INTERNATIONAL STANDARD

ISO/IEC 15408-1

Fourth edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 1: Introduction and general model

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:2022(E)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

The main changes are as follows:

— the document has been restructured;

— technical changes have been introduced:

  — the terminology has been reviewed and updated;

  — the exact conformance type has been introduced;

  — low assurance protection profiles (PPs) have been removed and direct rationale PPs have been introduced;

  — PP-Modules and PP-Configurations for modular evaluations have been introduced;

  — multi-assurance evaluation has been introduced.

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

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

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations 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.

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

The ISO/IEC 15408 series 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 the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/activities, 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 provides 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.

The ISO/IEC 15408 series 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. The ISO/IEC 15408 series may also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series 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 the ISO/IEC 15408 series. Some of these are identified below:

a) the ISO/IEC 15408 series 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) the ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied;

NOTE 1 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

c) the ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to 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 the ISO/IEC 15408 series. 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 the ISO/IEC 15408 series. In the case that independent assessment of mathematical properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied shall make provision for such assessments.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

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

This document introduces:

— the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;

— a description of the organization of security components throughout the model;

— the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;

— general information about the evaluation methods given in ISO/IEC 18045;

— guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;

— general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;

— information in regard to the scope of evaluation schemes.

2 Normative references

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

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

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

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

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 and ISO/IEC IEEE 24765 apply.

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

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

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

3.1
action
documented activity of the *evaluator* (3.45) or *developer* (3.33)

Note 1 to entry: Evaluator actions and developer actions are required by ISO/IEC 15408-3.

3.2
administrator
entity (3.36) that has a level of trust with respect to all policies implemented by the *TOE security functionality (TSF)* (3.92)

Note 1 to entry: Not all *protection profiles (PPs)* (3.68) or security targets (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 *target of evaluation (TOE)* (3.90). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment* (3.63).

3.3
adverse action
action (3.1) performed by a *threat agent* (3.91) on an *asset* (3.4)

3.4
asset
entity (3.36) that the owner of the *target of evaluation (TOE)* (3.90) presumably places value on

3.5
assignment
specification of an identified parameter in a functional or assurance component

3.6
assurance
grounds for confidence that a *target of evaluation (TOE)* (3.90) meets the *security functional requirements (SFRs)* (3.78)

3.7
assurance package
named set of *security assurance requirements* (3.76)

EXAMPLE "EAL 3".

3.8
attack potential
measure of the effort needed to exploit a vulnerability in a *target of evaluation (TOE)* (3.90)

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

3.9
attack surface
set of logical or physical interfaces to a target, consisting of points through which access to the target and its functions may be attempted

EXAMPLE 1 The casing of a payment terminal is a part of physical attack surface for that device.

EXAMPLE 2 The communications protocols available for connection to a network device are part of the logical attack surface for that network device.

3.10
augmentation
addition of one or more requirements to a package

Note 1 to entry: In case of a *functional package* (3.51), such an augmentation is considered only in the context of one package and is not considered in the context with other packages or *protection profiles (PPs)* (3.68) or *security targets (STs)* (3.82).

Note 2 to entry: In case of an *assurance package* (3.7), augmentation refers to one or more *security assurance requirements (SARs)* (3.76).

3.11
authorized user
entity (3.36) who may, in accordance with the *security functional requirements (SFRs)* (3.78), perform an operation on the *target of evaluation (TOE)* (3.90)

3.12
base component
independent entity (3.36) in a multi-component product that provides services and resources to one or more *dependent component(s)* (3.31)

Note 1 to entry: This applies in particular to '*composed TOEs*' (3.21) and 'composite products / *composite TOEs*' (3.25).

3.13
base Protection Profile
base PP
Protection Profile (3.68) specified in a *PP-Module* (3.71), as part of that PP-Module's *PP-Module Base* (3.72), used as a basis to build a *PP-Configuration* (3.69)

3.14
base PP-Module
PP-Module (3.71) specified in a different PP-Module, as part of that PP-Module's *PP-Module Base* (3.72), used as a basis to build a *PP-Configuration* (3.69)

Note 1 to entry: Specifying a base PP-Module in a PP-Module implicitly includes the base PP-Module's PP-Module Base.

3.15
base target of evaluation
base TOE
base component (3.12) which is itself the subject of an evaluation

Note 1 to entry: This applies in particular to *'composed TOEs'* (3.21) and 'composite products/*composite TOEs*' (3.25).

3.16
class
⟨taxonomy⟩ set of families that share a common focus

Note 1 to entry: Class is further defined in ISO/IEC 15408-2, which defines security functional classes and ISO/IEC 15408-3, which defines security assurance classes.

3.17
component
⟨taxonomy⟩ smallest selectable set of elements on which requirements may be based

3.18
component
<composition> *entity* (3.36) which provides resources and services in a product

3.19
component target of evaluation
component TOE
(evaluated) *target of evaluation (TOE)* (3.90) that is a component of another *composed TOE* (3.21)

3.20
composed assurance package
CAP
assurance package (3.7) consisting of components drawn predominately from the ACO *class* (3.16), representing a point on the pre-defined scale for composition assurance

3.21
composed target of evaluation
composed TOE
target of evaluation (TOE) (3.90) comprising solely two or more separately identified components with a security relationship between their *TOE security functionality (TSFs)* (3.92)

Note 1 to entry: Each of the separately identified components is itself a TOE.

3.22
composed evaluation
evaluation of a *composed TOE* (3.21) using the specific evaluation technique applicable to composed TOEs

Note 1 to entry: This evaluation technique refers to the ACO assurance *class* (3.16) that is defined in ISO/IEC 15408-3.

3.23
composite evaluation
evaluation of a *composite TOE/product* (3.25) using the specific composite evaluation technique

Note 1 to entry: This evaluation technique refers to the COMP related assurance families that are specified in ISO/IEC 15408-3 for the ADV, ASC, ASE, ATE and AVA *classes* (3.16).

3.24
composite product
product comprised of two or more components which can be organized in two layers: a layer of one already evaluated base *component (base TOE)* (3.15) and a layer of one *dependent component* (3.31)

3.25
composite target of evaluation
composite TOE
part of a *composite product* (3.24) including the *base TOE* (3.15) and the *dependent component* (3.31)

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

Note 2 to entry: A composite TOE can contain parts that are independent from the *base component* (3.12) or base TOE respectively. For simplification, such parts are considered as belonging to the dependent component.

Note 3 to entry: The *composite evaluation* (3.23) can be applied as many times as necessary to a multi-component/ multi-layered product, in an incremental approach.

3.26
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 24765:2017, 3.779 1]

3.27
configuration management system
set of procedures and tools (including their documentation) used by a *developer* (3.33) to develop and maintain configurations of their products during their life-cycles

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

3.28
counter, verb
act on or respond to a particular threat so that the threat is eradicated or mitigated

3.29
demonstrable conformance
DC
relation between a *protection profile (PP)* (3.68)/*security target* (3.82) (PP/ST) and a PP, or an ST and a *PP-Configuration* (3.69), where the PP/ST provides an equivalent or more restrictive solution that solves the generic security problem in the PP/PP-Configuration

3.30
dependency
relationship between components such that a *protection profile (PP)* (3.68), *security target (ST)* (3.82), *functional package* (3.51) or *assurance package* (3.7) including a component also includes any other components that are identified as being depended upon or include a rationale as to why they are not

3.31
dependent component
dependent entity (3.36) in a multi-component product that relies on the provision of services and resources by one or more *base components* (3.12)

Note 1 to entry: This applies in particular to *'composed TOEs'* (3.21) and 'composite products / *composite TOE'* (3.25).

3.32
dependent target of evaluation
dependent TOE
dependent component (3.31) which is itself the subject of an evaluation

Note 1 to entry: This applies only to *'composed TOEs'* (3.21) and not to 'composite products / *composite TOEs'* (3.25).

3.33
developer
organization responsible for the development of the *target of evaluation (TOE)* (3.90)

3.34
direct rationale
type of *Protection Profile* (3.68), *PP-Module* (3.71) or *Security Target* (3.82) in which the *security problem definition (SPD)* (3.80) elements are mapped directly to the *security functional requirements (SFRs)* (3.78) and possibly to the *security objectives* (3.79) for the *operational environment* (3.63)

Note 1 to entry: Direct rationale does not include security objectives for the *target of evaluation (TOE)* (3.90).

3.35
element
⟨taxonomy⟩ self-contained description of a security need assigned to *security assurance requirement (SAR)* (3.76) or *security functional requirement (SFR)* (3.78)

3.36
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.

3.37
evaluation
assessment of a *PP-Configuration* (3.69), *protection profile (PP)* (3.68), a *security target (ST)* (3.82), or a *target of evaluation (TOE)* (3.90), against defined criteria

3.38
evaluation activity
EA
activity derived from one or more work units

Note 1 to entry: Work units are defined in ISO/IEC 18045.

Note 2 to entry: Derivation mechanisms are defined in ISO/IEC 15408-4.

3.39
evaluation assurance level
EAL
well-formed package of *security assurance requirements* (3.76) representing a point on the pre-defined assurance scale

Note 1 to entry: EALs are defined in ISO/IEC 15408-5.

3.40
evaluation authority
body operating an *evaluation scheme* (3.42)

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

3.41
evaluation method
EM
set of one or more *evaluation activities* (3.38) for application in a specific context

3.42
evaluation scheme
rules, procedures and management to carrying evaluations of IT product security

Note 1 to entry: An evaluation scheme implements all parts of the ISO/IEC 15408 series.

3.43
evaluation technical report
ETR
documentation of the *overall verdict* (3.66) and its justification, produced by the *evaluator* (3.45), and submitted to an *evaluation authority* (3.40)

3.44
evaluation technical report for composite evaluation
ETR for composite evaluation
ETR_COMP
documentation intended to be used within the *composite evaluation* (3.23) approach and derived by the *base component* (3.12) *evaluator* (3.45) from the full *evaluation technical report (ETR)* (3.43) for the evaluated base component

Note 1 to entry: The ETR for composite evaluation belongs to the base component and its evaluation and is used for the evaluation of a composite product with such base component when using the composite evaluation approach.

Note 2 to entry: The ETR for composite evaluation related to a base component is set up to provide sufficient information for a composite evaluation of a composite product that integrates such already evaluated base component. It enables the composite product *evaluator* (3.45) and the respective composite product *evaluation authority* (3.40) to understand the attack paths and the tests that have been considered and performed for the base component and the effectiveness of the countermeasures implemented by the base component.

3.45
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, 3.5]

3.46
exact conformance
EC
hierarchical relationship between a *protection profile (PP)* (3.68) or *PP Configuration* (3.69) and a *security target (ST)* (3.82) where all the requirements in the ST are drawn only from the PP/PP-Configuration

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

3.47
exploitable vulnerability
weakness in the *target of evaluation (TOE)* (3.90) that can be used to violate the *security functional requirements (SFRs)* (3.78) in the *operational environment* (3.63) for the TOE

3.48
extended security requirement
security requirement developed according to the rules in this document, but which are not listed in any part of the ISO/IEC 15408 series

Note 1 to entry: An extended security requirement preserves the form and syntax described in ISO/IEC 15408-2.

Note 2 to entry: Extended security requirements can be defined by authors of *security target (ST)* (3.82) or *protection profile (PP)* (3.68) or *PP-Module* (3.71).

3.49
external entity
user
human technical system or one of its components interacting with the *target of evaluation (TOE)* (3.90) from outside of the TOE boundary

3.50
family
⟨taxonomy⟩ set of components that shares a similar goal but differs in emphasis or rigour

3.51
functional package
named set of *security functional requirements* (3.78) that may be accompanied by a *security problem definition (SPD)* (3.80) and *security objectives* (3.79) derived from that SPD

3.52
global assurance package
assurance package (3.7) that applies to the entire *target of evaluation (TOE)* (3.90) in a *multi-assurance evaluation* (3.60)

Note 1 to entry: Global assurance package can contain extended assurance components.

3.53
guidance documentation
documentation that describes the delivery, preparation, operation, management and/or use of the *target of evaluation (TOE)* (3.90)

3.54
implementation representation
least abstract representation of the *TOE security functionality (TSF)* (3.92), specifically the one that is used to create the TSF itself without further design *refinement* (3.73)

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.

3.55
internally consistent, adj.
no apparent contradictions exist between any aspects of an *entity* (3.36)

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.

3.56
interpretation
clarification or amplification of a standard or an evaluation scheme requirement

3.57
iteration
use of the same component to express two or more distinct requirements

3.58
layering
design technique where separate groups of components are hierarchically organized to have separate responsibilities such that a group of components depends on groups of components below it in the hierarchy for services, and provides its services to the groups of components above it

3.59
module
architectural unit specified at a level suitable for implementation of the unit

Note 1 to entry: Properties related to division of a *target of evaluation (TOE)* (3.90) into modules are described in ISO/IEC 15408-3, in the ADV_TDS and ADV_INT families.

3.60
multi-assurance evaluation
evaluation of a *target of evaluation (TOE)* (3.90) using a *PP-Configuration* (3.68) where each PP-Configuration component is associated with its own set of assurance requirements

Note 1 to entry: At least one of the PP-Configuration components contains a different set of assurance requirements to the others.

3.61
object
entity (3.36) in the *target of evaluation (TOE)* (3.90) that contains or receives information, and upon which subjects perform operations

3.62
operation
⟨on an object⟩ specific type of *action* (3.1) performed by a subject on an object

3.63
operational environment
environment in which the *target of evaluation (TOE)* (3.90) is operated, consisting of everything that is outside the TOE boundary

3.64
optional Security Functional Requirement
optional SFR
security functional requirement (SFR) (3.78) in a *Protection Profile (PP)* (3.68), *functional package* (3.51), or *PP-Module* (3.71) that contributes to a stated aspect of the PP's security problem description but whose inclusion in a conformant PP's or *security target (ST's)* (3.82) list of SFRs is not mandatory

Note 1 to entry: An optional SFR can address appropriate *security problem definition (SPD)* (3.80) elements threat(s) and/or organizational security policies (OSPs) stated in the main body of the PP, functional package, or PP-Module, or reference associated SPD elements/objectives that themselves are optional (in that they are addressed solely by the optional SFR).

3.65
organizational security policy
OSP
set of security rules, procedures, or guidelines for an organization

Note 1 to entry: A policy can pertain to a specific *operational environment* (3.63).

3.66
overall verdict
statement issued by an *evaluator* (3.45) with respect to the result of an evaluation

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

3.67
potential vulnerability
suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the *security functional requirements (SFRs)* (3.78).

3.68
Protection Profile
PP
implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type

3.69
Protection Profile Configuration
PP-Configuration
implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type containing at least one *protection profile (PP)* (3.68) and an additional non-empty set of PPs and *PP-Modules* (3.71) (with the associated PP-Modules Bases)

3.70
Protection Profile Configuration component
PP-Configuration component
Protection Profile (PP) (3.68) or *PP-Module* (3.71) included in a *PP-Configuration* (3.69)

3.71
Protection Profile module
PP-Module
implementation-independent statement of security needs for a *target of evaluation (TOE)* (3.90) type complementary to one or more base *Protection Profiles* (3.68) and possibly some *base PP-Modules* (3.14)

3.72
Protection Profile Module Base
PP-Module Base
set of either *PP-Modules* (3.71) or *Protection Profiles (PPs)* (3.68) or both, specified by a PP-Module as a basis for building a *PP-Configuration* (3.69)

Note 1 to entry: The notion of a PP-Module Base is iterative in that the base of a PP-Module can contain another PP-Module with its own base, with that base containing a PP-Module. However, this "chain" terminates with a PP-Module that has only PP(s) as its base.

3.73
refinement
addition of details to a security component

3.74
residual vulnerability
weakness that cannot be exploited in the *operational environment* (3.63) for the *target of evaluation (TOE)* (3.90), but that can be used to violate the *security functional requirements (SFRs)* (3.78) by an attacker with greater *attack potential* (3.8) than is anticipated in the operational environment for the TOE

3.75
role
pre-defined set of rules establishing the allowed interactions between a user and the *target of evaluation (TOE)* (3.90)

3.76
security assurance requirement
SAR
security requirement that refers to the conditions and processes for the development and delivery of the *target of evaluation (TOE)* (3.90), and the *actions* (3.1) required of *evaluators* (3.45) with respect to evidence produced from these conditions and processes

3.77
security attribute
property of subjects, users, objects, information, sessions and/or resources that is used in defining the *security functional requirements (SFRs)* (3.78) and whose values are used in enforcing the SFRs

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

3.78
security functional requirement
SFR
security requirement, which contributes to fulfil the *target of evaluation (TOE)* (3.90) *security problem definition (SPD)* (3.80) as defined in a specific *security target (ST)* (3.82) or in a *protection profile (PP)* (3.68)

Note 1 to entry: A security functional requirement can be addressed directly as in the *direct rationale* (3.34) model, or indirectly, through the *security objectives* (3.79) for the TOE, as in the general model.

3.79
security objective
statement of an intent to *counter* (3.28) identified threats and/or satisfy identified organization security policies and/or assumptions

3.80
security problem
security problem definition
SPD
statement, which in a formal manner defines the nature and scope of the security that the *target of evaluation (TOE)* (3.90) 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* (3.63), the organizational security policies (OSPs) enforced by the TOE and its operational environment, and the assumptions that are upheld for the operational environment of the TOE.

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

3.81
security requirement
requirement, which is part of a *target of evaluation (TOE)* (3.90) security specification as defined in a specific *security target* (ST) (3.82) or in a *protection profile (PP)* (3.68)Note 1 to entry:
Requirements are stated in a language, i.e. form and syntax, specified in the ISO/IEC 15408 series.

3.82
Security Target
ST
implementation-dependent statement of security requirements for a *target of evaluation (TOE)* (3.90) based on a *security problem definition* (3.80)

3.83
selection
specification of one or more items from a list in a component

3.84
selection-based security functional requirement
selection-based SFR
security functional requirement (SFR) (3.78) in a *Protection Profile (PP)* (3.78), *PP-Module* (3.71), or *functional package* (3.51) that contributes to a stated aspect of the PP's, PP-Module's or functional package's *security problem definition* (3.80) that is to be included in a conformant PP or ST if a selection choice identified in the PP/PP-Module/functional package indicates that it has an associated selection-based SFR

3.85
single-assurance evaluation
evaluation of a *target of evaluation (TOE)* (3.90) using one set of assurance requirements

3.86
strict conformance
SC
hierarchical relationship between a *protection profile (PP)* (3.68) and a PP/*security target (ST)* (3.82) where all the requirements in the PP also exist in the PP/ST

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

3.87
sub-TOE security functionality
sub-TSF
combined functionality of all hardware, software, and firmware of a *target of evaluation (TOE)* (3.90) that is relied upon for the correct enforcement of the security functional requirements (SFRs) defined in one *PP-Configuration* (3.69) component

Note 1 to entry: This set of SFRs is closed by dependencies, objectives, and *security problem definition (SPD)* (3.80) elements in the PP-Configuration component.

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

Note 3 to entry: Each sub-TSF is associated with its own set of security assurance requirements (SARs) in a multi-assurance PP-Configuration/ST. In the rest of the document, a set of SARs can be an *assurance package* (3.7).

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

3.88
subject
entity (3.36) in the *target of evaluation (TOE)* (3.90) that performs operations on objects

3.89
tailoring
addition of one or more functional requirements to a *functional package* (3.51), and/or the addition of one or more selections to a *security functional requirement (SFR)* (3.78) in a functional package

Note 1 to entry: Such tailoring is considered only in the context of one package and is not considered in the context with other packages, *protection profiles (PPs)* (3.68), or PP-Modules.

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

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

3.90
target of evaluation
TOE
set of software, firmware and/or hardware possibly accompanied by guidance, which is the subject of an evaluation

3.91
threat agent
entity (3.36) that has potential to exercise adverse *actions* (3.3) on *assets* (3.4) protected by the *target of evaluation (TOE)* (3.90)

3.92
TOE security functionality
TSF
combined functionality of all hardware, software, and firmware of a *target of evaluation (TOE)* (3.90) that is relied upon for the correct enforcement of the *security functional requirements (SFRs)* (3.78)

3.93
TOE type
set of characteristics common to a group of *target of evaluations (TOEs)* (3.90)

Note 1 to entry: The TOE type can be more explicitly defined in a *protection profile (PP)* (3.68).

3.94
translation
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 *security functional requirement (SFR)* (3.78) expressed in standardized language can also be translated back to the *security objectives* (3.79).

