language for several reasons:

- to provide an exact 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 exact description of the functionality of the TOE.
- to allow comparison between two STs. As different ST authors can use different terminology in describing their Security Objectives, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

There is no translation required in ISO/IEC 15408 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. See the bibliography for items relevant to the security assessment of operational systems.

If the PP or PP-Configuration components contain optional requirements, the ST can instantiate these requirements, being sure to include any required SPD elements associated with those requirements. This can be done regardless of the conformance required by the PP or PP-Configuration. Omitting optional SFRs in an ST does not constitute “partial conformance” to a PP, and thus is allowed.

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.

D.4.6.2.1 How ISO/IEC 15408 supports this translation

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

a) by providing a pre-defined precise “language” designed to describe exactly 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 7.4.

b) by providing operations: mechanisms that allow the ST author to modify the SFRs to provide a more accurate translation of the Security Objectives for the TOE. This document defines the four allowed operations: assignment, selection, iteration, and refinement. These are described further in 7.2.

c) by providing dependencies: a mechanism that supports a more complete translation to SFRs. In ISO/IEC 15408-2 language, an SFR can have a dependency on other SFRs. This signifies that if an

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 7.3.

D.4.6.2.2 Relation between SFRs and Security Objectives

The ST also contains 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.

D.4.6.2.2.1 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 can trace to the same security objective for the TOE, indicating that the combination of those security requirements meets that security objective for the TOE.

D.4.6.2.2.2 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.

In cases where SFRs very closely resemble Security Objectives for the TOE, the demonstration can be much simpler.

D.4.6.3 Security assurance requirements (SARs)

The SARs are a description of how the TOE is to be evaluated. This description uses a standardized language for two reasons:

- to provide an exact description of how the TOE is to be evaluated. Using a standardized language assists in creating an exact description and avoids ambiguity.
- to allow comparison between two STs. As different ST authors could use different terminology in describing the evaluation, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

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 ST author to modify the SARs. ISO/IEC 15408 has four operations: assignment, selection, iteration, and refinement. These are described further in 7.2.

b) by providing dependencies: a mechanism that supports a more complete translation to SARs. In ISO/IEC 15408-3 language, an SAR can have a dependency on other SARs. This signifies that if an ST uses that SAR, it generally needs to use those other SARs as well. This makes it much harder for the ST author to overlook including necessary SARs and thereby improves the completeness of STs. Dependencies are described further in 7.3.

D.4.6.3.1 SARs and the security requirement rationale

The ST also contains a security requirements rationale that explains why the chosen set of SARs was deemed appropriate. There are no specific requirements for this explanation. The goal for this explanation is to allow the ST readers to understand the reasons why this particular set was chosen.

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. Some SARs relate to an operational TOE such as secure delivery process and flaw remediation.

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

D.4.6.4 Security requirements: conclusion

In the Security Problem Definition section of the 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.