3.95
vulnerability
weakness in the *target of evaluation (TOE)* (3.90) that can be used to violate the *security functional requirements (SFRs)* (3.78) in some environment

4 Abbreviated terms

AP	assurance package
API	application programming interface
CAP	composition assurance package
CD	compact disk
CM	configuration management
COMP	composite product assurance package
DAC	discretionary access control
DC	demonstrable conformance
DPA	differential power analysis
DRBG	deterministic random bit generator
EA	evaluation activity
EAL	evaluation assurance level
EC	exact conformance
EM	evaluation method
EMS	electromagnetic spectrum
ETR	evaluation technical report
GAP	global assurance package

GB	gigabyte
GHz	gigahertz
GUI	graphical user interface
HSM	hardware security module
HTTPS	hypertext transfer protocol secure
IC	integrated circuit
IOCTL	input output control
IP	internet protocol
IPsec	IP security (protocol)
IT	information technology
LDAP	lightweight directory access protocol
MAC	mandatory access control
MB	megabyte
MBps	megabytes per second
OR	observation report
OS	operating system
OSP	organizational security policy
OTP	one-time programmable
PC	personal computer
PCI	peripheral component interconnect
PKI	public key infrastructure
PP	protection profile
PPA	protection profile assurance package
RAM	random access memory
RBG	random bit generator
RNG	random number generator
RPC	remote procedure call
SAR	security assurance requirement
SC	strict conformance
SFP	security function policies
SFR	security functional requirement

SPA	simple power analysis
SPD	security problem definition
SSH	secure shell
ST	security target
STA	security target assurance package
TCP	transmission control protocol
TLS	transport layer security
TOE	target of evaluation
TSF	TOE security functionality
TSFI	TSF interface
USB	universal serial bus
VPN	virtual private network

5 Overview

5.1 General

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

5.2 ISO/IEC 15408 series description

5.2.1 General

The ISO/IEC 15408 series is presented as a set of distinct but related parts as identified below:

a) **ISO/IEC 15408-1, Introduction, and general model** is the introduction to the ISO/IEC 15408 series. 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 (SFRs) 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 the ISO/IEC 15408 series. ISO/IEC 18045 is fundamental to ISO/IEC 15408-4;

e) **ISO/IEC 15408-5, Pre-defined packages of security requirements** provides packages of security assurance and SFRs 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 the application of the ISO/IEC 15408 series, a justification shall be provided whenever the recommended option is not chosen.

In support of the ISO/IEC 15408 series, other documents have been published. The Bibliography provides a list of supportive documents.

NOTE ISO/IEC 18045 provides the baseline methodology for IT security evaluations performed in accordance with the ISO/IEC 15408 series.

5.2.2 Audience

5.2.2.1 General

There are five main groups with a general interest in evaluation of the security properties of TOEs: consumers (risk owners), developers, technical working groups, evaluators and others. The information presented in the ISO/IEC 15408 series has been structured to support the needs of all of these groups which are considered to be the principal users of the ISO/IEC 15408 series. The groups can benefit from the criteria as explained in 5.2.2.2 through 5.2.2.6.

5.2.2.2 Consumers (Risk owners)

The ISO/IEC 15408 series 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.

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

5.2.2.3 Developers

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

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

5.2.2.4 Technical working groups

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

5.2.2.5 Evaluators

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

NOTE The ISO/IEC 15408 series does not specify procedures to be followed in carrying out those actions. More information on these procedures can be found in Clause 13.

5.2.2.6 Others

While the ISO/IEC 15408 series 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 the ISO/IEC 15408 series 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 can 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;

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

Table 1 presents the interest of each part of ISO/IEC 15408 series to each of the audience groupings.

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

ISO/IEC 15408 parts	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 1	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications and security problem definitions (SPDs) for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for TOEs.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use for the development of security specifications for packages, PPs, PP-Modules and PP-Configurations.	Should use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition. Shall use when evaluating PPs, PP-Configurations and STs.	May use for background information, reference purposes, and for guidance on the structure of PPs, PP-Modules, PP-Configurations, STs and composition.

Table 1 *(continued)*

ISO/IEC 15408 parts	Consumers (Risk owners)	Developers	Technical working groups	Evaluators	Others
Part 2	Shall use for guidance and reference when formulating statements of security functional components for their risk-environment.	Shall use for reference when interpreting statements of security functional components in packages, PPs and PP-Modules. Shall use when developing STs. May use when formulating security functionality for IT products.	Shall use for reference when formulating statements of security functional components in packages, PPs and PP-Modules.	Shall use for reference when evaluating security functional components given in packages, PPs and PP-Modules or security functional requirements (SFRs) in STs.	May use for reference when reviewing security functional components given in packages, PPs and PP-Modules or security functional requirements (SFRs) in STs.
Part 3	Shall use for guidance and reference when determining the security assurance required for their risk-environment.	Shall use for reference when interpreting statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations. Shall use when developing STs May use when formulating or improving development processes.	Shall use for reference when formulating statements of security assurance components in packages, PPs, PP-Modules and PP-Configurations.	Shall use for reference when evaluating security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.	May use for reference when reviewing security functional components given in packages, PPs, PP-Modules and PP-Configurations or security assurance requirements in STs.
Part 4	Should use for reference and background information in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation method(s) and/or activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities.	Should use for reference purposes and for guidance in the structure of evaluation methods and activities. Should use when formulating specific evaluation methods and activities.	May use for reference purposes and for guidance in the structure of evaluation methods and activities.
Part 5	Should use for reference in determining the contents of any claimed pre-defined packages of security requirements.	Shall use when developing STs claiming conformance to pre-defined packages of security requirements. Shall use for reference when preparing a TOE for evaluation conformant to pre-defined packages of security requirements.	Shall use when developing PPs, PP-Modules and PP-Configurations claiming conformance to pre-defined packages of security requirements.	Shall use for reference when evaluating PPs, PP-Modules and PP-Configurations or STs claiming conformance to pre-defined packages of security requirements.	May use for reference in determining the contents of any claimed pre-defined packages of security requirements.

5.3 Target of evaluation (TOE)

5.3.1 General

The ISO/IEC 15408 series is flexible in what is evaluated and is therefore not tied to the boundaries of IT products as commonly understood. Therefore, in the context of evaluation the ISO/IEC 15408 series 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 can never be made into a product, or a combination of these.

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

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

— a network device;

— a software application;

— an operating system;

— a virtualization system;

— an integrated circuit;

— the cryptographic co-processor of an integrated circuit;

— an application for a mobile device;

— a database application excluding the remote client software normally associated with that database application.

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

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

— a mobile device;

— gateways and hubs;

— a software application in combination with an operating system;

— a multi-function device, such as a multi-function printer;

— a Hardware Security Module (HSM).

5.3.2 TOE boundaries

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

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

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

5.3.3 Different representations of the TOE

In the ISO/IEC 15408 series, 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, e.g. 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 the ISO/IEC 15408 series, the context determines the representation that is described.

5.3.4 Different configurations of the TOE

In general, IT products can be configured in many ways with different options enabled or disabled. During an evaluation performed in accordance with the ISO/IEC 15408 series, it will be determined whether a TOE meets certain requirements. It is often the case that the guidance part of the TOE constrains the possible configurations of the TOE, i.e. the guidance for the TOE can be different from the general guidance of the IT product.

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

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.

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

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

5.3.5 Operational environment of the TOE

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

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

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

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

EXAMPLE Secure key generation and injection premises and processes is an example of a security objective for the operational environment which supports the TOE cryptographic services specified using FCS components from ISO/IEC 15408-2.

5.4 Presentation of material in this document

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

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

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

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

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

6 General model

6.1 Background

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

The ISO/IEC 15408 series 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 the ISO/IEC 15408 series. However, the concepts themselves are not intended to restrict the class of IT security problems to which the ISO/IEC 15408 series is applicable. Clause 6 assumes that the reader has knowledge of IT security and it is not intended to act as a tutorial in this area.

6.2 Assets and security controls

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

EXAMPLE 1 An example of an asset is the contents of a file or a server.

Examples of operational environments in the context of such an asset are:

— a data centre where the server is installed;

— a computer network connected to the Internet which connects the server to the world;

— a LAN which connects the server to other servers and/or workstations;

— the every-day environment of a user who uses information from the server or a particular file;

— a general office environment which provides communication facilities to the server and/or a particular file.

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 can 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.

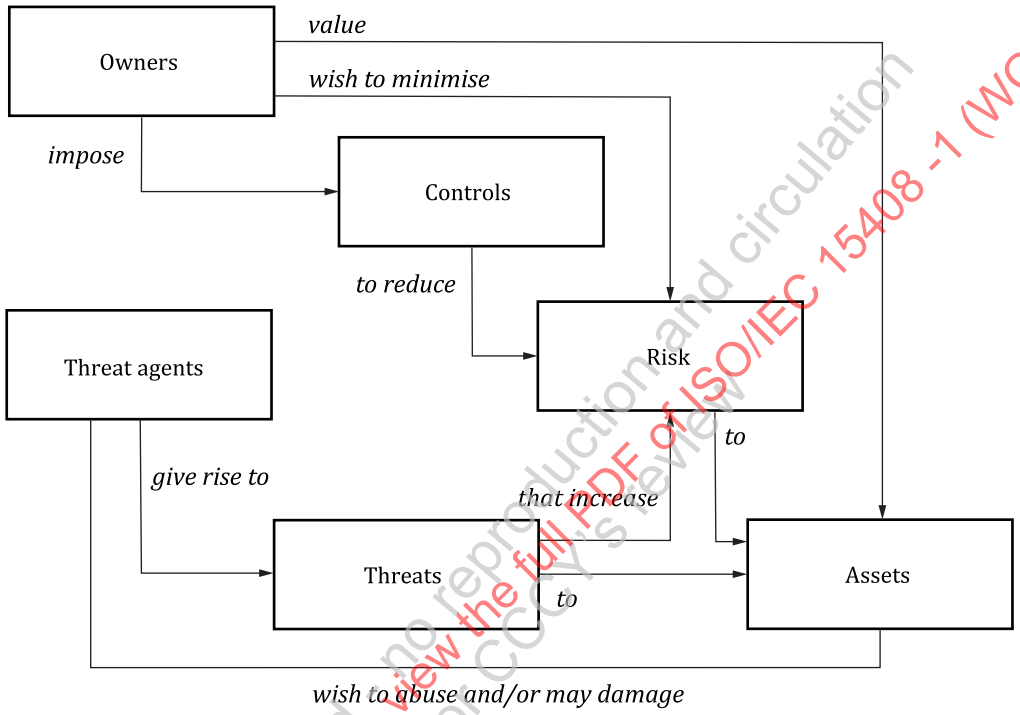

Figure 1 — Security concepts and relationships

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

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

These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realized and the impact on the assets when that threat is realized. Subsequently controls are imposed to reduce the risks to assets. These controls can consist of IT-related controls (e.g. firewalls and smart cards) and non-IT controls (e.g. 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: if 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 do not always wish to rely solely on the assertions of the developers of the security controls. These consumers can therefore choose to increase their confidence in the sufficiency and correctness of some or all of their security controls by ordering an evaluation of these security controls.

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

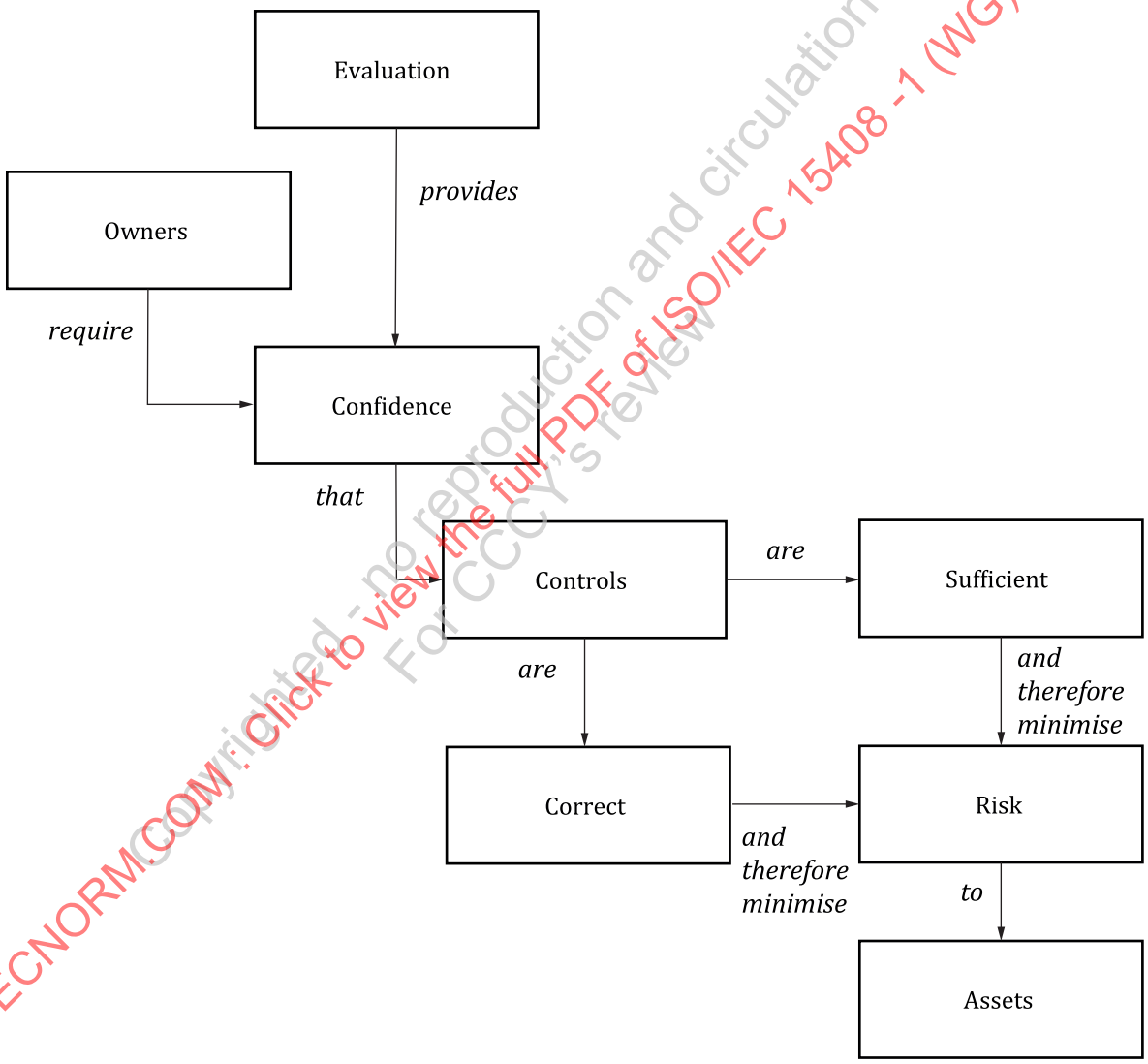

Figure 2 — Evaluation concepts and relationships

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

6.3 Core constructs of the paradigm of the ISO/IEC 15408 series

6.3.1 General

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

To allow consumer groups and technical communities to express their security needs, and to facilitate authoring appropriate documents that express these needs, five constructs are provided in the paradigm: package, PP, PP-Module, PP-Configuration and ST.

As an evaluation can need to meet varying assurance needs of consumers (risk owners), the ISO/IEC 15408 series provides different tools including well-formed security assurance components (ISO/IEC 15408-3) as well as a mechanism to define extended assurance components (ISO/IEC 15408-1).

Users of ISO/IEC 15408 series may also choose from pre-defined packages including those for EALs (based on ISO/IEC 15408-5), or from a framework for defining evaluation methods and activities (ISO/IEC 15408-4), and the associated evaluation methodology (based on ISO/IEC 18045).

6.3.2 Conformance types

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

PPs, PP-Modules and PP-Configurations shall specify a conformance type.

STs claim conformance to PPs and PP-Configurations according to their conformance types. PPs can also claim conformance to other PPs according to their conformance type.

Conformance types, conformance claims, and relationships of conformance types of PPs, PP-Modules and PP-Configurations are described in Annex E and shall be used in conjunction with the clauses of this document.

6.3.3 Communicating security requirements

6.3.3.1 Packages

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

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

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

Core requirements for packages can be found in Clause 9. Annex A provides additional information and requirements about packages that shall be used in conjunction with the clauses of this document.

ISO/IEC 15408-3 provides evaluation criteria, and specific requirements for STs, PPs and PP-Modules undergoing evaluation that may use packages and ISO/IEC 15408-5 provides some pre-defined assurance packages that may be used by PP, PP-Module, PP-Configuration and ST authors.

6.3.3.2 Protection Profiles (PPs)

PPs describe a TOE type and the security assurance requirements (SARs) and 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 can be found in Clause 10 and further information is found in Annex B that shall be used in conjunction with the clauses of this document.

ISO/IEC 15408-3 provides evaluation criteria for PPs.

6.3.3.3 PP-Modules and PP-Configurations

PP-Configurations build upon the concepts of PP and PP-Module.

A PP-Module may be used to refine the generic TOE type of a base PP, or to add security requirements for particular technologies which may be optionally associated with the TOE type defined in the base PPs. PP-Modules may also be based on other PP-Modules. Further, PP-Configurations consist of a TOE type and set of requirements specified in several PPs and possibly PP-Modules (these are the PP-Configuration components).

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

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

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

a) operating system with Bluetooth,

b) operating system with Wireless client,

c) operating system with Bluetooth and Wireless client,

d) mobile device with Bluetooth,

e) mobile device with Wireless client,

f) mobile device with Bluetooth and Wireless client.

6.3.3.4 Security Targets (STs)

6.3.3.4.1 General

The clause presents a simplified view of the ST construct. A more detailed and complete description of the ST concept and the content requirements can be found in 11.3.3 and Annex D which shall be used in conjunction with the clauses of this document.

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

6.3.3.4.2 Purpose of a ST

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

The two groups of security controls are:

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

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

The reasons for this division are:

— the ISO/IEC 15408 series is suitable for assessing the correctness of IT development and production environments and product life cycle management. Security controls required from the operational environment are out of the scope of the evaluation according to the ISO/IEC 15408 series.

— assessing the correctness of security controls costs time and money, possibly making it infeasible to assess the correctness of all security controls.

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

The ST further details the security objectives for the TOE by means of specifying SFRs. These SFRs shall be formulated in a standardized language, described in ISO/IEC 15408-2, to ensure precision and facilitate comparability.

In summary, the ST demonstrates that:

— the SFRs meet the security objectives for the TOE;

— the security objectives for the TOE and the security objectives for the operational environment address the SPD and, in particular, counter the threats;

— and therefore, the SFRs and the security objectives for the operational environment address the SPD and, in particular, 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 that meets the security objectives for the operational environment, will counter the threats. In 6.3.3.4.3 and 6.3.3.4.4 correctness of the TOE and correctness of the operational environment are discussed separately.

In some cases, defining a ST that omits security objectives for the TOE and directly maps the SFRs to the SPD is appropriate. This is a “Direct Rationale” ST, and is explained in detail in 11.3.3 and Annex D.

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

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

6.3.3.4.3 Correctness of the TOE

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

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

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

— testing the TOE;

— examining various design representations of the TOE;

— examining the physical security of the development environment of the TOE.

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

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

6.3.3.4.4 Correctness of the operational environment

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

However, in the ISO/IEC 15408 series, no assurance is obtained regarding the correctness of the operational environment, i.e. 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 this operational environment.

EXAMPLE 1 If, for an Operating System TOE, the security objectives for the operational environment state "The operational environment ensure that entities from an untrusted network can only access the TOE using the FTP protocol", the consumer can select an evaluated firewall and configure it to only allow FTP access to the TOE.

EXAMPLE 2 If the security objectives for the operational environment state: "The operational environment shall ensure that all administrative personnel do not behave maliciously", the consumer can adapt their contracts with administrative personnel to include punitive sanctions for malicious behaviour, but this determination is not part of an evaluation using the ISO/IEC 15408 series as a basis.

NOTE The Internet is an example of an untrusted network.

6.3.4 Meeting the needs of consumers (risk owners)

6.3.4.1 General

Consumers (risk owners) can have different approaches for obtaining the assurance that the products they use to address the SPD. 6.3.4.2 and 6.3.4.3 introduce these approaches. Moreover, ISO/IEC 15408-4 provides methods to define specific evaluation activities for the assurance requirements.

6.3.4.2 Single assurance evaluation

Single assurance evaluation is the type of evaluation that has been specified in previous revisions of the ISO/IEC 15408 series. In single assurance evaluation a single set of SARs are applied to the entire TOE.

The single assurance evaluation paradigm:

— requires that the entire TOE has been subject to the same SARs;

— is used when a single set of SARs are commensurate with the security needs for the TOE.

A single assurance evaluation is based on an ST that may claim conformance with PP(s), or a PP-Configuration but is reliant on all claimed PPs or PP-Configuration components specifying identical sets or supersets of security assurance components. An evaluation based on an ST that does not make any conformance claim with PPs or a PP-Configuration is by its nature a single-assurance evaluation.

6.3.4.3 Multi-assurance evaluation

The multi-assurance evaluation paradigm consists in applying different assurance requirements to different parts of the TSF (sub-TSFs), while enforcing a global set of SARs for the entire TOE.

The multi-assurance evaluation paradigm:

— addresses heterogeneous IT products where different security needs require a different assurance within a single evaluation;

— ensures that the multiple assurance requirements are sound with regard to the security needs for the IT product.