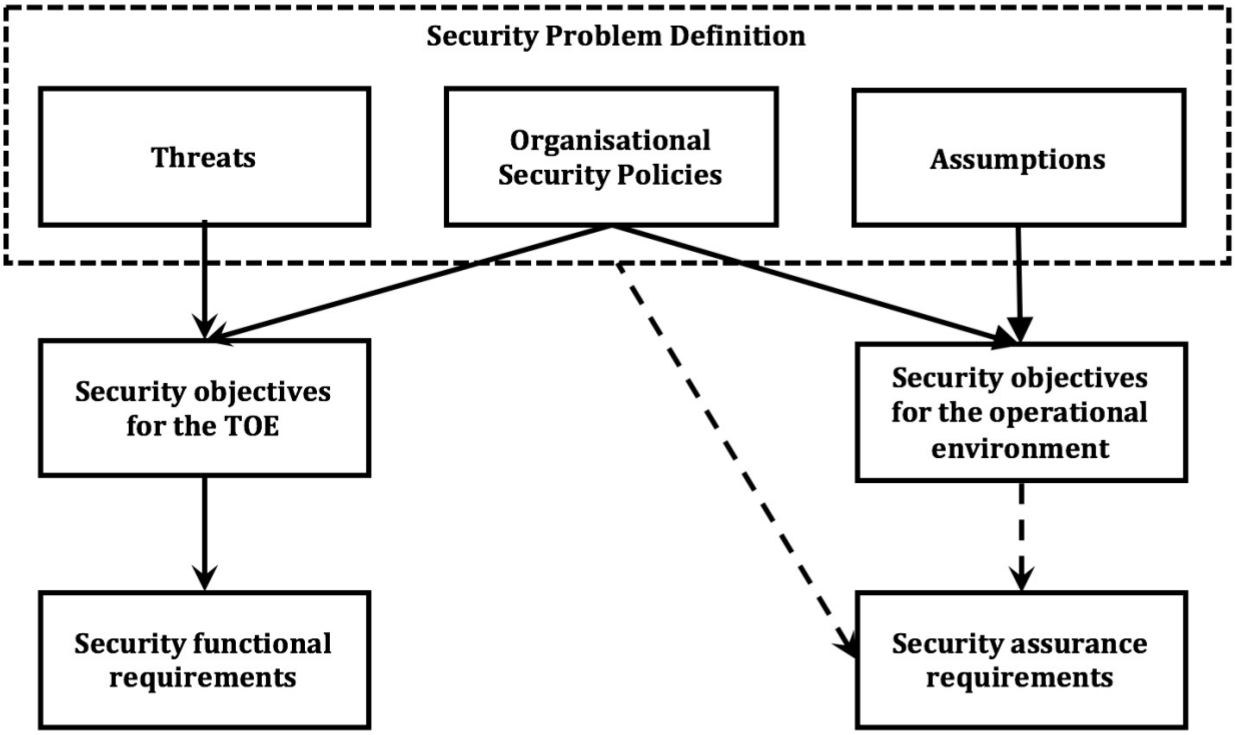

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the TOE
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure D.3 — Relations between the SPD, the Security Objectives, and the security requirements

In the security requirements section of the ST, 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 must be in line with the security expectations derived from the SPD. The explanation for SAR selection can 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 an 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 can be 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 D.3.

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.

D.4.7 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 must 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.

D.4.8 Referring to other standards in an ST

In some cases, an ST 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 an ST. 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 developer 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

].

Conformance to the standard as part of the fulfilment of the SFR by the TOE is then assessed in one of the following ways:

1) If an explicit Evaluation Activity has been defined for the SFR in accordance with the ISO/IEC 15408-4 framework, then the evaluator actions in that Evaluation Activity are carried out;

2) 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. This means that, as with any other aspect of an SFR during ADV: Development and ATE: Tests it is analysed, by design analysis and tests, to determine that the SFR is completely and fully implemented in the TOE.”

If reference to only a certain part of a standard is desired, that part must be unambiguously stated in the SFR refinement.

c) As a technical standard referenced in the TOE summary specification.

The TOE summary specification is only considered as an explanation of how the SFRs are realized and is not strictly used as a strict implementation requirement like the SFRs or the documents delivered for ADV: Development. So, the evaluator could detect an inconsistency if the TSS references a technical standard and this is not reflected in ADV: Development documentation, but there is no routine activity to test fulfilment of the standard.

EXAMPLE

TSS content
“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 The ST author is reminded that referring to a standard in SFRs can impose a significant burden on a developer developing a TOE to meet that ST (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.

D.4.9 Direct Rationale STs

D.4.9.1 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 SPD and, where appropriate, Security Objectives for the operational environment, to the SFRs.

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.

Because of its directness and additional description of SFRs in natural language, this type of ST can be easier for end-users and risk owners to understand and use.

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.4.9.2 and D.4.9.3, below.

The content of a Direct Rationale ST is shown in Figure D.4

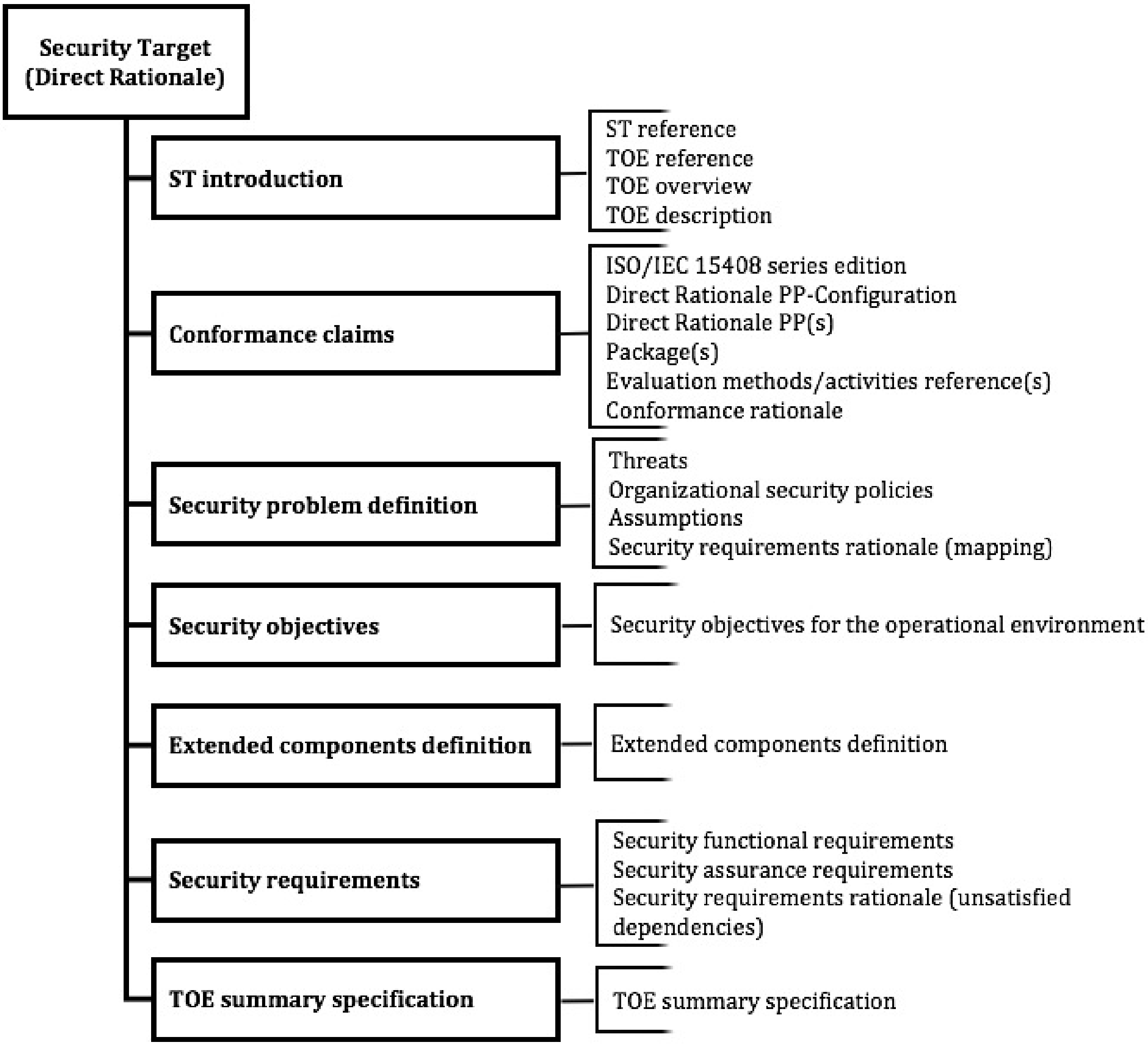

Security Target (Direct Rationale)
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
ISO/IEC 15408 series edition
Direct Rationale PP-Configuration
Direct Rationale PP(s)
Package(s)
Evaluation methods/activities reference(s)
Conformance rationale
Security problem definition
Threats
Organizational security policies
Assumptions
Security requirements rationale (mapping)
Security objectives
Security objectives for the operational environment
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale (unsatisfied dependencies)
TOE summary specification
TOE summary specification

Figure D.4 — Contents of a Direct Rationale ST

D.4.9.2 Conformance claims (ASE_CCL) for Direct Rationale STs

A Direct Rationale ST can only claim conformance to one or more other Direct Rationale PPs (see 11.2.1 and Annex B).