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

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

— a product where some security functionality requires a higher assurance than the rest, e.g. a key storage and processing unit, a secure boot module;

— a product where some parts of the security functionality do not require the same high evaluation assurance as other more exposed parts, for instance an internet gateway with support for personal area network protocols;

— a family of products where some security functionality is shared across all the products with the same assurance, and some security functionality is implemented in different ways for different use cases, for instance in a tamper-resistant module or in a software module or through COTS, requiring a different assurance;

  An example is a family of biometric authentication devices, with either match-on-device or match-on-SE, or both. This can give rise to a PP for the authentication device excluding the matching function, and two PP-Modules for the different types of matching functions, each with a dedicated set of assurance requirements. Three PP-Configurations can be defined for the device: PP with each of the PP-Modules, PP with both PP-Modules. A similar situation arises, for instance, for a family of mobile applications which uses either software crypto library secured by with-box techniques or a hardware-based crypto library, or for a family of payment terminals with either IC and/or magstripe readers.

Multi-assurance is also relevant for products claiming conformance to different PPs with different assurance packages: by defining and evaluating a PP-Configuration, the multi-assurance paradigm allows better control over possible inconsistencies between these PPs. The evaluation of electronic passports implementing both Basic Access Control and Extended Access Control constitutes a typical example, as these access control mechanisms are subject to different security problems and assurance requirements.

7 Specifying security requirements

7.1 Security problem definition (SPD)

7.1.1 General

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

SPD elements can be associated with configurations or requirements that are optional for the given TOE type, for example, in a case where the TOE is distributed, or where optional functional requirements (as outlined in 7.3.2.6) are specified. This is allowed as long as the optional nature of the SPD elements (and any associated objectives and functional requirements) are identified as specified in this document.

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

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

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

7.1.2 Threats

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

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

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

Threat agents may be described as individual entities, but in some cases, it is preferable to describe them as, e.g. types of entities, groups of entities.

EXAMPLE 1

Examples of threat agents are:

— hackers;

— users;

— computer processes;

— accidents.

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

EXAMPLE 2

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.

7.1.3 Organizational security policies (OSPs)

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

OSPs are security rules, procedures, or guidelines imposed 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 shall conform to the national standard for password generation and encryption";

— "Only users with system administrator privilege and clearance of Department Secret shall be allowed to manage the Department Fileserver".

7.1.4 Assumptions

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

EXAMPLE Examples of assumptions are:

— assumptions on the non-TOE part of the product;

  — it is assumed that the TOE will be integrated into a device that provides a hardware-based root of trust.

— assumptions on physical aspects of the operational environment;

  — it is assumed that the TOE will be placed in a room that is designed to minimize electromagnetic emanations;

  — it is assumed that the administrator consoles of the TOE will be placed in a restricted access area.

— assumptions on personnel aspects of the operational environment;

  — it is assumed that users of the TOE will be trained sufficiently in order to operate the TOE;

  — it is assumed that users of the TOE are approved for information that is classified as National Secret;

  — it is assumed that users of the TOE will not write down their passwords.

— assumptions on connectivity aspects of the operational environment;

  — it is assumed that a PC workstation with at least 10GB of disk space is available to run the TOE on;

  — it is assumed that the TOE is the only non-OS application running on this workstation;

  — it is assumed that the TOE will not be connected to an untrusted network.

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

7.2 Security objectives

7.2.1 General

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

a) provide a high-level, natural language solution of the problem. The security objectives consist of a set of statements without overly much detail that together form a high-level solution to the security problem. The level of abstraction of the security objectives aims at being clear and understandable to knowledgeable potential consumers of the TOE. The security objectives are in natural language;

b) divide this solution into two part-wise solutions, that reflect the roles of the TOE and its operational environment to address each part of the problem. In a ST the high-level security solution, as described by the security objectives, is divided into two part-wise solutions. These part-wise solutions are called the security objectives for the TOE and the security objectives for the operational environment;

c) demonstrate that these part-wise solutions form a complete solution to the problem.

7.2.2 Security objectives for the TOE

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

EXAMPLE Examples of security objectives for the TOE are:

— "The TOE shall keep confidential the content of all files transmitted between it and a Server";

— "The TOE shall identify and authenticate all users before allowing them access to the Transmission Service provided by the TOE";

— "The TOE shall restrict user access to data according to the Data Access policy described in Annex 3 of the PP".

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

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

7.2.3 Security objectives for the operational environment

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

EXAMPLE

Examples of security objectives for the operational environment are:

— "The operational environment shall provide a workstation with the OS Linux version 3.01b to execute the TOE on";

— "The operational environment shall ensure that all human TOE users receive appropriate training before allowing them to work with the TOE";

— "The operational environment of the TOE shall restrict physical access to the TOE to administrative personnel and maintenance personnel accompanied by administrative personnel";

— "The operational environment shall ensure the confidentiality of the audit logs received from the TOE on the Audit Server".

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

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

7.2.4 Relation between security objectives and the SPD

STs, PPs, PP-Modules and packages also contain a security objectives rationale containing two sections:

a) a tracing that shows which security objectives address which SPD-elements;

b) a set of justifications that shows that all SPD-elements are effectively addressed by the security objectives.

NOTE In Direct Rationale PPs a rationale for security objectives in the TOE is not included. See D.4.

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

7.2.5 Tracing between security objectives and the SPD

The tracing shows how the security objectives trace back to the SPD-elements and that:

a) *there are no spurious objectives;*

Each security objective traces to at least one SPD-element.

b) *the security problem definition is completely covered;*

Each SPD-element has at least one security objective tracing to it;

c) *the tracing is correct*.

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

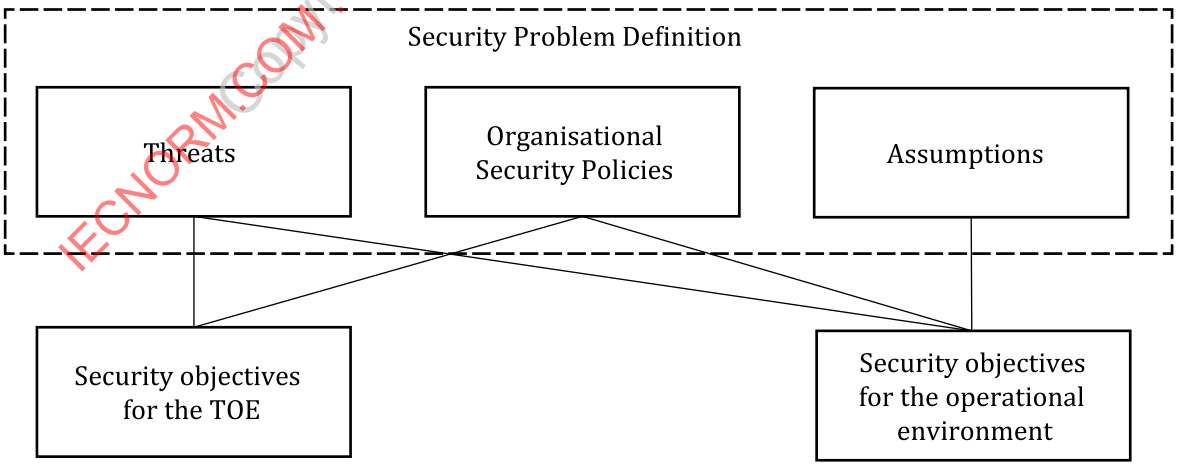

Figure 3 — Tracings between security objectives and the SPD

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

7.2.6 Providing a justification for the tracing

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

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

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

7.2.7 On countering threats

Countering a threat does not necessarily mean removing that threat, it can also mean sufficiently diminishing that threat or sufficiently mitigating the associated risk.

EXAMPLE Examples of removing a threat are:

— removing the ability to execute the adverse action from the threat agent;

— moving, changing, or protecting the asset in such a way that the adverse action is no longer applicable to it;

— removing the threat agent, e.g. removing machines from a network that frequently crash that network.

Examples of diminishing a threat are:

— restricting the ability of a threat agent to perform adverse actions;

— restricting the opportunity to execute an adverse action of a threat agent;

— reducing the likelihood of an executed adverse action being successful;

— reducing the motivation to execute an adverse action of a threat agent by deterrence;

— requiring greater expertise or greater resources from the threat agent.

Examples of mitigating the effects of a threat are:

— making frequent back-ups of the asset;

— obtaining spare copies of an asset;

— insuring an asset;

— ensuring that successful adverse actions are always timely detected, so that appropriate action can be taken.

7.2.8 Security objectives: conclusion

Based on the security objectives and the security objectives rationale, the following conclusion is drawn: If all security objectives are achieved then the security problem as defined in SPD is solved. All threats are countered, all OSPs are enforced, and all assumptions are upheld.

NOTE The ASE_SPD family in ISO/IEC 15408-3 supports this determination.

7.3 Security requirements

7.3.1 General

As mentioned in 6.3.3.4 and 6.3.3, packages, PPs, PP-Modules, PP-Configurations and STs specify the detailed security requirements applicable to a TOE that have been derived from the stated SPD. SFRs and SARs shall be drawn from security components defined in ISO/IEC 15408-2 and ISO/IEC 15408-3

respectively, which are a template for security requirements written in a standardized language. The process of deriving a security requirement from a security component involves digesting the components and is known as “completion”.

NOTE 1 In Clause 7, the term “author” includes authors of STs, PPs, PP-Modules, PP-Configurations and packages.

Security requirements are specified as a result of the description of the in a ST and possibly PP, PP-Module, and packages. Security requirements are specified by a choosing the components given in ISO/IEC 15408-2, ISO/IEC 15408-3 or that have been defined as extended components in accordance with 8.4. The tailoring process uses the operations in 8.2.

NOTE 2 Since a ST specifies the security requirements for a specific TOE it presents only fully completed components. PPs, PP-Modules and packages often present uncompleted security components allowing authors basing documents upon them appropriate flexibility.

The security requirements consist of two groups of requirements:

a) ***the security functional requirements*** (SFRs): a description of how the TOE addresses the SPD in a standardized language;

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

NOTE 3 SARs concern the adherence of the TOE to the ST. SARs play no role in the coverage of the SPD, which is covered by security objectives and SFRs.

These two groups are discussed in 7.3.2 and 7.3.3.

7.3.2 Security Functional Requirements (SFRs)

7.3.2.1 General

The SFRs contribute to fulfil the TOE’s SPD and address the security objectives defined for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives for the TOE shall be completely addressed). The ISO/IEC 15408 series requires this translation into a standardized language for the following reasons:

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

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

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

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

NOTE 1 See the Bibliography for items relevant to the security assessment of operational systems.

NOTE 2 It can be the case that parts of the operational environment are evaluated in another evaluation, but this is not within the scope of the ISO/IEC 15408 series.

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

7.3.2.2 How this translation is supported

The ISO/IEC 15408 series supports this translation in three ways:

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

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

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

7.3.2.3 Relation between SFRs and security objectives

Packages, PPs, PP-Modules and STs contain a SFRs rationale, consisting of two sections:

a) a tracing that shows which SFRs address which security objectives for the TOE;

b) a set of justifications that shows that all security objectives for the TOE are effectively addressed by the SFRs.

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

7.3.2.4 Tracing between SFRs and the security objectives for the TOE

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

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

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

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

7.3.2.5 Providing a justification for the tracing

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

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

7.3.2.6 Special types of SFR

SFRs can be designated in packages, PPs and PP-Modules as optional requirements or selection-based requirements.

A. Optional requirements

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

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

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

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

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

B. Selection-based requirements

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

7.3.3 Security assurance requirements (SARs)

7.3.3.1 General

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

— to provide a precise description of how the TOE is to be evaluated;

— to allow comparison between two STs. The standardized language enforces using the same terminology and concepts.

This standardized language is rendered by components defined in ISO/IEC 15408-3, and permitted operations are defined in Clause 8. The use of this language is mandatory, though some exceptions exist. The ISO/IEC 15408 series enhances this language in two ways:

a) By providing operations: mechanisms that allow the package/PP/PP-Module/PP-Configuration/ST author to modify the SARs. The ISO/IEC 15408 series has four operations: assignment, selection, iteration, and refinement. These are described further in 8.2;

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

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

7.3.3.2 SARs and the security requirement rationale

Assurance packages, PPs, PP-Modules, PP-Configurations, and STs also contain a security requirements rationale that explains why the chosen set(s) of SARs are deemed appropriate.

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

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

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

7.3.4 Security requirements: conclusion

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

— security objectives for the TOE;

— security objectives for the operational environment.

Additionally, the security objectives rationale is provided to justify that the security problem is solved if all security objectives are met.

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

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

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

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

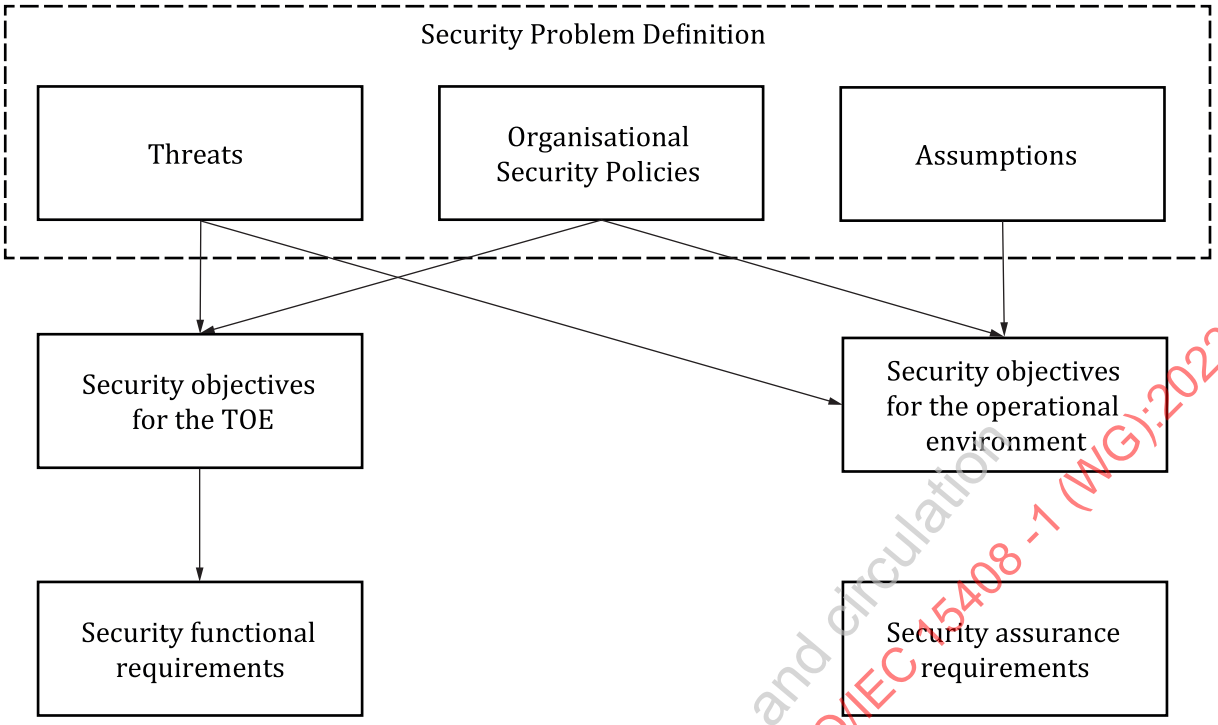

Figure 4 — Relations between the SPD, the security objectives, and the security requirements

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

8 Security components

8.1 Hierarchical structure of security components

8.1.1 General

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

— classes, consisting of;

— families, consisting of;

— components, consisting of;

— elements, which cannot be decomposed.

8.1.2 Class

The requirements for functional classes are given in ISO/IEC 15408-2: 2022, 6.1.2. The requirements for assurance classes are given in ISO/IEC 15408-3: 2022, 6.2.

A class consists of a set of families.

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

8.1.3 Family

The requirements for functional families are provided in ISO/IEC 15408-2: 2022, 6.1.3. The requirements for assurance families are given in ISO/IEC 15408-3: 2022, 6.3.

A family consists of a set of components.

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

8.1.4 Component

The requirements for functional component structure are provided in ISO/IEC 15408-2:2022, 6.1.4. The requirements for assurance components are given in ISO/IEC 15408-3:2022, 6.4.

A component consists of a set of elements.

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

8.1.5 Element

The requirements for functional elements are provided in ISO/IEC 15408-2:2022, 6.1.4. The requirements for assurance elements are given in ISO/IEC 15408-3:2022, 6.5.

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

8.2 Operations

8.2.1 General

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

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

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

a) iteration: allows a component to be used more than once with varying operations;

b) assignment: allows the specification of parameters;

c) selection: allows the specification of one or more items from a list; and

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

— "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.

— 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.

8.2.2 Iteration

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

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

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

— cryptographic operation (RSA signatures) (FCS_COP.1(RSA signatures));

— cryptographic operation (AES data encryption/decryption) (FCS_COP.1(AES data encryption/decryption)).

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

8.2.3 Assignment

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

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

a) leave the assignment uncompleted;

  EXAMPLE 1 The author can include FIA_AFL.1.2 in the PP, PP-Module or package.

  "When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF **shall [assignment: list of actions]**."

  In this case, the ST author can complete FIA_AFL.1.2 thus:

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

b) complete the assignment;

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

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

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

EXAMPLE 3 The author can include FIA_AFL.1.1 in the PP, PP-Module or package.

"The TSF shall detect when [assignment: positive integer] unsuccessful authentication attempts occur …"

In this case, the ST author can complete FIA_AFL.1.1 thus:

"The TSF shall detect when **3** unsuccessful authentication attempts occur …"

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

EXAMPLE 4 The author can include FIA_AFL.1.2 in the PP, PP-Module or package.

"When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [selection: prevent that user from binding to any subject in the future, notify the administrator]."

In this case, the ST author can complete FIA_AFL.1.2 thus:

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

An ST author shall complete all the assignments.

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

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

EXAMPLE 5 Where the set is "subjects":

— all subjects;

— all subjects of type X;

— all subjects except subject a.

8.2.4 Selection

8.2.4.1 General

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

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

a) leave the selection uncompleted;

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

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

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

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

EXAMPLE 1 An example of an element with a selection is:

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

8.2.4.2 Selection-based security functional components and SFRs

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

— a selection choice identified in the PP, PP-Module or package indicates that it has an associated selection-based SFR;

— that selection is made by the author.

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

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

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

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

The following is another example of such an SFR:

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

FTP_ITC.1.1 The TSF shall be capable of using [selection: IPsec, SSH, TLS, HTTPS] to provide a trusted communication channel between...
Application Note:
In the selection for FTP_ITC.1.1, the ST author selects the mechanism or mechanisms supported by the TOE, and then ensures that the selection-based requirements in Appendix B of this PP that correspond to the selected mechanism or mechanisms are included in the ST.
And in Appendix B of the example PP:
The following SFRs are included in the ST if the ST author selects "IPsec" in FTP_ITC.1.1:
FCS_IPSEC.1 [...]

8.2.5 Refinement

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

NOTE 1 A series of refined iteration operations can be used to cover all of the subjects, objects, operations, security attributes and/or external entities, but where each individual refinement does not.

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

EXAMPLE 2 An example of a valid refinement is:

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

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

EXAMPLE 3 An example of a such an exception is:

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

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

EXAMPLE 4 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 may be made in a requirement, i.e. rephrasing a sentence due to adherence to proper English grammar, or to make it more understandable to the reader. This change is not allowed to modify the meaning of the requirement in any way.

EXAMPLE 5 An example of an editorial refinement is:

The SFR FPT_FLS.1, "The TSF shall continue to preserve a secure state when the following failures occur: **breakdown of one CPU**" that could be refined to FPT_FLS.1, "The TSF shall continue to preserve a secure state when the following failure occurs: **breakdown of one CPU**" or even FPT_FLS.1, "The TSF shall continue to preserve a secure state when **one CPU breaks down**".

8.3 Dependencies between components

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

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

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

Component dependency descriptions are determined by consulting the component definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, or the extended components definition. In order to ensure completeness of the TOE security requirements, dependencies should be satisfied when requirements based on components with dependencies are incorporated into PPs, PP-Modules, packages or STs. Dependencies should also be considered when constructing packages, i.e. if component A has a dependency on component B, this means that whenever a PP, PP-Module, package or ST contains a security requirement based on component A, the PP, PP-Module, package or ST shall also contain one of:

a) a security requirement based on component B; or

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

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

In cases a) and b), when a security requirement is included because of a dependency, it can 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 (e.g. extended SFRs, combinations of SFRs).

8.4 Extended components

8.4.1 General

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

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

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

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

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

After the new components have been defined correctly, the author 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 the ISO/IEC 15408 series and SFRs and SARs based on extended components.

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

8.4.2 Defining extended components

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

The author also shall make sure that all of the applicable dependencies of an extended component are included in the definition of that extended component.

EXAMPLE

Examples of possible dependencies are:

a) an extended component that refers to auditing, can include dependencies to components of the FAU: Security audit class;

b) an extended component that modifies or accesses data, can include dependencies to components of the Access control policy (FDP_ACC) family;

c) an extended component that uses a particular design description can include a dependency to the appropriate ADV: Development family.

In the case of an extended functional component, the author also shall 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 may also provide a suitable evaluation methodology for the component, similar to the method provided in ISO/IEC 18045.

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

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

9 Packages

9.1 General

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

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

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

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

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

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

Functional packages cannot be claimed directly by a PP-Configuration; they shall be part of a PP-Configuration component.