A Direct Rationale ST can only claim conformance to a PP-Configuration if that PP-Configuration also uses the Direct Rationale approach. (see 11.2.1)

D.4.9.3 Security Problem Definition (ASE_SPD) for Direct Rationale STs

D.4.9.3.1 General

A Direct Rationale ST has the following differences when compared to an 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 SPD-elements to the SFRs and to any Security Objectives for the operational environment 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 an ST that contain Security Objectives for the TOE, 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, 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.

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.

D.4.9.3.2 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.

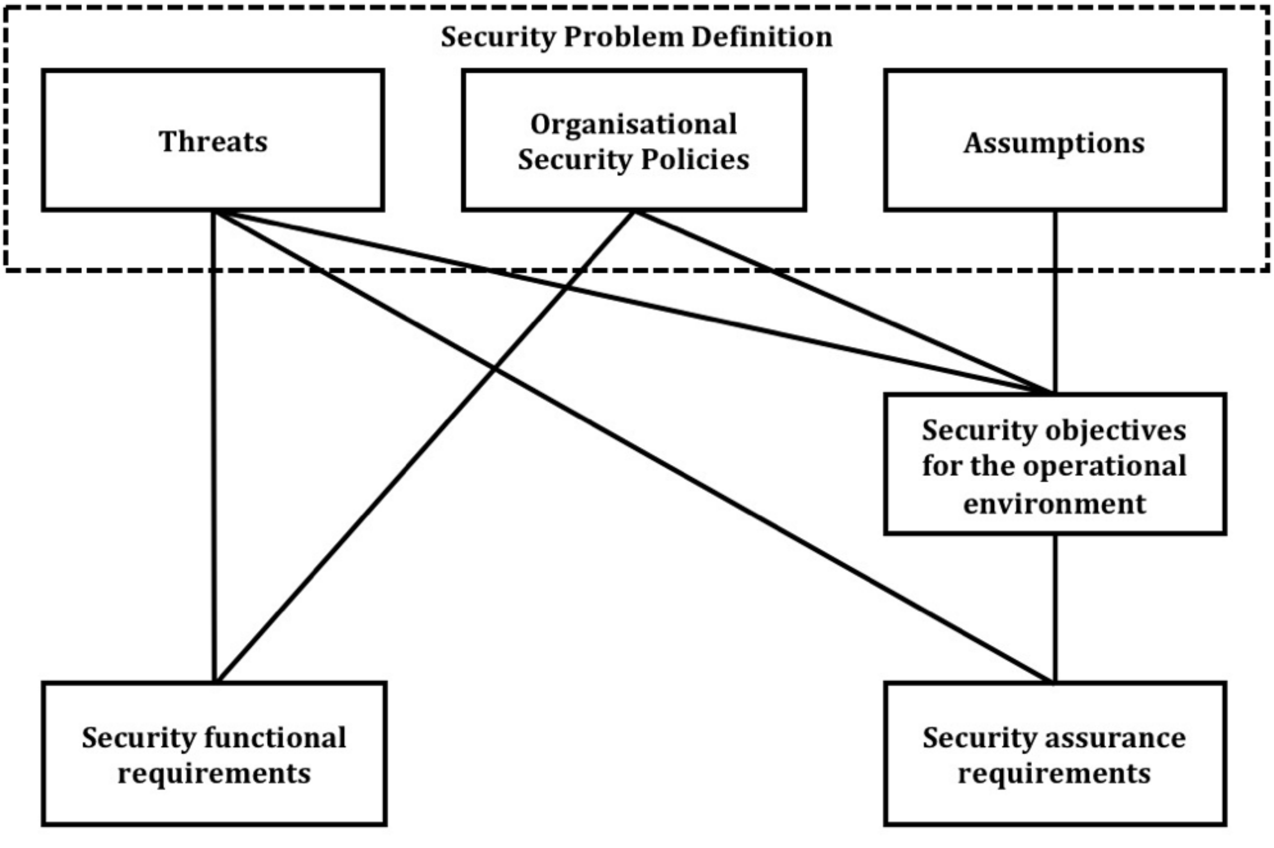

Security Problem Definition
Threats
Organisational Security Policies
Assumptions
Security objectives for the operational environment
Security functional requirements
Security assurance requirements

Figure D.5 shows the more direct specification of the SFRs that is used in the Direct Rationale approach.

Figure D.5 — Relations between the security problem definition, the Security Objectives, and the security requirements for Direct Rationale STs

Annex E
(informative)

Guidance for Operations

E.1 Introduction

Protection Profiles, PP-Modules, Packages and Security Targets can contain pre-defined security requirements, as well as providing PP and ST authors the ability to extend the component lists in some circumstances. By applying operations to these security components, they can be tailored precisely to the author's needs.

E.2 Examples of operations

E.2.1 General

The four types of operations are given in 7.2. Examples of the various operations are described below:

E.2.2 The iteration operation

As described in 7.2.1, the iteration operation can be performed on every component. The PP/ST author performs an iteration operation by including multiple requirements based on the same component. Each iteration of a component is 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 are uniquely identified to allow clear rationales and tracings to and from these requirements.

> EXAMPLE A typical example of iteration is:
>
> 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 and DSA signatures) (FCS_COP.1(1))
>
> Cryptographic operation (TLS/SSL: symmetric operations) (FCS_COP.1(2))

E.2.3 The assignment operation

As described in 7.2.2, an assignment operation occurs where a given component contains an element with a parameter that can be set by the PP/ST author. The parameter can be an unrestricted variable, or a rule that narrows the variable to a specific range of values.

> EXAMPLE
>
> An example of an element with an assignment is:
>
> FIA_AFL.1.2 "When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: list of actions]."

E.2.4 The selection operation

As described in 7.2.3 the selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

> EXAMPLE 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..."

7.2.3 also describes the notion of a selection-based SFR. The following is an example of such an SFR; FTP_ITC.1.1 is the SFR with the selection and FCS_IPSEC.1 is the selection-based SFR.

EXAMPLE

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.

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 [...]

E.2.5 The refinement operation

As described in 7.2.4, the refinement operation can be performed on every requirement. The PP/ST author performs a refinement by altering that requirement.

EXAMPLE 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 first rule for a refinement is that a TOE meeting the refined requirement also meets the unrefined requirement in the context of the PP/ST (i.e. a refined requirement must be "stricter" than the original requirement)

The only exception to this rule is that a PP/ST author is allowed to refine a SFR to apply to some but not all subjects, objects, operations, security attributes and/or external entities.

EXAMPLE 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 given is that the refinement must be related to the original component. For example, refining an audit component with an extra element on prevention of electromagnetic radiation is not allowed.

A special case of refinement is an editorial refinement, where a small change is 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 An example of an editorial refinements 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**".

E.3 Organization of components

E.3.1 General

ISO/IEC 15408-2 and ISO/IEC 15408-3 have organized the components in into hierarchical structures:

- Classes, consisting of
- Families, consisting of
- Components, consisting of
- Elements.

This organization into a hierarchy of class - family - component - element is provided to assist consumers, developers, and evaluators in locating specific components.

ISO/IEC 15408 (all parts) present functional and assurance components in the same general hierarchical style and use the same organization and terminology for each.

E.3.2 Class

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.

E.3.3 Family

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.

E.3.4 Component

EXAMPLE

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

E.3.5 Element

EXAMPLE

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

E.4 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 evaluatable (it is possible to systematically demonstrate whether a requirement based on that component holds for a TOE). Extended components must 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 might have to be included;

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

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

EXAMPLE An example of the ADV development family is the Functional Specification.

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 method for the component, similar to the method provided in ISO/IEC 18045.

Extended components can 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 must 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 can 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 must 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.

Annex F

(informative)

PP Conformance

F.1 General

A PP is intended to be used as a "template" for an ST. That is: the PP describes a set of user needs, while an ST that conforms to that PP describes a TOE that satisfies those needs.

NOTE 1 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 an ST vs. a PP. For clarity, this annex describes only the PP/ST case, but it holds also for the PP/PP case.