Further information on packages is given in Annex A.

9.2 Package types

9.2.1 General

A package shall be either:

— a functional package, containing functional components or requirements, but no assurance components or requirements; or

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

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

All packages shall include:

a) the package identification giving a unique name, short name, version, date, sponsor, and the relevant parts of the ISO/IEC 15408 series;

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;

e) identification of evaluation methods(s) and/or activities, if such evaluation methods/activities derived from ISO/IEC 18045 have been specified;

f) one or more security components or requirements;

g) if extended components have been specified, then the package includes an extended components definition;

h) a component rationale that provides the rationale for selecting the functional or assurance components/requirements included in the package.

9.2.2 Assurance packages

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

An assurance package shall not include an SPD or security objectives nor any security functional components or requirements.

Assurance packages may be used within PPs, PP-Modules, PP-Configurations and STs. A set of pre-defined hierarchic assurance packages is given in ISO/IEC 15408-5.

EXAMPLE The EALs that are defined in ISO/IEC 15408-5 are comprised of SARs drawn from ISO/IEC 15408-3. EALs are pre-defined security assurance packages.

9.2.3 Functional packages

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

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

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

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

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

— the ST claims conformance to the PP (which includes functional package A);

— the ST claims conformance to the PP and functional package B;

— the ST claims conformance to the PP and functional packages B and C;

— the ST claims conformance to the PP and functional package D;

— the ST claims conformance to the PP and functional packages B, C, and D.

The following would not be allowed:

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

9.3 Package dependencies

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

9.4 Evaluation method(s) and activities

Packages may include evaluation methods/activities that have been derived from ISO/IEC 18045. If evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 are to be used to evaluate the package, then these shall be identified in the relevant security requirement section by including a statement in the following form:

"This package requires the use of evaluation methods/ evaluation activities defined in <reference(s)>."

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 document containing the package, or to one or more separate documents.

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

10 Protection Profiles (PPs)

10.1 General

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

— as a ST template for any TOEs that meet the PP's TOE type;

— as a template for other PPs in order to further refine the TOE type;

— as a basis for a PP-Module, in which context it is known as a base PP.

A detailed description of PPs is given in Annex B.

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

10.2 PP introduction

The introduction to the PP shall include a reference identifier for the PP.

The introduction to the PP shall include an overview of the PP, including a description of the TOE type.

The reference identifier for a PP shall be unique within a catalogue.

EXAMPLE A TOE type can be "Firewall";

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

A specific TOE related to that TOE type can 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.

10.3 Conformance claims and conformance statements

In this subclause the use of italic text indicates literal text that shall appear in the text of the PP.

The conformance claims of PPs:

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

b) shall describe the conformance to ISO/IEC 15408-2 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 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 also include a conformance claim with respect to other PPs:

— "*PP Conformant*";

A PP is "PP Conformant" when it meets other specific PP(s).

e) 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 Conformant*";

A PP is conformant to a package if:

— for functional packages, all constituent parts (SPD, security objectives, and SFRs) of the functional package are present in the corresponding parts of the PP without modification;

— for assurance packages, the SARs of that PP are identical to the SARs in the assurance package;

— a PP that restricts some selections of SFRs in a package may still claim it is package conformant.

— "*Package Augmented*";

A PP claims an augmentation of a package if:

— for functional packages, all constituent parts (SPD, security objectives, and SFRs) of that PP contain all constituent parts given in the functional package but shall have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package;

— for assurance packages, the SARs of that PP contain all SARs in the assurance package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package.

— "*Package Tailored*".

A PP claims tailoring of a package if:

— for functional packages, all constituent parts (SPD, Security Objectives, and SFRs) of that PP contain all constituent parts given in the functional package, but shall have additional selection items for an SFR with existing selections in the package, and optionally, at least one additional SFR and/or one SFR that is hierarchically higher than an SFR in the functional package;

— assurance packages and STs shall not claim (or perform) tailoring.

More than one package may be claimed in a PP.

Where PPs claim strict or demonstrable conformance to PP(s) they shall not also claim conformance to the packages claimed in the PPs they claim conformance to, unless the PP augments the package. The PP claims <package>-augmented only in the case where the PP augments the packages beyond that claimed by the PP to which it claims conformance to.

NOTE 1 PPs cannot claim exact conformance to PP(s).

f) PPs shall contain a conformance claim rationale;

The conformance claim rationale describes the reasons and the logical basis for the authors choice of conformance claims and statement.

g) PPs shall provide a conformance statement.

The conformance statement shall describe the manner in which other PPs or STs shall conform to this PP: The conformance statement shall be one of:

— "*Exact conformance*";

If the PP states that exact conformance is required, a ST shall conform to the PP in an exact manner, i.e. a conformant ST shall contain SPD and objectives identical to the PP's, and the same set of PP's SFRs with all the assignments and selections resolved;

— "*Strict conformance*";

If the PP states that strict conformance is required, a PP/ST shall conform to the PP in a strict manner, i.e. a conformant PP/ST shall contain a superset of PP's SPD, objectives and SFRs, where the new assumptions (if any) do not weaken the PP's SPD, and all the PP's SFRs have their assignments and selections unchanged or where appropriate, resolved;

Strict conformance allows the conformant PP/ST not to add any element to the PP's SPD, set of objectives and SFRs, i.e. the superset defined in the PP/ST may be identical to the PP's, with all the SFRs resolved;

— "*Demonstrable conformance*".

If the PP states that demonstrable conformance is required, the PP/ST shall conform to the PP in a strict or demonstrable manner, i.e. a conformant PP/ST shall contain a SPD, set of objectives and set of SFRs that are equivalent to a superset of PP's SPD, objectives and SFRs, where the new assumptions (if any) do not weaken the PP's SPD, and where the set of the conformant PP/ST SFRs imply the PP's SFRs.

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

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

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

The conformance statement may also include a reference to any evaluation methods/ activities that have been derived from ISO/IEC 18045. If evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 are to be used to evaluate the PP then these shall be identified with the relevant security requirement section by including a statement in the following form:

"*This PP requires the use of evaluation methods/ evaluation activities defined in <reference(s)>.*"

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 document containing the PP or to one or more separate documents.

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

10.4 Security assurance requirements (SARs)

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

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

NOTE Pre-defined EAL's are given in ISO/IEC 15408-5.

10.5 Additional requirements common to strict and demonstrable conformance

10.5.1 Conformance claims and conformance statements

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

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

— all TOEs that meet the PP/ST also meet the PP;

— 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 SPD, the security objectives for the TOE, the security objectives for the environment, and the security functional and SARs.

10.5.2 Security problem definition (SPD)

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

— all TOEs that meet the SPD in the PP/ST also meet the SPD in the PP;

— all operational environments that meet the SPD in the PP also meet the SPD in the PP/ST.

10.5.3 Security objectives

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

— TOEs that meet the security objectives for the TOE in the PP/ST also meet the security objectives for the TOE in the PP;

— operational environments that meet the security objectives for the operational environment in the PP also meet the security objectives for the operational environment in the PP/ST.

10.6 Additional requirements specific to strict conformance

10.6.1 Requirements for the security problem definition (SPD)

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

— an assumption (or a part of an assumption) specified in the PP may be omitted from the PP/ST if all security objectives for the operational environment defined in the PP addressing this assumption (or this part of an assumption) are replaced by security objectives for the TOE in the PP/ST;

— a new assumption may be added in the PP/ST to the set of assumptions defined in the PP, if this new assumption does not mitigate a threat (or part of a threat) meant to be addressed by security objectives for the TOE in the PP and if this assumption doesn't fulfil an OSP (or a part of an OSP) meant to be addressed by security objectives for the TOE in the PP.

10.6.2 Requirements for the security objectives

The PP/ST:

— shall contain all security objectives for the TOE of the PP but may specify additional security objectives for the TOE;

— shall contain all security objectives for the operational environment as defined in the PP with two exceptions as explained in the next two bullet points;

— may specify that certain security objectives for the operational environment in the PP are security objectives for the TOE in the PP/ST. This is called re-assigning a security objective. If a security objective is re-assigned to the security objectives for the TOE, the security objectives justification has to make clear which assumption/OSP or part of the assumption/OSP is no longer necessary;

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

10.6.3 Requirements for the security requirements

The PP/ST:

— shall contain all SFRs and SARs in the PP;

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

NOTE The rules of refinement apply.

10.7 Additional requirements specific to demonstrable conformance

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

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

10.8 Additional requirements specific to exact conformance

10.8.1 General

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

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

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

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

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

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

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

If a PP requires exact conformance, then only those SFRs and SARs specified by that PP are allowed in the conformant ST. These security requirements are related to the SPD and security objectives specified in the PP, which are also included in the conformant ST. SFRs in an exact conformance PP can be iterated and refined (as stated in ISO/IEC 18045 for ASE_CCL.1-12).

10.8.2 Conformance claims and statements

If a PP requires exact conformance in its conformance statement, then

a) the PP shall include an allowed-with statement that states which other PPs and PP-Modules are allowed to be included in a conformance claim along with the PP;

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

c) all of the additional PPs an ST is claiming conformance to shall identify the PP in their respective allowed-with statements;

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

A PP-Module does not have to identify its own base PPs/PP-Module(s) in its conformance statement, however, the PP-Module Base shall be identified in its PP-Module introduction.

10.9 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 are found in Annex A and Annex B.

This allows the following process:

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

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

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

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

10.10 Conformance statements and claims in the case of multiple PPs

10.10.1 General

The ISO/IEC 15408 series allows both STs and PPs to claim conformance to multiple PPs. The case for a ST claiming conformance to multiple PPs is covered in 11.3.3. 10.10 covers the case where a PP claims conformance to multiple PPs.

10.10.2 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 can be used to develop specific PPs for different use cases, e.g. tachograph card, payment card, electronic passport, etc. A developer can then construct a ST conformant to any of those PPs.

10.10.3 Where exact conformance is specified

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

NOTE In cases where such a combination of functionality is needed, this can be achieved by creating a PP-Configuration that consists of the PPs to which conformance is desired to be claimed.

11 Modular requirements construction

11.1 General

In order to allow a modular description of the TOE's security features, STs can claim conformance to a PP-Configuration instead of PPs. Such PP-Configurations are composed of a set of PPs and PP-Modules which contains the PP-Module Base(s).

PP-Configurations can be constructed to accommodate either single-assurance or multi-assurance evaluations. In a single-assurance evaluation, a single set of assurance requirements applies to all the components of the PP-Configuration. In a multi-assurance evaluation, there is a single global set of assurance requirements that applies to all the components of the PP-Configuration, but additionally each component (PP or PP-Module) has its own set of assurance requirements to which it is subject. The following subclauses present the content-related details for these two evaluation approaches; the actual evaluation particulars using these approaches is discussed in Clause 13.

11.2 PP-Modules

11.2.1 General

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

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

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

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

11.2.2 PP-Module Base

A given PP-Module specifies one or several PP-Module Base(s) consisting of a set of PPs and possibly other PP-Modules. Anytime the given PP-Module is used in a PP-Configuration, one of its PP-Module Base(s) is required. See Clause 10 and Annex B.

11.2.3 Requirements for PP-Modules

11.2.3.1 General

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

The reference identifier for a PP-Module shall be unique within a catalogue.

A PP-Module shall define one or several PP-Module Base(s) which may be required to be used with the PP-Module in a PP-Configuration.

A PP-Module shall specify the TOE types relative to each of its PP-Module Bases.

A PP-Module may introduce new SPD-elements and objectives and may also refine some of the SPD-elements or objectives of its PP-Module Bases.

A PP-Module shall define a non-empty set of SFRs that are refinement of the SFRs of the PP-Module Bases or new.

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

NOTE 1 The TOE type defined in the PP-Module can supplement the TOE type defined in each of its PP-Module Bases.

A PP-Module shall provide a consistency rationale ensuring that the union of the elements defined in the PP-Module and in each of its PP-Module Bases do not lead to contradiction.

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

The evaluation of a PP-Module alone is meaningless. A PP-Module shall be evaluated as part of a PP-Configuration, at least with one PP-Module Base.

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

11.2.3.2 Direct Rationale

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

11.2.3.3 Conformance claims and conformance statements

In this subclause the use of italic text indicates literal text that shall appear in the text of the PP-Module.

The conformance claims of a PP-Module:

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

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

— "*ISO/IEC 15408-2 conformant*";

NOTE 1 A PP-Module is ISO/IEC 15408-2 conformant if all SFRs in that PP-Module are based only upon functional components in ISO/IEC 15408-2.

or

— "*ISO/IEC 15408-2 extended*".

NOTE 2 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;

NOTE 3 A PP-Module does not claim conformance to a functional package that is already claimed by one of the PPs or PP-Modules in the PP-Module Bases. The exception to this rule is when the PP-Module augments or tailors the functional package as it is instantiated in its PP-Module Base; in this case the PP-Module would claim the functional package as "Package Augmented" or "Package Tailored" (as appropriate) in its package conformance claim statement.

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

— *"Package Conformant";*

A 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 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 an SFR in the functional package;

— *"Package Tailored".*

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

d) shall include a conformance claim in respect to ISO/IEC 15408-3. The conformance claim to ISO/IEC 15408-3 shall be either:

— "*ISO/IEC 15408-3 conformant*";

A PP-Module is ISO/IEC 15408-3 conformant if all SARs in that PP-Module are based only upon assurance components in ISO/IEC 15408-3.

or

— *"ISO/IEC 15408-3 extended"*.

A PP-Module is ISO/IEC 15408-3 extended if at least one SAR in that PP-Module is not based upon assurance components in ISO/IEC 15408-3;

— may include a conformance claim made with respect to assurance packages. More than one assurance package may be claimed by a PP-Module. Overlap between the claimed assurance packages is allowed; by construction the hierarchically higher SAR takes precedence over the other and is applied in the PP-Configuration.

In the strict and demonstrable cases, a PP-Module may claim conformance to more than one assurance package, for instance an ALC-based package and an ADV-based package.

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

— "*Package Conformant*";

A PP-Module is conformant to an assurance package if all constituent parts of the assurance package are present in the PP-Module without modification;

— "*Package Augmented*".

A PP-Module claims an augmentation of an assurance package if all constituent parts of the assurance package contained in the PP-Module are identical to those given in the assurance package, but shall also contain at least one SAR that is either additional or hierarchically higher than those SARs contained in the package;

The conformance statement of a PP-Module:

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

— "*Exact conformance*";

The PP-Module shall require exact conformance if and only if all its PP-Module Base(s) are of exact conformance. A ST shall conform to the PP-Module, as part of a PP-Configuration, in an exact manner. Additionally:

— the allowed-with Statement shall state which other PPs and PP-Modules (which are not in the set of PP-Module Bases) are allowed to be used in a PP-Configuration with that PP-Module;

— each PP and PP-Module in the PP-Module Base for the PP-Module being defined, and all of the additional PPs and PP-Modules (that are not in the PP-Module Base) that are allowed to

be specified with the PP-Module in a PP-Configuration, shall identify the PP-Module being defined in their respective allowed-with statements.

— all of the referenced PP-Module Bases shall also require exact conformance.

— "*Strict conformance*";

If the PP-Module states that strict conformance is required, a ST shall conform to the PP-Module, as part of a PP-Configuration, in a strict manner;

— "*Demonstrable conformance".*

If the PP-Module states that demonstrable conformance is required, the ST shall conform to the PP-Module, as part of a PP-Configuration, in a strict or demonstrable manner. A ST is only allowed to conform to a PP-Module, as part of a PP-Configuration, in a demonstrable manner if the PP-Module explicitly allows this;

NOTE 1 A PP-Module can require strict or demonstrable conformance although its PP-Module Base(s) do not all require strict or demonstrable conformance. The combination of demonstrable and strict conformance will be validated in the PP-Configuration evaluation.

NOTE 2 The explicit declaration of strict or demonstrable conformance allows sponsors to make the most appropriate statement in each PP-Module, independently of its PP-Module Base(s).

NOTE 3 PP-Module Base(s) do not need to be specified in the PP-Modules' conformance statement.

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

If evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 are to be used to evaluate the PP-Module, then these shall be identified with the relevant security requirement section by including a statement in the following form:

"This PP-Module requires the use of evaluation methods/ evaluation activities defined in <reference(s)>."

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 document containing the PP-Module, or to one or more separate documents.

For more information and requirements on the conformance types, claims and statements for PP-Modules, Annex C shall be used in conjunction with the clauses of this document.

11.2.3.4 Assurance requirements

A PP-Module shall define the set of SARs that applies to the TSF defined in the PP-Module, which can be either inherited from the PP-Module Base(s) or explicitly declared by the PP-Module author.

A PP-Module may define a distinctive name for its set of SARs. However, if the PP-Module declares an (augmented) pre-defined EAL (EAL1 to EAL7) or an (augmented) assurance package defined in an applicable external reference or inherits the set of SARs from its PP-Module Base(s), then the same name shall be used.

A PP-Module shall provide an assurance rationale that justifies the internal consistency of its set of SARs, i.e.:

— the consistency of the set of SARs with regard to the threat model as defined in the SPD of the PP-Module;

— if the PP-Module does not inherit its set of SARs from its PP-Module Base(s), the consistency of the set of SARs with all the sets of SARs defined in the PP-Module Base(s) of the PP-Module.

NOTE 1 Consistency refers to the absence of contradiction. An example of an inconsistency between SARs and SPD would be to consider highly skilled threat agents together with a low AVA_VAN level that cannot consider these threat agents by definition.

NOTE 2 The PP-Module assurance rationale ensures that the set of SARs defined in the PP-Module does not undermine the security that is expected for the assets that are shared between the PP-Module and its PP-Module Base(s) (if shared assets exist).

NOTE 3 The assurance rationale at PP-Module level contributes but is not sufficient to ensure the consistency of the assurance requirements at PP-Configuration level. See 11.3.2.4.

NOTE 4 The assurance rationale can rely on the relationship of the set of SARs in the PP-Module with the pre-defined EALs to demonstrate the internal consistency.

11.3 PP-Configurations

11.3.1 General

A PP-Configuration is a specification for the construction of a set of requirements to which conformance can be claimed.

A PP-Configuration is intended to describe a general TOE type. A PP-Configuration:

— may be used as a ST template for any TOEs that meet the PP-Configuration's TOE type;

— cannot be used as a template for other PP-Configurations, PPs or PP-Modules.

A PP-Configuration contains a set of PPs and PP-Modules (the PP-Configuration components) and cannot claim conformance to any functional packages, except indirectly through its PPs/PP-Modules. PP-Configurations may contain SARs and claim conformance to assurance packages.

Two types of PP-Configurations are identified, each has different requirements for their construction and are applicable depending on the needs of the consumer (risk owner). These are:

— Single Assurance PP-Configuration: This describes a configuration type in which the set of SARs that apply to the PP-Configuration's components are identical.

— Multi Assurance PP-Configuration: This describes a configuration type in which the SARs in the PP-Configuration components are not identical.

11.3.2 Requirements for PP-Configurations

11.3.2.1 General

A PP-Configuration shall be identified with a reference.

The reference identifier for a PP-Configuration shall be unique within a catalogue.

A PP-Configuration shall define the PP-Configuration components statement, a list that uniquely identifies all the PPs and PP-Modules that compose, by reference, the PP-Configuration. A PP-Configuration shall contain one PP and at least another PP-Configuration component. It may contain a PP-Module provided one of the PP-Module Bases are also included in the PP-Configuration. It may contain PPs that have no associated PP-Module.

A PP-Configuration shall define the TOE type to which it applies.

A PP-Configuration contains exactly, by reference, the SPD, security objectives, SFRs, and functional packages defined in its components; the specification of any additional element shall be done in one of its components.

A PP-Configuration shall provide a consistency rationale ensuring that the union of the elements defined in its components do not lead to contradiction.

A multi-assurance PP-Configuration shall describe the organization of the TSF in terms of the sub-TSFs that are defined in its components and shall define for each sub-TSF a set of SARs that is consistent with the corresponding component.

NOTE In the case of a multi-assurance PP-Configuration containing one PP and one PP-Module with different sets of SARs, the TSF organization is the following: the TSF is the union of the SFRs defined in the PP and in the PP-Module, and there are two sub-TSFs, which consist of the PP's TSF and the PP-Module's TSF. The same organization holds for a PP-Configuration composed of two PPs, which define the two sub-TSFs.

The sub-TSFs contained in a multi-assurance PP-Configuration may have some overlap. This does not impact on the applicable assurance requirements: Each sub-TSF shall be evaluated against its own set of SARs. This means that the overlapping parts may be evaluated against multiple sets of assurance requirements.

A PP-Configuration:

— may be used in context with the Direct Rationale approach described in B.5 and C.2.3. 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.

11.3.2.2 Components statement

A PP-Configuration:

— shall identify all the components of the PP-Configuration in a components statement. The components statement shall contain one PP and at least another component;

NOTE 1 The components statement is further described in C.3.3.

— shall not claim conformance to another PP-Configuration;

NOTE 2 If this is desired, the effect can be achieved by directly including all components from both PP-Configurations in one new defined PP-Configuration, where exact conformance can be checked and maintained.

— shall include the PP-Module Bases of all the PP-Modules included in the PP-Configuration. If a PP-Module defines alternative sets of PP-Module Bases, then only one of these sets shall be used in a PP-Configuration;

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

— for single-assurance PP-Configurations, may identify the sub-TSF that corresponds to each component defined by the PP-Configuration;

— for multi-assurance PP-Configurations, shall identify the sub-TSF that corresponds to each component defined by the PP-Configuration.

For a PP-Configuration that requires exact conformance, all PP-Configuration components shall specify each other in their respective allowed-with statements.

An exception to listing in the allowed-with statement is that a PP-Module shall not list any PPs or PP-Modules contained in its PP-Module Base in its allowed-with statement (because they are explicitly allowed by virtue of the fact that they are a base for the PP-Module).

11.3.2.3 Conformance claims and conformance statement

In this subclause the use of italic text indicates literal text that shall appear in the text of the PP-Configuration.

The conformance claims of a PP-Configuration:

a) shall state the edition of the relevant parts of the ISO/IEC 15408 series to which the PP-Configuration components claim conformance.

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

— *"ISO/IEC 15408-2 conformant";*

A PP-Configuration is ISO/IEC 15408-2 conformant if all the PPs and PP-Modules in the PP-Configuration are ISO/IEC 15408-2 conformant.

or

— *"ISO/IEC 15408-2 extended".*

A PP-Configuration is ISO/IEC 15408-2 extended if at least one PP or PP-Module is not based upon functional components in ISO/IEC 15408-2.

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

— "*ISO/IEC 15408-3 conformant*";

A PP-Configuration is ISO/IEC 15408-3 conformant if all SARs in that PP-Configuration, which may be simply inherited from its components, are based only upon assurance components in ISO/IEC 15408-3; or

— *"ISO/IEC 15408-3 extended".*

A PP-Configuration is ISO/IEC 15408-3 extended if at least one SAR in that PP-Configuration, which may be simply inherited from its components, is not based upon assurance components in ISO/IEC 15408-3.

d) may include an assurance package conformance claim;

More than one package may be claimed in a PP-Configuration. If an assurance package claim is made, it shall consist of one of the following statements for each package claim:

— "*Package Conformant*";

A PP-Configuration is conformant to an assurance package if the SARs of that PP-Configuration, which may be inherited from its components, are identical to the SARs in the assurance package.

— "*Package Augmented*"**.**

A PP-Configuration claims an augmentation of an assurance package if: the SARs of that PP-Configuration, which may be inherited from its components, contain all SARs in the assurance package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package.

e) shall not include a functional package conformance claim. Functional packages may be claimed by the components of the PP-Configuration;

f) shall not include a conformance claim with respect to other PP-Configurations, PPs or PP-Modules;

The PP-Configuration shall provide a conformance statement which describes the manner in which STs shall conform to this PP-Configuration:

g) for a PP-Configuration where all its PPs and PP-Modules are of the same conformance type, the conformance statement shall provide a single conformance type, that is one of:

   — "Exact conformance";

     If the PP-Configuration states that exact conformance is required, a ST shall conform to the PP-Configuration in an exact manner.

   — "Strict conformance";

     If the PP-Configuration states that strict conformance is required, a ST shall conform to the PP-Configuration in a strict manner.

   — "Demonstrable conformance".

     If the PP-Configuration states that demonstrable conformance is required, a ST shall conform to the PP-Configuration in a strict or demonstrable manner.

h) for a PP-Configuration where the PPs and PP-Modules do not require all the same conformance type, the conformance statement shall provide the list of the conformance types that are required by each of the PPs and PP-Modules composing the PP-Configuration. A ST shall conform to the PP-Configuration by conforming to each of the PPs and PP-Modules in the manner they require.

   NOTE This applies only to strict and demonstrable conformance, since the combination of exact conformance with other types of conformance is not allowed in a PP-Configuration.

   The compatibility of the multiple conformance shall be validated in the ST evaluation, in the same manner as when a ST claims conformance to several PPs that require different conformance.

i) may also include a reference to any evaluation methods/ activities that have been derived from ISO/IEC 18045. If evaluation methods/ activities that have been derived from ISO/IEC 18045 are associated with the PP-Configuration, then the conformance statement shall also include a statement in the following form:

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

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

NOTE 1 Specification of additional EMs/EAs that apply to one or more PP-Configuration components is only allowed for PP-Configurations of strict or demonstrable conformance type.

NOTE 2 There are implications for conformance statements in PP-Modules in the exact conformance case that are covered in C.2.2.5.

11.3.2.4 Assurance requirements

A PP-Configuration shall provide a SAR statement where the applicable assurance requirements and associated rationale are defined.

A single-assurance PP-Configuration shall define a single set of SARs for all the PP-Configuration components. In the exact conformance case, this set of SARs shall be identical to those declared in the individual PP-Configuration components. In the strict and demonstrable conformance case, this set of SARs shall be identical to or augment those declared in the individual PP-Configuration components.

A multi-assurance PP-Configuration shall define:

— The global set of SARs that applies to the entire TOE. In the exact conformance case, this set of SARs shall be identical to the common subset of SARs in the individual PP-Configuration components. In the strict and demonstrable conformance case, this set of SARs shall be identical to or augment the common subset of SARs in the individual PP-Configuration components;

— For each sub-TSF, the set of SARs that applies. In the exact conformance case, this set of SARs shall be identical to the set of SARs declared in the PP-Configuration component for the sub-TSF. In the strict and demonstrable conformance case, this shall be identical to or augment the set of SARs declared in the PP-Configuration component for the sub-TSF.

A PP-Configuration may use the pre-defined EALs (EAL1 to EAL7) given in ISO/IEC 15408-5, assurance packages defined in external references and/or SARs defined within the PP-Configuration itself to define its SAR statement.

NOTE 1 The multi-assurance evaluation allows applying multiple pre-defined EALs. However, for the same reasons as for PPs in the general model, PP-Configurations can claim sets of SARs that are different from pre-defined EALs and/or that contain extended SARs.

A PP-Configuration may define distinctive names for the sets of SARs that apply to the entire TOE and to each sub-TSF. However, the use of an (augmented) pre-defined EAL or an (augmented) assurance package defined in one of the PP-Configuration's components or in another external reference requires the usage of the same name.

A multi-assurance PP-Configuration shall provide an assurance rationale for:

— the consistency of the global set of SARs with regard to the threat models as defined in the SPDs of the PPs and PP-Modules in the PP-Configuration;

— the consistency of the global set of SARs and all the sets of SARs for the sub-TSF with each other.

In constructing the global set of SARs for the exact conformance case, the multi-assurance PP-Configuration author chooses the hierarchically lowest SAR if sub-TSFs specify hierarchically different SARs. For example, if there are three sub-TSFs with ADV_FSP.1, ADV_FSP.2 and ADV_FSP.3, respectively, then the global set of SARs would contain ADV_FSP.1. However, if one of the sub-TSFs did not contain an ADV_FSP component, then ADV_FSP would not be in the global set of SARs. For a strict/demonstrable case, the multi-assurance PP-Configuration author may choose ADV_FSP.1 or a higher component thus augmenting the assurance requirements for some of its sub-TSFs (even in the case when a sub-TSF does not define any ADV_FSP component) provided the assurance rationale is consistent.

NOTE 2 In most cases (and always in the exact conformance case), the global set of SARs can be built as the common set of SARs that apply to all of the sub-TSFs. However, as it is the case with STs in the general model, the PP-Configuration (of strict or demonstrable conformance type) can require additional or higher SARs. The evaluation of the PP-Configuration ensures the consistency of the claim, similar to the general model for the conformance with two or more PPs defining different sets of SARs, and similar to the approach for a multi-assurance ST which can extend the sets of SARs defined in the PP-Configuration the ST claims conformance to.

NOTE 3 A PP-Configuration cannot claim less assurance requirements as the global set of SARs/assurance package than those contained in the common set of SARs that apply to all of the sub-TSFs.

NOTE 4 The PP-Configuration assurance rationale contributes to ensuring that the multiple sets of SARs do not undermine the security expected for the assets that are shared between the PPs and PP-Modules in the PP-Configuration. The PP-Configuration assurance rationale relies on and/or reuses the assurance rationales given in the PPs and PP-Modules.

For exact conformance type PP-Configurations, augmentation of the SARs for each sub-TSF (by the PP-Configuration) is not allowed.

If additional SARs are specified, or SARs are replaced with hierarchically higher SARs then any derived evaluation methods / evaluation activities required by the components of the PP-Configuration shall be

addressed in the assurance rationale to demonstrate that the evaluation methods / evaluation activities required by the PP-Configuration:

— are still adequate, i.e. the new SAR has no effect on the EMs/EAs in the components and the assurance that they provide; or

— have been addressed by defined refinements to the original EMs/EAs in the components so that the resulting EMs/EAs required for the PP-Configuration generate assurance that is the same or higher than the original EMs/EAs applied to the components; or

— have been supplemented by additional EMs/EAs to so that the resulting EMs/EAs generate assurance that is the same or higher than the original EMs/EAs applied to the components.

EXAMPLE 1 An activity that was an examination of documentation for a lower SAR but where additional testing might be needed for a hierarchically higher SAR can supplement the original documentation evaluation activities with additional evaluation activities that require testing.

EXAMPLE 2 Figure 5 shows an example of multi-assurance PP-Configuration with one PP, A, and two PP-Modules, X and Y. It illustrates the default construction of the global set of SARs for the entire TOE, which consists of SAR_C, i.e. the common set of SARs of each of the PP-Configuration components A, X and Y. In the example, the sets of SARs that apply to the sub-TSFs defined in A, X and Y are unchanged as well.

NOTE 5 The rules allow the augmentation of the sets of SARs.

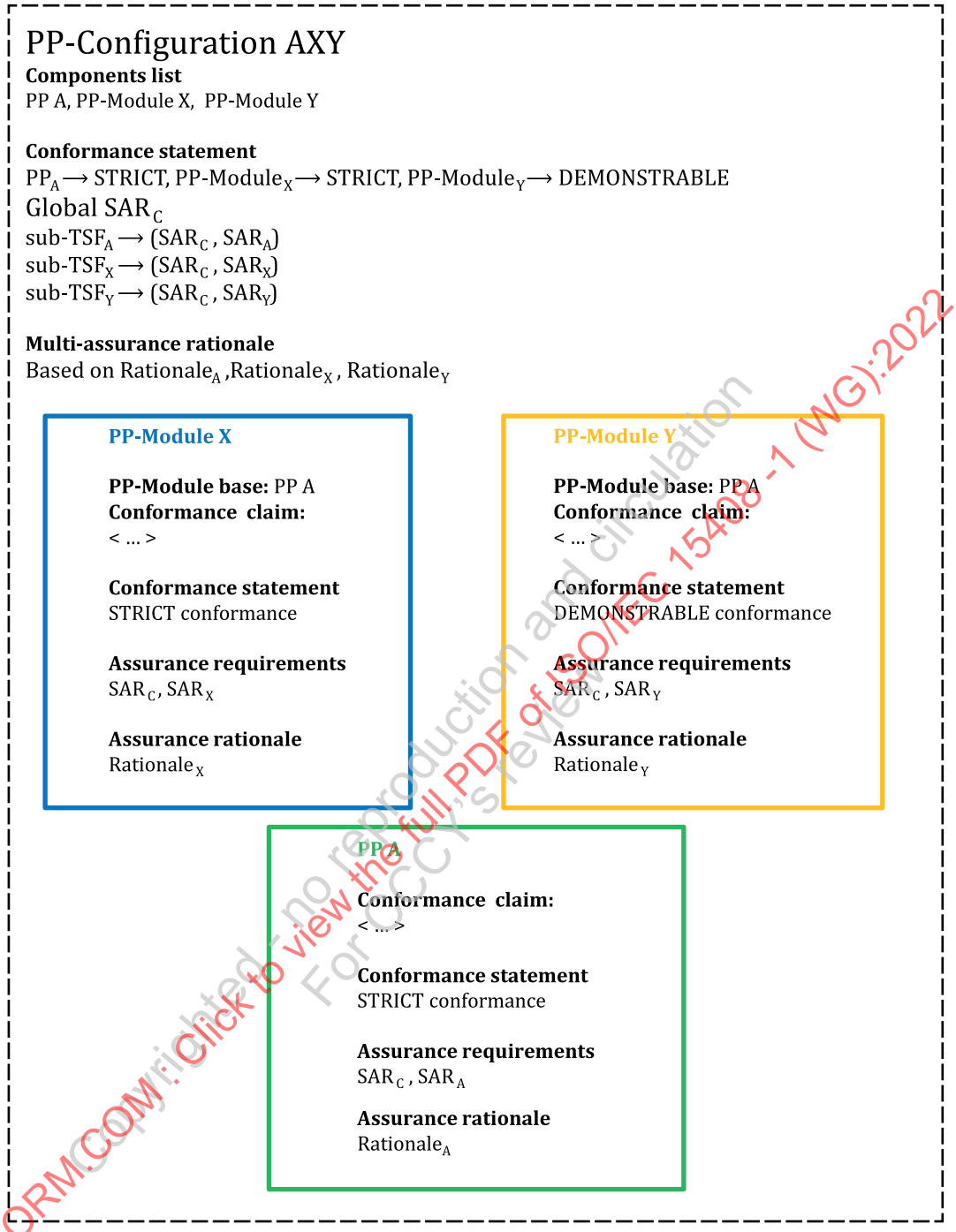

Figure 5 — Example of PP-Configuration

11.3.3 Usage of PP-Configurations

Figure 6 shows the usage of single and multi-assurance PP-Configurations. Figure 7 gives the detail of PP-Configuration components. Figure 8 shows the assurance classes that are used for evaluating PPs, PP-Configurations and STs.