ISO/IEC 15408 (all parts) does not allow any form of partial conformance, so if PP conformance is claimed, the PP/ST must conform to the referenced PP(s) or PP-Configuration.

NOTE 2 In the case of selection-based SFRs, the inclusion or exclusion of these types of SFRs as outlined in ISO/IEC 15408-2 is still considered to be conformant with the PP.

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. That is, the PP states, in accordance with B.2.3, what the allowed types of conformance for the derivative ST/PPs are.

As indicated in 9.2.1, if a PP specifies exact conformance, then an ST can only claim exact conformance to that PP, and any other PP to which the ST claims conformance must 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 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 PP/ST is claiming conformance is applicable to each PP to which an PP/ST can claim conformance on an individual basis. This can mean that the PP/ST conforms strictly to some other PPs and demonstrably to other PPs. A PP/ST is only allowed to conform to a PP in an exact manner if the PP explicitly allows this. However, a PP/ST can always conform either demonstrably or strictly to a PP that requires either demonstrable or strict conformance.

NOTE 2: A PP/ST is only allowed to conform to a PP in an demonstrable manner if the PP explicitly allows this. This means that PP/STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP. In principle that means that the PP/ST can contain statements that vary from the PP, 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.

F.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 must 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.

F.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.

An ST instantiating strict conformance to a PP can still introduce additional restrictions to those given in the PP.

F.4 Exact conformance

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 an ST can claim conformance in combination with the subject PP and still maintain exact conformance;

b) PP-Modules that can 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) 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 cannot 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 an 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 an ST claims conformance to PP A.

As indicated above, it is allowed for an ST to claim exact conformance with multiple exact conformance PPs. Also, a PP-Configuration is allowed to include 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 can be claimed along with their PP, the conformance statement in the PP, described in B.2.3, can also include a statement specifying which PPs an ST author may simultaneously claim conformance to with the subject PP. All identified PPs must require exact conformance in their conformance statement and must 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 these are indistinguishable from non-Base PPs in this aspect). An example of an ST claiming conformance to multiple PPs is given to clarify this concept.

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

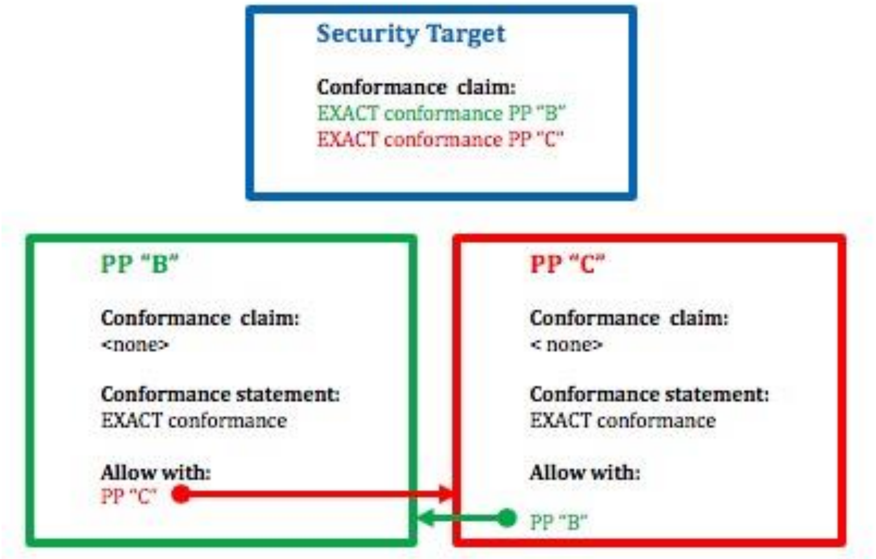


Figure F.1

Figure F.1 — Exact conformance of an ST to multiple PPs

Then the following would have to be true:

a) Both PP B and PP C would have to specific exact conformance in their conformance statement.

b) PP B would list PP C as allowed with PP B in its conformance statement.

c) PP C would list PP B as allowed with PP C in its conformance 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 the PP-Configurations. A PP-Module can identify a set of Base PPs; if one of the identified Base PPs has a conformance statement of exact conformance, then all of the Base PPs specified by the PP-Module must also have conformance statements specifying exact conformance. Further, in order to ensure that the PP-Modules are allowed for use with the Base PP, each Base PP specifies in its conformance statement the PP-Modules that are allowed to specify it as a Base PP 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 in the Allow with statement because it has implicitly done so by defining the PP as a Base PP.