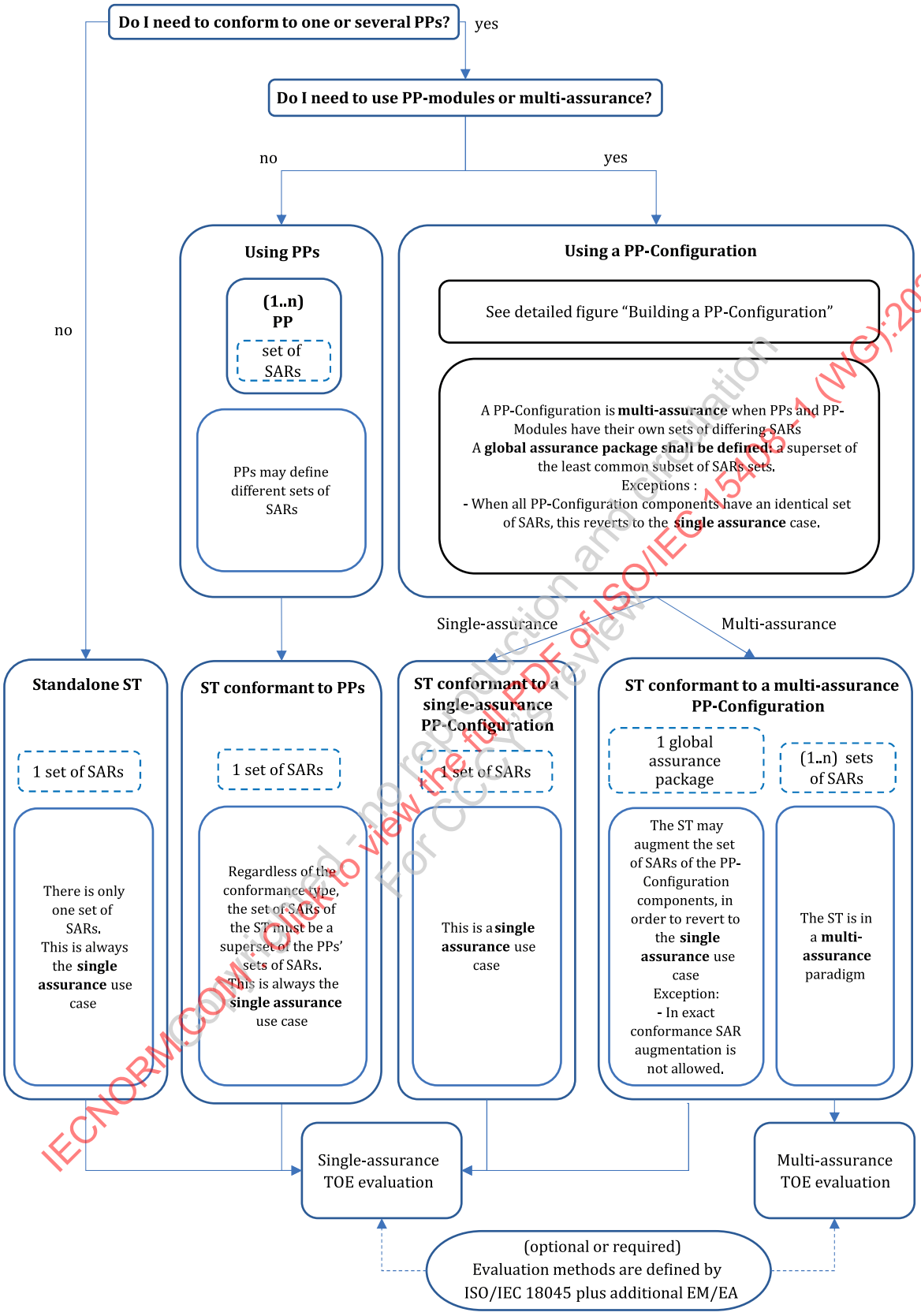

Figure 6 — Usage of single and multi-assurance PP-Configurations

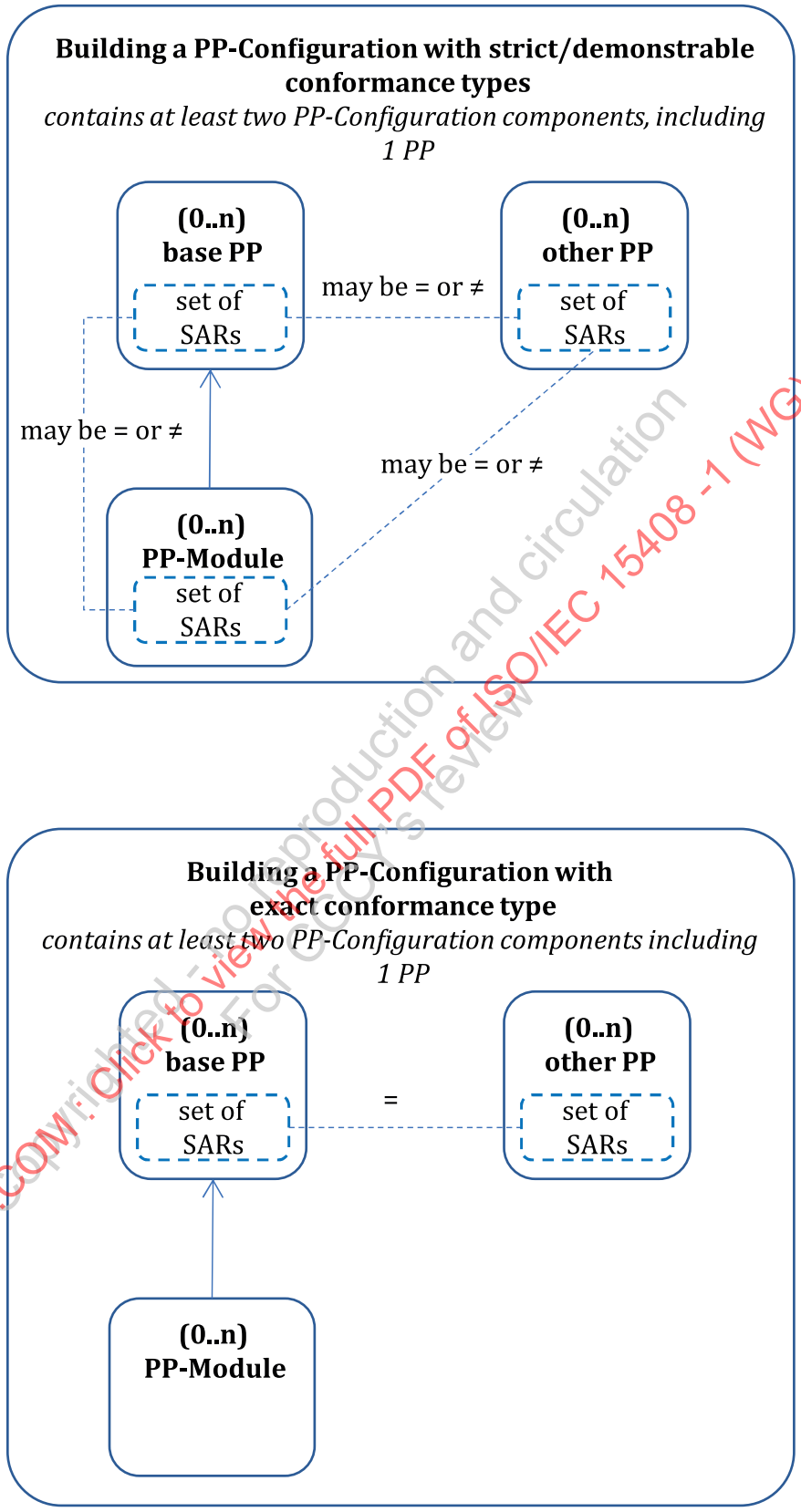

Figure 7 — Composition of PP Components

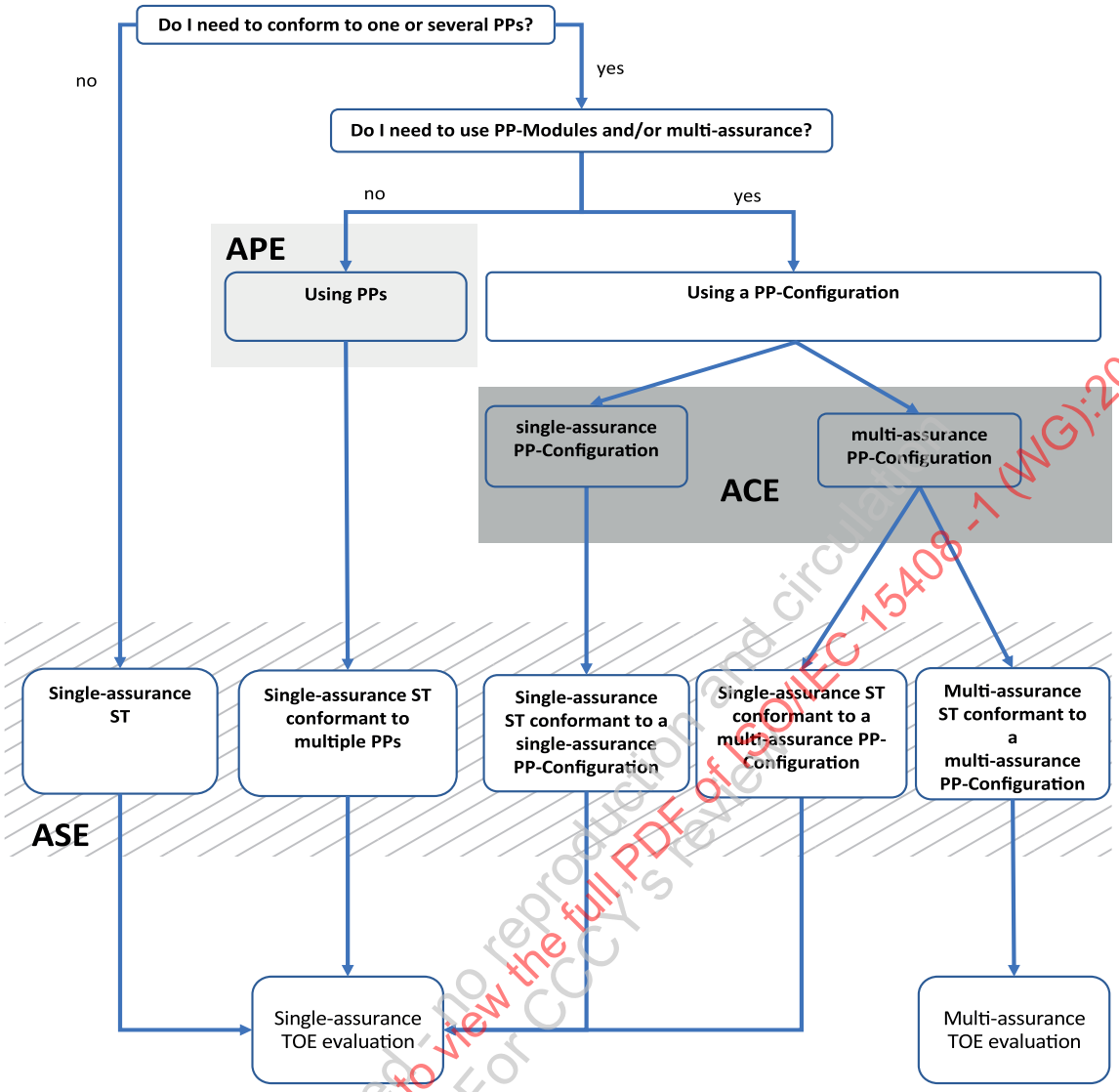

Figure 8 — Assurance classes used to evaluate PPs, PP-Configurations and STs

12 Security Targets (STs)

12.1 General

A ST is a document that describes a specific TOE, the conformance claims applicable to the evaluation of the TOE, the security problem to be addressed, the security objectives for the TOE and its operational environment, the security requirements applicable to solving the stated security problem, and additional material necessary to describe the TOE sufficiently for evaluation. STs are generally based upon PPs or PP-Configurations that describe a security problem and security requirements for a TOE type that is relevant to the specific TOE.

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

Further information about STs, Annex D shall be used in conjunction with the clauses of this document.

12.2 Conformance claims and statements

In this subclause the use of italic text indicates literal text that shall appear in the text of the ST.

The conformance claims of a ST:

a) shall state the edition of relevant parts of the ISO/IEC 15408 series to which the ST claims conformance;

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

— *"ISO/IEC 15408-2 conformant"*

A ST is ISO/IEC 15408-2 conformant if all SFRs in that ST are based only upon functional components in ISO/IEC 15408-2, or

— *"ISO/IEC 15408-2 extended".*

A ST is ISO/IEC 15408-2 extended if at least one SFR in that ST is not based upon functional components in ISO/IEC 15408-2.

NOTE 1 When a TOE is successfully evaluated to a ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also claim to be ISO/IEC 15408-2 conformant.

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

— *"ISO/IEC 15408-3 conformant";*

A ST is ISO/IEC 15408-3 conformant if all SARs in that ST are based only upon assurance components in ISO/IEC 15408-3, or

— *"ISO/IEC 15408-3 extended".*

A ST is ISO/IEC 15408-3 extended if at least one SAR in that ST is not based upon assurance components in ISO/IEC 15408-3.

d) may include a conformance claim made with respect to packages.

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

— *"Package Conformant"*:

A ST 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 ST without modification;

— for assurance packages, the SARs of that ST are identical to the SARs in the assurance package.

— *"Package Augmented"*

A ST claims augmentation of 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 ST but the ST contains at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package;

— for assurance packages, the ST contains all SARs in the assurance package but contains at least one additional SAR or one SAR that is hierarchically higher than an SAR in the assurance package.

— *"Package Tailored"*

STs shall not claim or perform tailoring.

More than one package may be claimed in a ST.

Where STs claim exact conformance to PP(s) they shall not claim conformance to any packages, including any packages claimed by the PP.

Where STs claim strict or demonstrable conformance to PPs they shall not also claim conformance to the packages claimed in the PPs unless the ST augments the package as claimed in the PP, i.e. the PP may claim a package as <package>-conformant, <package>-augmented or <package>- tailored, but if the ST does not itself augment the conformant/augmented/tailored version of the package in the PP, then it will not claim conformance to the package. The ST claims <package>-augmented only in the case where the ST augments the packages beyond that claimed by the PP.

Where STs claim conformance to a PP-Configuration they shall not also claim conformance to any functional packages, including any functional packages claimed by the PP-Configuration's components.

Where STs claim strict or demonstrable conformance to a PP-Configuration they shall not also claim conformance to the assurance packages claimed in the PP-Configuration unless the ST augments the assurance package as claimed in the PP-Configuration, i.e. the PP-Configuration may claim an assurance package as <package>-conformant or <package>-augmented but if the ST does not itself augment the conformant/augmented version of the package in the PP-Configuration, then it will not claim conformance to the assurance package. The ST claims <package>-augmented only in the case where the ST augments the assurance package beyond that claimed by the PP-Configuration.

NOTE 2 For exact conformance, it is allowed to claim conformance to a PP that claims conformance to a `package, or a PP-Configuration that has components that claim conformance to a package, but those are not reflected in the ST's conformance claim.

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

— "*PP Conformant*";

A PP or TOE meets specific PP(s).

A Direct Rationale ST may only claim conformance to one or more other Direct Rationale PPs. (See Annex B)

f) may also include a conformance claim with respect to PP-Configurations:

— a ST may claim conformance to exactly one PP-Configuration;

— a Direct Rationale ST shall only claim conformance to a PP-Configuration if that PP-Configuration uses the Direct Rationale approach.

NOTE 3 The evaluation of a PP-Configuration can be performed upfront, independently of any product evaluation. Alternatively, the evaluation of a PP-Configuration can be performed during the evaluation of a conformant ST, prior to evaluating the ST conformance claim. See 13.3 for a discussion of the evaluation of PP-Configurations.

PP-Modules are used to build specific PP-Configurations on top of one or more PP-Module Base(s). Hence, PP-Modules shall only be used by STs through claimed PP-Configurations.

g) if evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 are identified in the conformance statement of any package, PP, PP-Module, or PP-Configuration to which the ST claims conformance, then the conformance claim shall also include a claim in the following form:

"The TOE is evaluated using evaluation methods/ evaluation activities defined in <reference>."

In this statement, <reference> is replaced by the identification of the location of the relevant evaluation methods and evaluation activities.

STs that reference evaluation methods/ activities are not required to reproduce the text of the evaluation methods/ activities within the ST.

A ST shall only make a conformance claim for evaluation methods/ evaluation activities that are included in a package, PP, PP-Module, or PP-Configuration claimed by the ST.

NOTE 4 The reader is reminded that it can be the case that a ST claims no PP or PP-Configuration but can still directly specify a package.

A ST can claim conformance to several PPs. If one such PP has exact conformance type, then all PPs shall be of the exact conformance type. Otherwise, the PPs can have a mix of strict and demonstrable types, and the consistency of the combination of demonstrable and strict conformance shall be validated as part of the ST evaluation.

For more information and requirements on the conformance claims for STs see Annex D.

For more information and requirements on conformance types see Annex E.

12.3 Assurance requirements

A ST that claims conformance with ISO/IEC 15408-3 (possibly extended) shall define the global set of SARs that applies to the TOE.

A ST may define a distinctive name for the set of SARs that are applicable. However, the use of an (augmented) pre-defined EAL or an (augmented) assurance package defined in an applicable external reference shall require the usage of the same name.

If additional SARs are specified, or SARs are replaced with hierarchically higher SARs in an ST then any derived evaluation methods / evaluation activities shall be addressed in the assurance rationale to demonstrate that the evaluation methods / evaluation activities used by the ST:

— are still adequate, i.e. the new SAR has no effect on the EMs/EAs specified for use in the ST and the assurance that they provide; or

— have been addressed by defined refinements to the original EMs/EAs specified by the ST so that the resulting EMs/EAs required for the ST generate assurance that is the same or higher than the original EMs/EAs applied to the ST; or

— have been supplemented by additional EMs/EAs to so that the resulting EMs/EAs generate assurance that is the same or higher than the original EMs/EAs applied to the ST.

EXAMPLE An activity that was an examination of documentation for a lower SAR but where additional testing might be needed for a hierarchically higher SAR can supplement the original documentation evaluation activities with additional evaluation activities that require testing.

12.4 Additional requirements in the exact conformance case

12.4.1 Additional requirements for the conformance claim

A ST shall not claim conformance to an exact conformance PP/PP-Configuration and, at the same time, to other PPs which are not of exact conformance type, i.e. a PP/PP-Configuration of exact conformance shall not be combined with strict or demonstrable conformance.

12.4.2 Additional requirements for the SPD

A ST claiming exact conformance:

— shall contain the SPD of all the packages and the PPs or PP-Configuration to which it is claiming exact conformance, including all SPD elements;

— shall not include any SPD-elements that are not present in the packages or PPs/PP-Configuration to which it is claiming exact conformance.

NOTE The SPD that is instantiated in the ST from a PP-Configuration contains exactly the SPD-elements present in the PP-Configuration's components (PPs and PP-Modules). Note that PP-Configuration components can combine to change or eliminate SPD-elements (e.g. an assumption in a base PP can become a threat that is countered by a PP-Module on top of that base PP), so the result that appears in the ST considers these kinds of modifications. See 11.3.

12.4.3 Additional requirements for the security objectives

A ST claiming exact conformance:

— shall contain all the security objectives for the TOE specified in all of the PPs to which it claims conformance;

— shall not specify additional security objectives for the TOE that are not specified in the combination of the PPs to which it claims conformance;

— shall contain all of the security objectives for the operational environment that are specified in the combination of PPs to which it claims conformance; and

— shall not specify additional security objectives for the operational environment that are not present in the combination of PPs to which it claims conformance.

The same is true for PP-Configurations. The security objectives that are instantiated in the ST from a PP-Configuration contain exactly the security objectives present in the PP-Configuration's components. It should be noted that PP-Configuration components can combine to change or eliminate security objectives (e.g. a security objective for the environment in a base PP may become a TOE security objective in a PP-Module using that base PP), so the resulting ST reflects these kinds of modifications.

12.4.4 Additional requirements for the security requirements

A ST shall contain all the SARs present in the PPs, and all the SFRs present in the PP-Configuration components, with the following exceptions:

— ST authors shall not include additional or hierarchically higher security requirements;

— SFRs designated as selection-based SFRs in the PPs or PP-Modules shall be excluded if the selection that requires their inclusion is not chosen by the ST author;

— SFRs designated as optional SFRs in the PPs or PP-Modules may be included or excluded while maintaining its exact conformance claim.

NOTE 1 SFRs in an exact conformance PP can be iterated and refined (as stated in ISO/IEC 18045 for ASE_CCL.1-12).

NOTE 2 See 7.3.2.6 for further information in regard to optional and selection-based SFRs.

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

12.5 Additional requirements in the multi-assurance case

A multi-assurance ST shall claim conformance to exactly one multi-assurance PP-Configuration and no other PP or PP-Configuration.

A multi-assurance ST shall organize the TSF in sub-TSFs and claim a specific set of SARs for each of the sub-TSFs and a global set of SARs for the entire TOE: this can be achieved exclusively through the conformance to a multi-assurance PP-Configuration. The TSF structure defined in the ST is inherited from the PP-Configuration, and the sets of SARs that apply to them in the ST are either identical to the ones defined in the PP-Configuration or augmented.

A multi-assurance ST may extend the multi-assurance PP-Configuration (of strict or demonstrable conformance type) with additional SFRs (and related SPD and security objectives as necessary) so that

each new element completes at a minimum one PP or PP-Module of the PP-Configuration provided the required conformity rules are satisfied, i.e. the new SFRs are aimed at extending the sub-TSFs defined by the components of the PP-Configuration. As a consequence, the extended sub-TSFs are subject to the set of SARs as defined in the original PPs/PP-Modules.

A multi-assurance ST may claim the sets of SARs defined in the multi-assurance PP-Configuration, or, in the case of strict or demonstrable conformance type, may provide a rationale to claim "augmented" sets of SARs, similar to STs in the general model.

In order to conform with two or more PPs according to their respective sets of SARs, a multi-assurance PP-Configuration composed of the PPs shall be defined and claimed by the ST.

A ST that claims conformance with a multi-assurance PP-Configuration and augments all the applicable sets of SARs to reach the same set of SARs for the entire TOE and all of the sub-TSFs becomes a single-assurance ST. In this case, the evaluation of the TOE shall follow the single-assurance evaluation approach. This is only allowed for PP-Configurations of strict or demonstrable conformance type.

A ST that claims conformance with several PPs can only define a global set of SARs that applies to the entire TOE, thus giving rise to a single-assurance ST. The ASE rules for ensuring the consistency of the assurance requirements of the single-assurance ST with regard to the PPs apply.

A ST that claims conformance with one single-assurance PP-Configuration, i.e. which defines only one set of SARs for the entire TOE and its parts, cannot become a multi-assurance ST. The reason is that the multi-assurance consistency rules are defined at PP-Configuration level. In order to achieve this, a multi-assurance PP-Configuration derived from the PP-Configuration shall be defined and evaluated.

For more information on multi-assurance PP-Configurations and STs see 12.4.2. A ST that claims conformance with a multi-assurance PP-Configuration may become a multi-assurance ST by defining, for each sub-TSF, the applicable set of SARs. This will be either the same set of SARs inherited from the PP-Configuration, or a larger set (augmentation only valid only in the strict and demonstrable conformance type cases) which requires the update of the assurance rationale provided in the PP-Configuration.

A multi-assurance ST may define distinctive names for the sets of SARs that apply to the entire TOE and to each sub-TSF. The names shall be consistent with the names given in the PP-Configuration. The use of an (augmented) pre-defined EAL or an (augmented) assurance package defined in an applicable external reference requires the usage of the same name.

A multi-assurance ST that claims strict or demonstrable conformance to a PP-Configuration and extends the sets of SARs of the PP-Configuration it claims conformance to shall provide an assurance rationale that justifies the consistency of the extension.

A multi-assurance ST shall conform to each and all of the individual conformance types that are identified in the conformance statement of the multi-assurance PP-Configuration.

NOTE A ST that claims conformance with more than one PP can only define a global set of SARs, which applies to the entire TOE. In such a case, the ASE rules for ensuring the consistency of the assurance requirements of the ST with regard to the PPs apply.

Figure 9 shows an example of a multi-assurance ST that claims conformance to PP-Configuration "AXY" composed of PP A and two PP-Modules X and Y. The TSF structure consists of the sub-TSF defined in A, X and Y. The global set of SARs (SAR_C) and the multiple sets of SARs applicable to the sub-TSFs come from the PP-Configuration without any augmentation.

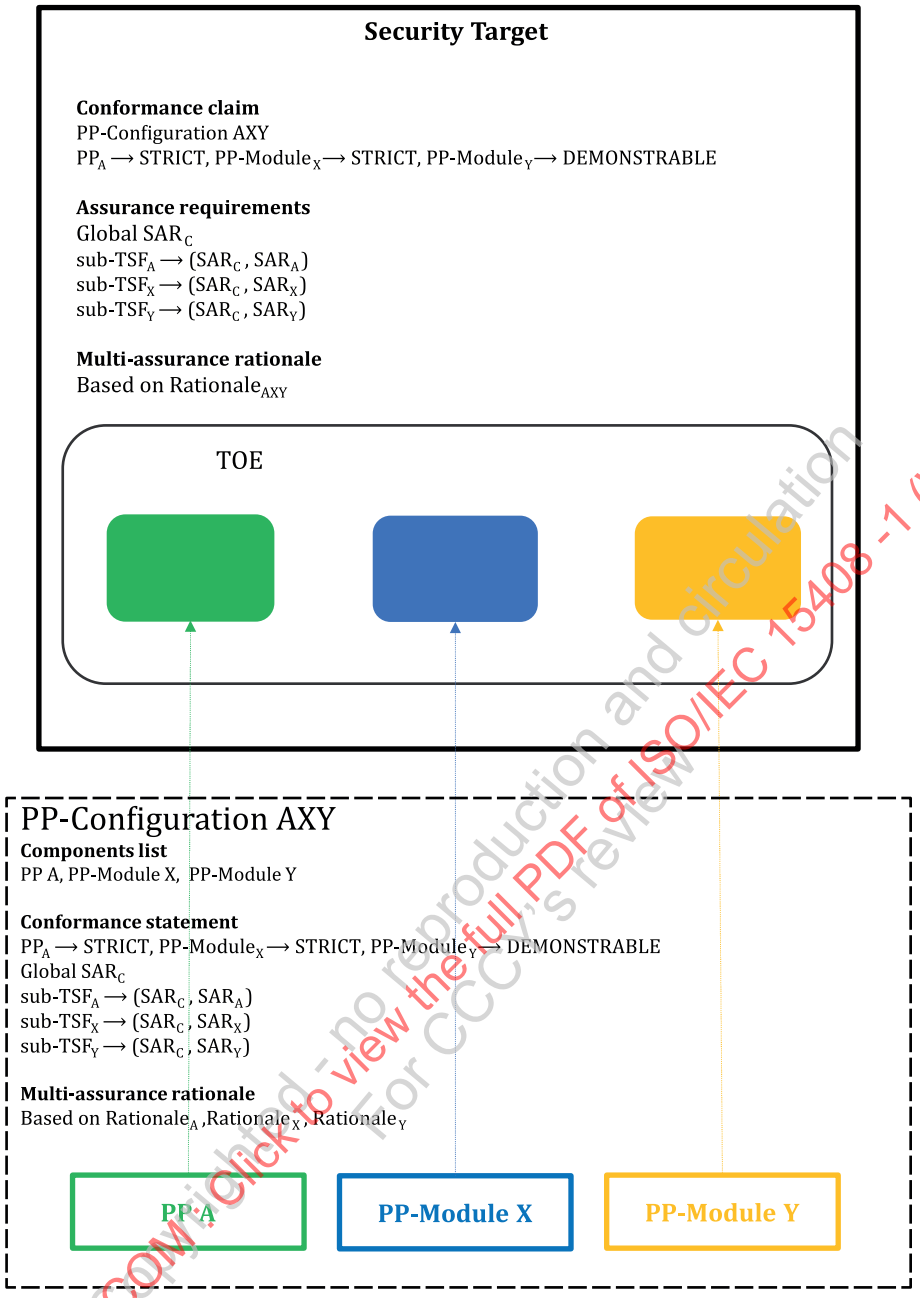

Figure 9 — Example of multi-assurance ST

13 Evaluation and evaluation results

13.1 General

This clause presents the expected results from PP, PP-Configuration and ST/TOE evaluations performed according to either ISO/IEC 18045, and/or additional evaluation methods and activities.

The goal of evaluation is to provide objective and repeatable results that can be cited as evidence, even if there is no absolute objective scale for representing the results of a security evaluation.

NOTE 1 A trade-off between following the relevant state of the art versus a sufficient level of repeatability is often necessary. Therefore, properties such as objectivity and repeatability are not seen as absolute by the standard, but rather as goals that can be approached in different ways. For example, ISO/IEC 15408-4 provides one such framework for preserving objectivity and repeatability when deriving evaluation activities from ISO/IEC 18045.

An evaluation result represents the findings of a specific type of investigation of the security properties of a TOE. Such a result does not automatically guarantee fitness for use in any particular application environment. The decision to accept a TOE for use in a specific application environment is based on consideration of many security issues including the evaluation findings.

Figure 10 describes the various evaluations that are needed to provide confidence in the evaluation results for a TOE.

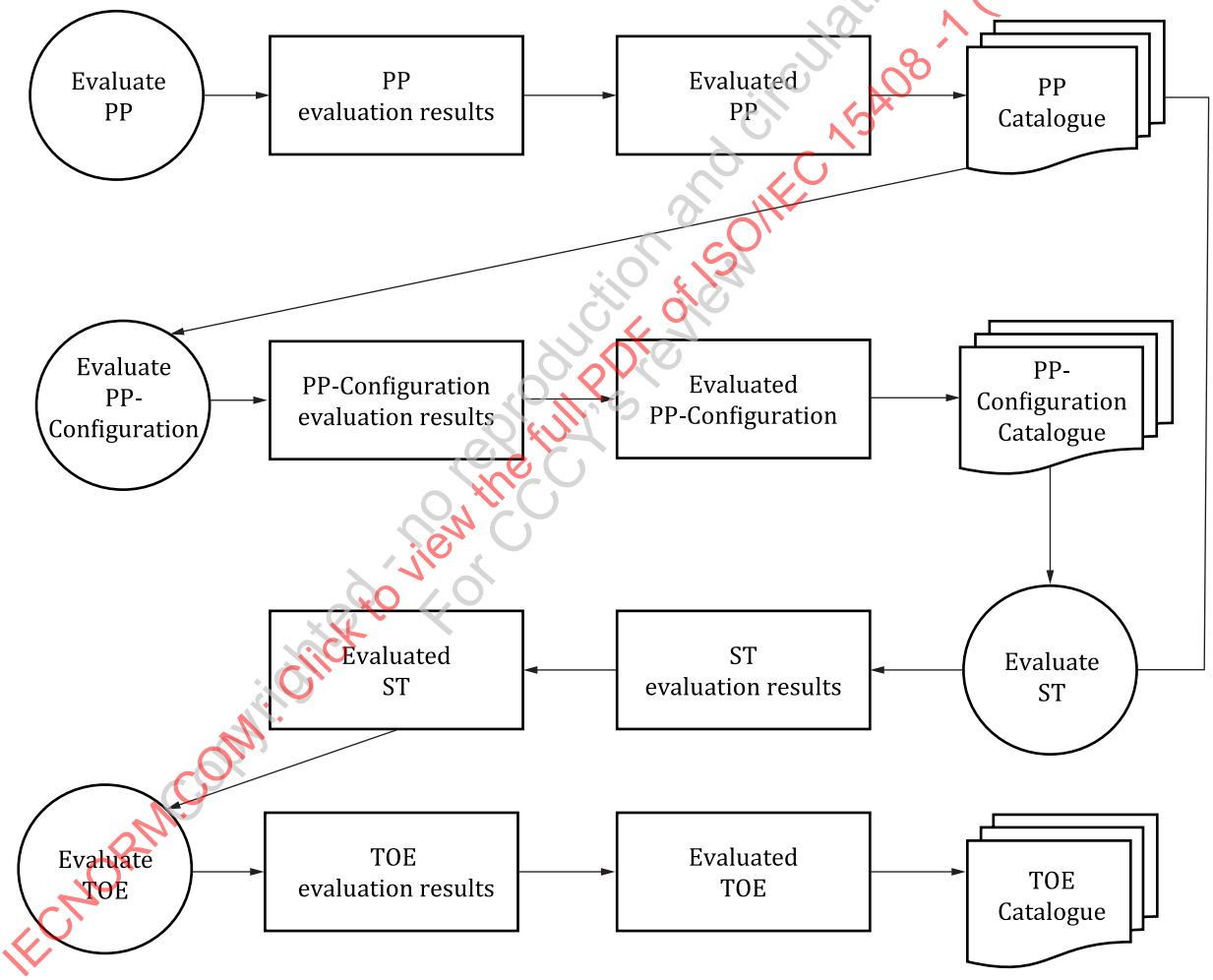

Figure 10 — Evaluation flow

The ISO/IEC 15408 series gives criteria for four types of evaluation:

a) a PP evaluation which is based on the APE class given in ISO/IEC 15408-3, described in 13.3;

b) a PP-Configuration evaluation which is based on the ACE class given in ISO/IEC 15408-3, described in 13.3;

c) a ST evaluation which is based on the ASE class given in ISO/IEC 15408-3, described in 13.4;

d) a TOE evaluation, which is based on an evaluated ST and the criteria for evaluating the security requirements claimed by the ST, described in 13.5.

PP and PP-Configuration evaluations provide confidence that the PP and/or PP-Configuration meets the requirements of the ISO/IEC 15408 series. Catalogues of PPs and PP-Configurations can be maintained by authorities or others which define the criteria for inclusion in the catalogue.

NOTE 2 The criteria for inclusion in a catalogue are out of scope for the ISO/IEC 15408 series.

PP-Modules are only evaluated as part of an evaluation based on a PP-Configuration.

Packages are only evaluated as part of a PP-Configuration, PP, or ST evaluation.

NOTE 3 In practice, a ST that claims conformance with some non-evaluated PP-Configurations can still be evaluated by performing the PP-Configuration evaluation first.

A ST evaluation leads to an intermediate result that is used in the frame of a TOE evaluation. Optionally, STs may be developed with conformance claims to packages, PPs and PP-Configurations.

ST/TOE evaluations can lead to catalogues of evaluated TOEs. In many cases these catalogues refer to the IT products that the TOEs are derived from rather than the specific TOE. Therefore, the existence of an IT product in a catalogue cannot be construed as meaning that the whole IT product has been evaluated; instead the actual ST defines the actual extent of the TOE evaluation.

Refer to the Bibliography for examples of such catalogues.

13.2 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 series does not state requirements for such evaluation schemes.

Supporting greater comparability between evaluation results is also achieved through the use of common evaluation methods producing these evaluation results. Use of a common evaluation methodology contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgement and background knowledge for which consistency is more difficult to achieve. In order to enhance the consistency of the evaluation findings, the final evaluation results can be submitted to a certification process.

NOTE 2 The ISO/IEC 15408 series does not provide requirements to assess the competences of developers or evaluators. ISO/IEC 19896-3 provides competency requirements for the ISO/IEC 15408 series evaluators that can be used as a support in the evaluation process. However, it only addresses basic methodology competences and does not address the way to assess:

— technology-specific knowledge and skills such as those required to perform ADV, ATE or AVA_VAN evaluation on a given product type;

— sector-specific knowledge that is typically required to perform ASE, APE or ACE evaluation.

Additionally, specific skills required by evaluations made in accordance with ISO/IEC 15408 can require additional competence assessment methods. For example, to assess skills related to formal methods.

For the ISO/IEC 15408 series, the generic methodology for IT security evaluations is given in ISO/IEC 18045. More specific evaluation methods and activities may be derived from ISO/IEC 18045 by using the framework given in ISO/IEC 15408-4, by refining standard assurance components or by defining extended assurance components.

It can be necessary for PP authors to augment the generic methodology for IT security evaluations given in ISO/IEC 18045 with a method that includes technology-specific evaluation activities.

A certification process, which is outside the scope of the ISO/IEC 15408 series, can include an independent inspection of the results of the evaluation leading to the production of a final certificate or

approval, which can be made publicly available. The certification process is a means of gaining greater consistency in the application of IT security criteria.

13.3 Evaluation of PPs and PP-Configurations

Basing a PP or a ST on an evaluated PP/PP-Configuration has two advantages:

— there is much less risk that there are errors, ambiguities, or gaps in the PP/PP-Configuration. If any problems with that would have been found during the evaluation of that PP/PP-Configuration, are found during the writing or evaluation of the new ST, significant time can elapse before the PP/PP-Configuration is corrected;

— evaluation of the new PP/PP-Configuration can re-use the previous evaluation results, resulting in less effort being employed in the evaluation of the new PP/PP-Configuration.

If the evaluation of a PP is required then the APE criteria, given in ISO/IEC 15408-3 shall be used.

If the evaluation of a PP-Configuration is required, then the ACE criteria given in ISO/IEC 15408-3 shall be used.

The goal of such evaluations is to demonstrate that the PP, or PP-Configuration is complete, internally consistent, and technically sound and suitable for use as a template on which to build a ST or another PP.

The method of stating evaluation results for PPs and PP-Configurations is described in 13.7.

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

13.4 Evaluation of STs

A ST evaluation determines the sufficiency of the TOE, the operational environment and the internal consistency of the descriptions and requirements it contains.

The ST evaluation shall be carried out by applying the ASE evaluation criteria, defined in ISO/IEC 15408-3. The methods and activities used to apply the ASE criteria are determined by the evaluation methodology that is associated with the ST, which is specified in ISO/IEC 18045 or by evaluation methods/ activities that are derived from ISO/IEC 18045. Derived evaluation methods/ evaluation activities are validated outside of the ISO/IEC 15408 series and ISO/IEC 18045 framework.

Users of this document/series should be aware that evaluation schemes do not always approve the use of particular evaluation methods/evaluation activities. A ST can require evaluation methods/evaluation activities, and an evaluation scheme can decide not to carry out evaluations following this ST.

The method of stating ST evaluation results is described in 13.7. These results also identify any PP(s) and package(s) to which the ST claims conformance.

13.5 Evaluation of TOEs

A TOE evaluation determines that the correctness of the TOE against the criteria defined in the ST. As said earlier, the TOE evaluation does not assess the correctness of the operational environment.

The TOE evaluation is more complex. The principal inputs to a TOE evaluation are the evaluation evidence, which includes the TOE and the ST, but will usually also include input from the development environment, such as design documents or developer test results.

The TOE evaluation consists of applying the SARs (from the ST) to the evaluation evidence. The method to apply a specific SAR to a TOE is determined by ISO/IEC 18045 and by evaluation methods/ activities that are derived from ISO/IEC 18045. Derived evaluation methods/evaluation activities are validated outside of the ISO/IEC 15408 series and ISO/IEC 18045 framework. Users of this document/ series should be aware that evaluation schemes do not always approve the use of particular evaluation

methods/evaluation activities. A ST may require evaluation methods/evaluation activities, and an evaluation scheme can decide not to carry out evaluations following this ST.

How the results of applying the SARs are documented, and what reports need to be generated and in what detail, is determined by both the evaluation methodology that is used and the evaluation scheme under which the evaluation is carried out.

The TOE evaluation may be carried out after TOE development has finished, or in parallel with TOE development, provided that the appropriate assurance components are chosen for this evaluation.

The method of stating ST/TOE evaluation results is described in 13.7.

13.6 Evaluation methods and evaluation activities

Generic IT evaluation methods and activities for each of the security assurance classes given in ISO/IEC 15408-3 are provided in ISO/IEC 18045. The evaluation methods and activities given in ISO/IEC 18045 are high level and depending on the technology type, the assurance level, or the security problem described, the provision of more specific evaluation methods and activities can be needed.

Such evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 may be published either as an inclusion in PPs, PP-Modules and packages or as separate supporting documents.

13.7 Evaluation results

13.7.1 Results of a PP evaluation

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

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

13.7.2 Results of a PP-Configuration evaluation

The results of a PP-Configuration evaluation shall include a “conformance claim” in accordance with 11.3.

Once a PP-Configuration has been evaluated, a ST evaluation may rely on the results of the PP-Configuration evaluation.

NOTE 1 ISO/IEC 15408-3 provides evaluation criteria for PP-Configurations in the ACE class.

NOTE 2 The evaluation of a PP-Configuration can arise in two situations, with no impact on the evaluation methodology:

— independently of any product evaluation, or

— as the first step of the evaluation of a ST that claims conformity with the PP-Configuration. Otherwise the conformance claim is meaningless, and the ST evaluation would fail in this aspect.

13.7.3 Results of a ST/TOE evaluation

13.7.3.1 General

The results of a ST evaluation shall include a “conformance claim” as defined in 12.2.

A successful TOE evaluation requires a successful ST evaluation. The result of the TOE evaluation process is either:

— a statement that all SARs have been met, and that therefore there is the specified level of assurance that the TOE meets the SFRs as stated in the ST;

— a statement that not all SARs have been met and that therefore there is not the specified level of assurance that the TOE meets the SFRs as stated in the ST.

NOTE In some cases the evaluation results are subsequently used in a certification process, but this certification process is outside the scope of the ISO/IEC 15408 series.

If the TOE evaluation has resulted in a pass statement, the underlying product can be eligible for inclusion in a catalogue of successfully evaluated products.

13.7.3.2 Use of ST/TOE evaluation results

Once a ST and a TOE have been evaluated, asset owners can have the assurance, as defined in the ST, that the TOE, together with the operational environment, counters the stated threats. The evaluation results may be used by the asset owner as part of a risk-acceptance decision related to exposing the assets to the threats.

However, risk owners should carefully check whether:

a) the SPD in the ST matches their own security problem;

b) their operational environments conform (or can be made to conform) to the security objectives for the operational environment described in the ST;

c) any guidance documents provided by the developer in the context of the TOE evaluation are followed during the installation, configuration, and operation of the TOE.

If any of these conditions do not hold true, the associated assurance cannot be relied on and the evaluation results should be treated accordingly 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 can 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 can no longer be valid.

NOTE If assurance is to be maintained, re-evaluation is needed. The ISO/IEC 15408 series can be used for this re-evaluation, but detailed procedures for re-evaluation are outside of the scope of this document.

13.8 Multi-assurance evaluation

For a multi-assurance PP-Configuration, the ACE requirements, given in ISO/IEC 15408-3, ensure that the combination of different sets of SARs does not undermine the expected security of the underlying assets, as defined in the SPDs of the PPs and PP-Modules that compose the PP-Configuration.

For a multi-assurance ST, the ASE requirements, given in ISO/IEC 15408-3, ensure that the ST is conformant to a multi-assurance PP-Configuration which satisfies ACE assurance requirements. This means that the organization of the TSF in sub-TSFs and the sets of SARs that apply to them are consistent with the PP-Configuration. For each sub-TSF this means that the multi-assurance ST claims a set of SARs that is identical or an augmentation of the set of SARs defined in the PP-Configuration for the corresponding component (PP or PP-Module).

The general model of the standard, which holds in a multi-assurance evaluation, requires that the evaluator evaluates the TSF in order to ensure the security of the TOE. In the context of multi-assurance, the evaluator still considers the impact on the entire TOE, when evaluating each of the sub-TSFs.

In practice, a multi-assurance evaluation can be seen as several evaluations of the same TOE, according to different PPs. The multi-assurance evaluation adds the consistency checks that are required to ensure that these evaluations can be performed together. This means in particular that the set of SARs associated with a sub-TSF does not impact on the other sub-TSFs. Therefore, the evidence required by

the SARs of one sub-TSF cannot be negatively impacted by the SARs that have been chosen for the other sub-TSFs.

EXAMPLE Let us imagine that a PP-Configuration selects AVA_VAN.3 for one sub-TSF. ADV_TDS.3 will then be required by dependency. The evaluation of ADV_TDS.3 for this sub-TSF will, by definition, consider all the subsystems of the TOE, regardless of the ADV_TDS levels of the other sub-TSFs defined in the TOE.

The multi-assurance evaluation of a TOE which conforms with a multi-assurance ST consists in evaluating the entire TOE against the global set of SARs and evaluating each of the sub-TSFs against the corresponding sets of SARs, as defined in the ST. The order of the evaluation activities is left to the evaluator. The most suitable order depends on factors such as the actual structure of the TSF in terms of the sub-TSFs and the difference between the global set of SARs and the sets of SARs that apply to the sub-TSFs.

The limitation of multi-assurance evaluation to TOEs (and ST s) that conform with one multi-assurance PP-Configuration and the definition of the multi-assurance consistency rules in ACE allow to limit the impact on the other assurance classes. Performing a multi-assurance evaluation consists in applying a uniform interpretation of all the assurance classes, as defined in ISO/IEC 18405: in the context of a multi-assurance evaluation, whenever a SAR mentions the "TOE" it refers to the entire TOE. Whenever a SAR mentions the "TSF", it refers to the sub-TSF to which the SAR applies.

A multi-assurance ST reflects the TSF organization in sub-TSFs defined in the PP-Configuration to which the ST claims conformance. This TSF organization does not describe the organization of the TOE's implementation in subsystems and modules, but rather associates a given set of security functionalities (sub-TSF) with specific assurance requirements. It can happen that sub-TSFs are implemented by different sets of subsystems/modules, but there can also be some degree of overlap: a subsystem or module can implement functionalities belonging to two different sub-TSFs. This means that the two sets of SARs apply to the common subsystem or module (i.e. the union of the sets of SARs applies). In both cases, for each sub-TSF, all of the other sub-TSFs belong to the TOE and the corresponding subsystems/modules shall be evaluated through the prism of the requirements of the sub-TSF.

14 Composition of assurance

14.1 General

IT products are almost always composed from several components, whereby some of them are evaluated and some are not. Independent product components are often evaluated separately, and the question of composing the security assurance of the single components to determine the security assurance of the entire product arises.

EXAMPLE Software is composed with evaluated hardware to create an IT product.

Composition of assurance is dependent upon:

— the type of composition;

— the security function policies, and OSPs that the component evaluation was based on;

— the claimed security assurance, for example the assurance level;

— the overall security policies for the entire product.

Concepts of composition models are described in 14.2. Evaluation methods by which security assurance in such composition models can be provided are given in 14.3. Considerations about the re-use of evaluation results related to individual product components in the composition approach are addressed in 14.4. 14.5 addresses the relationship between composite and multi-assurance evaluation approaches.

14.2 Composition models

14.2.1 Layered composition model

In this type of composition, one component is built on top of another component, as pictured in Figure 11.

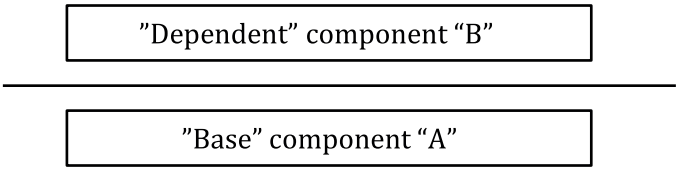

Figure 11 — Layered composition model

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

— the base component is independent from the dependent component;

— the base component is not modified by the dependent component;

— the dependent component uses the functionality of the base component and not vice versa.

Those performing such a composition should consider that:

— the dependent component can depend on other functionality than the security functionality in the scope of the evaluation of the base component;

Two examples are given to clarify the layered composition model described in Figure 11.

EXAMPLE 1 The first and main example comes from the smartcard domain, where an evaluation technique has been defined for the layered composition model. In this context, a smartcard is built up with a combination of two parts:

— a hardware integrated circuit (IC) part (as a base component);

— a software part on top of it (as a dependent component).

The software part can depend on functionality that does not belong to the evaluated security functionality of the underlying hardware. However, in general almost all instructions of the hardware are part of the hardware's security functionality and are used to implement the security functionality of the software part.

The software part of the smartcard is potentially layered itself, consisting of an

— 'Operating System' layer with possibly integrated applicative functionality (as a base component);

— 'Application' layer on top of it that contains different applications (as a dependent component).

All these parts can be developed by different actors with specific objectives.

EXAMPLE 2 Applications running on a personal computer follow the same principle, with an operating system (OS) acting as a base component and the application layer as a dependent component: the application uses Identification and Authentication provided by the OS, builds its own objects on top of the OS file system, builds its own application structure on top of the OS address space management and separation, and needs to enforce specific properties (e.g. fault tolerance, information flow control). If the OS has already been evaluated, then the security functionality of the application layer can be broken down to the evaluated security functionality of the base component. Where this is not possible, the dependent component implements the security functionality by itself. Furthermore, the dependent component can depend on functionality that does not belong to the evaluated security functionality of the underlying base component.

14.2.2 Network or bi-directional composition model

In this type of composition, a component uses the specific functionality of another component communicating via some communication channel, as pictured in Figure 12.