Furthermore, a PP-Module also specifies which other PP-Modules or Protection Profiles in the PP-Configuration that are not included as one of the PP-Module's Base PPs can be used in combination with it in a PP-Configuration.

In exact conformance a PP can only claim conformance to one PP-Configuration. However, an ST can claim conformance to more than one PP-Configuration.

EXAMPLE 3

Figure F.2 describes a case for exact conformance involving both PPs and PP-Modules.

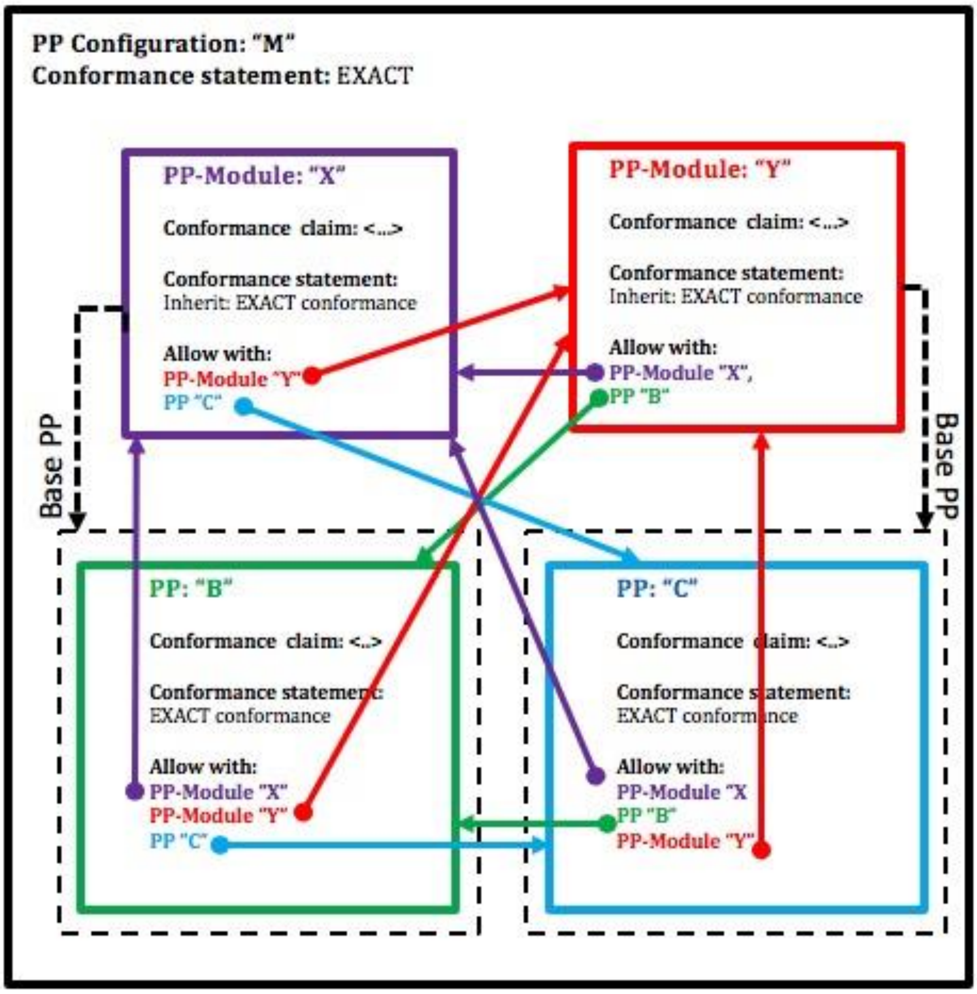


Figure F.2 — Exact conformance with a PP-Configuration including multiple PPs and PP-Modules

4440

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 Security Targets*

[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