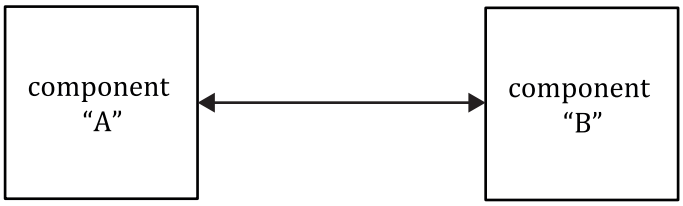

Figure 12 — Network or bi-directional composition model

The following assumptions are made in regard to the network or bi-directional composition model:

— the security interdependencies are clearly described;

— both products are separated such that there is no other channel or influence than the defined one;

— both products implement the functionality required to protect the communication channel.

EXAMPLE 1 An application (component “A”) using the functionality of an external LDAP server (component “B”).

Those performing such a composition consider that:

— security functionality might not fit together.

EXAMPLE 2 Access control can be based on different objects.

— assumptions made on a component might not be valid.

EXAMPLE 3 Assumption on the protection of critical data transferred to another component:

— security functionality can have unwanted side effects.

EXAMPLE 4 A covert channel leaking cryptographic keys.

If these kinds of issues are identified, then they should be clearly documented along with the determination of appropriate mitigating controls.

14.2.3 Embedded composition model

In this type of composition, a component is used as part of a larger component or product, as pictured in Figure 13.

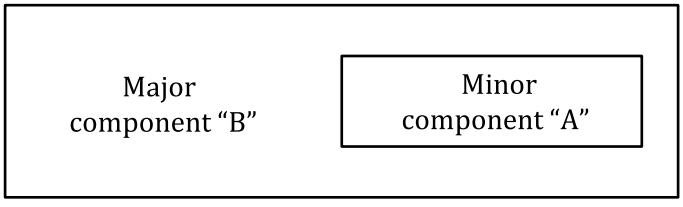

Figure 13 — Embedded composition model

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

— there is usually no separation between the components;

— each part can influence the other via channels and interfaces other than the intended ones.

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

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

— bypass the security functionality of the other components;

— modify the security functionality and security policy of other components and of the whole product;

— introduce a number of critical side effects.

NOTE If separation is specified, ADV_ARC given in ISO/IEC 15408-3 describes the criteria for evaluation.

14.3 Evaluation techniques for providing assurance in composition models

14.3.1 General

To achieve reliable and repeatable evaluation results for the evaluation of IT products (TOEs) that make use of the composition models described in 14.2, a corresponding suitably defined evaluation method is needed.

14.3.2 and 14.3.3 address evaluation techniques for the layered composition model. 14.3.2 describes how the ACO class defined in ISO/IEC 15408-3 may be used for composed TOEs, and in 14.3.3 an evaluation technique for composite products is provided which is already widely applied in the industry and shows multiple advantages (see 14.3.3.1).

The other two composition models (i.e. bi-directional and embedded) are not explicitly addressed by constructs defined in the ISO/IEC 15408 series.

14.3.2 ACO class for composed TOEs

The ACO class specified in ISO/IEC 15408-3 addresses a TOE composed of two TOEs using a layered composition model as described in 14.2, both of which have been separately evaluated. These component TOEs can be described as a base TOE and a dependent TOE, as shown in Figure 14. In such a case, the ACO class is used for evaluating the composed TOE.

An evaluation of such a composed TOE consists of evaluating the interaction between both TOEs, whereby reuse of the evaluation results from both the base TOE and the dependent TOE takes place.

ISO/IEC 15408-5 provides pre-defined CAPs that may be used for determining the composed TOE's assurance level.

The ACO class is applicable up to 'Enhanced-basic' assurance level.

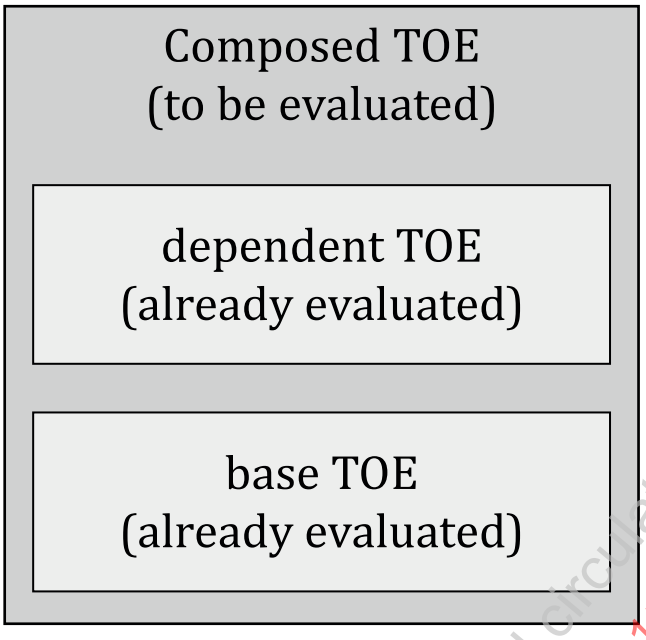

Figure 14 — Composed TOE evaluated using the ACO class

14.3.3 Composite evaluation for composite products

14.3.3.1 General

The composite evaluation technique addresses the layered composition model for composite products as described in 14.2 and is devised to meet the following objectives:

— independently perform the evaluation of a base component to address several dependent components and customers;

— create one or several dependent component(s) to use with an evaluated base component;

— install one dependent component onto an evaluated base component to reduce the evaluation effort keeping a high level of confidence.

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

The COMP related assurance families specified in ISO/IEC 15408-3 for the ADV, ALC, ASE, ATE and AVA classes provide evaluation criteria pertinent to composite products using this layered model.

14.3.3.2 Objectives

This method for composition of assurance applies to layered products that comprise one independently evaluated base component and one dependent component.

NOTE A dependent component potentially consists of one or more dependent sub-components. For simplification, they are considered as 'one dependent component' in the following.

The composite product is made of the integration of the already evaluated base component (including its base TOE) and the dependent component. Hereby, the base TOE is part of the composite TOE. In the composite evaluation approach, the evaluation results already obtained for the base TOE are reused, and the evaluation of the dependent component is performed within the evaluation of the composite product, whereby in particular focus is laid on the evaluation of the relationship between the base TOE and the dependent component. Therefore, an assurance level is claimed for and applies to the composite product as a whole and not to the dependent component only.

The composite product, with its base component (including the base TOE) and dependent component, is intended to be efficiently evaluated. The specific composite evaluation technique is set up with the objective to optimize the evaluation of such a composite product.

Unlike ACO-based evaluation, this allows a direct comparison with similar products that are evaluated at once without using composition techniques. Moreover, there is no limitation in the assurance level, i.e. the composite product can claim any pre-defined EAL or well-defined assurance package, including resistance up to 'High attack potential' as defined in ISO/IEC 15408-3 AVA_VAN.5, whereas ACO is limited by CAP requirements up to 'Enhanced-basic' attack potential. The aim is not to define an additional assurance class, but to define additional assurance requirements for a composite evaluation.

EXAMPLE Examples of smartcard devices requiring high-level assurance include payment and digital signature applications.

14.3.3.3 Design of composite product and composite TOE

The composite product is composed of one base component (including its base TOE) and one dependent component whereby in view of evaluation aspects the following rules and constraints apply for the composite product and its composite TOE part:

— the base component builds the underlying independent layer of the composite product and contains the base TOE. The base component with its base TOE shall already have been evaluated;

— the dependent component builds a supplementary layer of the composite product that is dependent on the base component and that shall be evaluated in the framework of the composite evaluation;

— the composite TOE is part of the composite product and covers the entire dependent component, and the base TOE, more detailed a superset of the base TOE functionalities is required for the correct and secure execution of the composite product;

NOTE 1 A composite TOE can contain parts that are independent from the base component / base TOE. For simplification, such parts are considered as belonging to the dependent component.

— the dependent component can rely on base component functionalities that are in the base component, but lie outside the base TOE (that is, functionalities in the non-TOE part of the base component);

— the non-TOE part of the composite product can use base component functionalities, in particular base TOE functionalities. As usual, the composite evaluation needs to determine that this non-TOE part of the composite product is non-interfering with the dependent component – neither directly nor through the usage of the base component functionalities;

— non-TOE parts of the composite product, in particular non-TOE parts of the evaluated base component (that is, parts in the base component lying outside the base TOE), are considered part of the operational environment of the composite TOE.

NOTE 2 Composite evaluation is applicable independently of the 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 3 This document only addresses cases where the level of assurance of the base component is equivalent or higher compared to the composite evaluation level.

NOTE 4 In the case where both base component and dependent component have already been evaluated using the ISO/IEC 15408 series, the composite evaluation work potentially relies on the results already obtained both from the previous base component evaluation and the previous dependent component evaluation. Nevertheless, the composite evaluation objective as defined in this document has still to be achieved.

Figure 15 illustrates the general design and layering of a composite product and composite TOE in the framework of the composite evaluation approach.

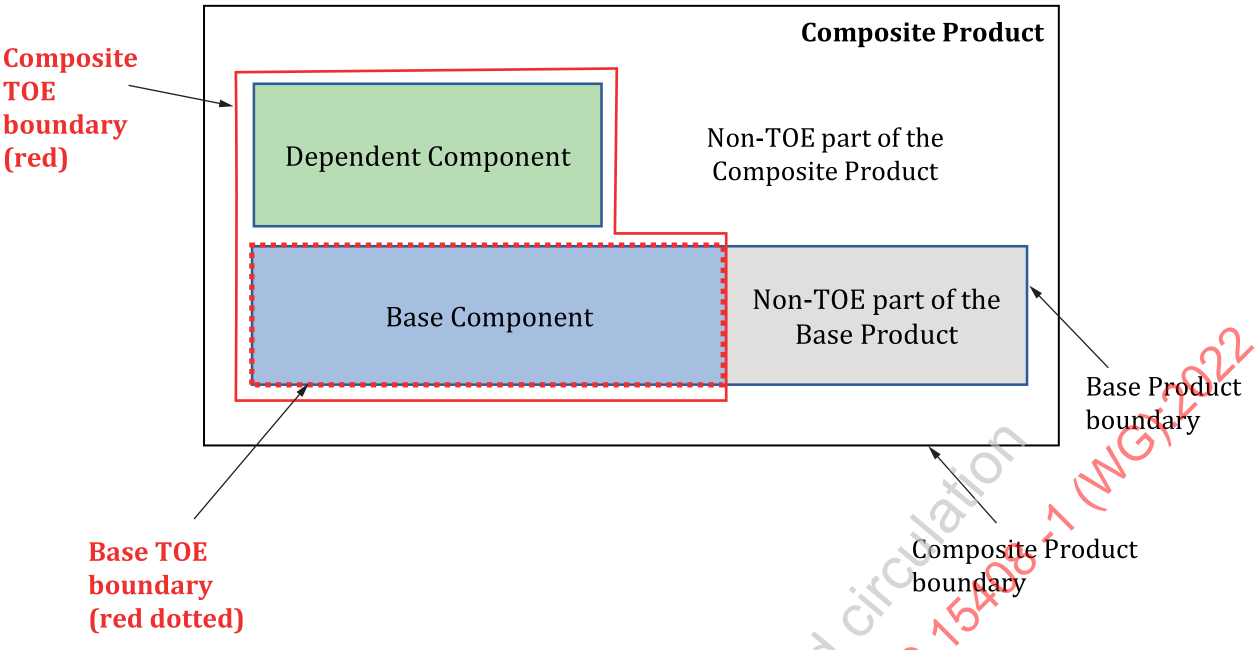

Figure 15 — Composite evaluation

Several composition steps can follow each other. In other terms, the base component can itself be a composite product consisting of an own already evaluated base component and a dependent component.

14.3.3.4 Roles

The base component and the composite product, more precisely the base TOE and the composite TOE, are both undergoing an evaluation. Therefore, both of them have a sponsor, a developer, an evaluator, and an evaluation authority.

For the composite evaluation model addressing the evaluation of the composite product, a preceding finalized evaluation of the base component with its base TOE is expected. The composite evaluation performs the evaluation of the composite product by re-using the evaluation results of the already evaluated base component. Hence, the evaluation of the composite product focuses on the evaluation of the dependent component including its relationship to the base component and hereby takes the base TOE with its related evaluation results into account.

In practice, there is no composite product developer since the composite product results from the integration of the dependent component and the base component. Instead, the relevant developer-related roles here are:

— the dependent component developer responsible for implementing the dependent component (and further non-TOE parts of the composite product, if applicable);

— the base component developer responsible for implementing the base component;

— the composite product integrator responsible for the integration of the base component and the dependent component.

In order to address this role model, the composite evaluation approach and technique defines additional evaluation activities for the above-mentioned dependent component developer, the base component developer, and the composite product integrator.

NOTE 1 As already mentioned, the dependent component can have undergone a separate evaluation, but the evaluator and evaluation authority of this previous evaluation are not considered here. If the base component and the dependent component were evaluated separately, each of them would have a sponsor, a developer, an evaluator, and an evaluation authority.

NOTE 2 As in the general cases, some actors involved can be the same. The composite evaluation context also leads to specific cases of actors having several roles. Each evaluation will associate particular organizations or persons to these generic roles.

EXAMPLE 1

— the base component developer can also be the base component sponsor;

— the base component evaluation authority can also be the composite product evaluation authority.

NOTE 3 The composite product integrator is a different role than the developer. While this integrator can, in some cases, also be one of the developers defined previously, this is not always the case.

The following example illustrates the role of the composite product integrator:

EXAMPLE 2

— native smartcards: The underlying base component is an integrated circuit and the base component developer is the integrated circuit (chip) manufacturer; the dependent component is a card operating system and its application(s) and the dependent component developer is the developer of the smartcard operating system and the application(s). In this case, the role of the composite product integrator is played by:

  — the chip manufacturer embedding the core of the operating system into the ROM of the chip, then by;

  — the card manufacturer usually loading some parts of the operating system and the applications into NV-Memories (EEPROM and/or Flash) of the chip.

— Java Card technology-enabled devices: The underlying base component is the Java Card System (Java Card Runtime Environment, Virtual Machine and APIs) on chip and the base component developer is the card manufacturer/issuer; the dependent component is a Java Card applet, which can be developed by an applet developer playing the role of the dependent component developer. In this case, the composite product integrator role can be played by the domain/application service provider or by a trust centre loading the applet and often personalizing the card electronically.

14.3.3.5 Action elements and required information

To allow the evaluation of a composite product, the composite evaluation technique identifies two main sets of issues, leading to the following rules:

— the composite product can be insecure due to gaps in the definition, integration or test of the base component and dependent component security mechanisms. In particular, the following properties are to be enforced:

  — the assets to be protected are the final composite product assets defined in a dedicated composite product ST;

  — the security mechanisms involved in the protection of these assets are those provided by the base component and by the dependent component;

  — some of the security mechanisms and security services provided by the base component may require configuration, programming, or activation as allowed for the base TOE by the dependent component;

  — evaluation is performed and validated on the final composite product.

To this effect, the composite evaluation technique defines specific action elements to be performed by the actors involved in the evaluation of the base component, as well as in the development of the dependent component and in the evaluation of the composite product.

— the aforementioned action elements are potentially impossible to perform due to a lack of information sharing between actors. To avoid this, the composite evaluation technique explicitly defines which information is required for each action element.

Table 2 and Table 3 define which SARs shall be selected in the composite product ST, and the information that is required to be available for the dependent component developer, the composite product evaluator and the composite product evaluation authority to allow and support a composite evaluation.

Table 2 — Information to be provided to the dependent component developer

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	ST of the base component. Information to build the composite product ST and to ensure consistency of the security definition between the base component and dependent component. Information related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer
Composite design compliance (ADV_COMP)	Information (usually in the form of a guidance or user's manual) related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer

Potentially, the composite product evaluator does not need all the detailed results of the base component evaluation for performing a composite evaluation of a composite product that integrates such evaluated base component. However, for reusing the base component evaluation results the composite product evaluator needs complementary information on the assurance measures where the base component and the dependent component interfere. In particular, for the examination that the dependent component meets the security requirements imposed by the base component and for the vulnerability analysis of the composite product, the composite product evaluator makes use of the evaluated base component's user guidance, the related report of the base component evaluation authority (i.e. the report for an evaluated product that confirms the acceptance of the evaluation results provided by the evaluator) and the so-called *ETR for composite evaluation* (ETR_COMP) described in 14.3.3.6.

All in all, for making use of the composite evaluation technique, in addition to the standard amount of information required by the assurance package chosen for the composite evaluation (e.g. an EAL), the following is needed as outlined in Table 3.

Table 3 — Information to be provided to the composite product evaluator and composite product evaluation authority

SAR defining the action elements	Information required	Originator of the information
Consistency of composite product Security Target (ASE_COMP)	ST of the base component. Information related to the composite product ST for ensuring consistency of the security definition between the base component and dependent component. Information related to the base component's security mechanisms and security services that the dependent component has to manage or use.	Base component developer
	ST of the composite product (including information on the compatibility of the ST of the composite product with the ST of the base component).	Dependent component developer

Table 3 *(continued)*

SAR defining the action elements	Information required	Originator of the information
Integration of composition parts and consistency check of delivery procedures (ALC_COMP)	Composite configuration evidence. Organizational evidence of version correctness, on the basis of configuration lists containing unambiguous version information of the evaluated base component and the dependent component having been integrated into the final composite product. Evidence elements that security measures prescribed by the base component developer and the dependent component developer are actually being applied by the composite product integrator.	Composite product integrator
	Delivery and acceptance procedures evidence. Information on the compliance of the delivery procedures of the base component developer and the dependent component developer with the acceptance procedure of the composite product integrator. Organizational evidence that components (dependent component and base component) transmitted from an actor to another are securely received, accepted and parameterized.	Composite product integrator Base component developer Dependent component developer
Composite design compliance (ADV_COMP)	Base component-related integration requirements and recommendations, typically including the user guidance.	Base component developer
	ETR for composite evaluation. Base component-related integration requirements and recommendations.	Base component evaluator
	Design compliance evidence. Evidence that the composite product meets the base component-related integration requirements and recommendations. It enfolds evidence elements on how the requirements on the dependent component design, imposed by the base component's user guidance and report of the base component evaluation authority are fulfilled in the composite product. If such a requirement was not followed, a rationale that the chosen composite product implementation is still secure shall be given here.	Composite product integrator Dependent component developer
	Report for the base component evaluation generated by the base component evaluation authority. (Additional) Base component-related integration requirements and recommendations.	Base component evaluation authority
Composite functional testing (ATE_COMP)	Composite product samples suitable for testing.	Composite product integrator

Table 3 *(continued)*

SAR defining the action elements	Information required	Originator of the information
Composite vulnerability assessment (AVA_COMP)	*ETR for composite evaluation.* Evidence allowing the composite product evaluator and the respective evaluation authority to understand the attack paths and the tests that have been considered and performed for the base component and the effectiveness of the countermeasures implemented by the base component, and explanations related to residual vulnerabilities of the base component linked to integration recommendations included in the base component user guidance.	Base component evaluator
	Report for the base component evaluation generated by the base component evaluation authority. (Additional) Base component-related integration requirements and recommendations, obligations, information on vulnerabilities.	Base component evaluation authority
	The base component-related user guidance.	Base component developer

NOTE The report for the base component evaluation generated by the base component evaluation authority can also be relevant for the SARs ASE_COMP, ALC_COMP and ATE_COMP even if not directly addressed in Table 3.

In the case of composition, the term 'developer' needs further clarification in order to distinguish the actors. Here, the base component developer, the dependent component developer and the composite product integrator can be different entities. Similarly, for the terms 'evaluator' and 'evaluation authority (evaluation scheme)' further distinguishing of the different entities involved needs to be made.

In the case where both base component and dependent component have already been evaluated, a reduced amount of evaluation activities is possibly sufficient to be performed considering the evaluation results already obtained from the previous dependent component evaluation. Nevertheless, the composite evaluation tasks as defined in this document are still required.

EXAMPLE Smartcard.

The smartcard architecture is composed of a hardware platform and a software application on top of the platform. In this case, the platform is the base component, and the application is the dependent component. In a composite evaluation, the platform is already evaluated, the application is evaluated as part of the composite evaluation and the results of the platform evaluation are re-used.

The hardware platform provides functionality supporting the protection of the composite product's assets, but the composite product behaviour depends on the software application having to use, configure, and activate the security functionality.

Therefore, the hardware platform evaluation results usually provide specific security recommendations and conditions for the software application implementation. The composite evaluation includes examination that the combination of both components does not lead to any exploitable vulnerability.

A composite evaluation method and associated evaluation activities are provided that include precise work units with clear statements on the information required from the platform developer and provide an agreed 'framework' for information transfer from the platform evaluator to the composite product evaluator.

The information required is already available from the platform evaluation tasks and no additional work is required from the platform developer.

There are no further requirements for the development class ADV.

The user guidance (AGD) of the platform is considered early in the development of the composite product and provides all of the interfaces on which information is needed.

The development and the evaluation of the composite product rely on the proper implementation of the evaluated interfaces of the platform.

The proper use of all relevant interfaces between the platform and the application is in the scope of the composite evaluation.

Test (ATE) and vulnerability assessment (AVA) are performed on the composite product taking advantage of the available platform evaluation results.

14.3.3.6 ETR for composite evaluation (ETR_COMP)

14.3.3.6.1 Objective of the document

The *ETR for composite evaluation* (ETR_COMP) document is compiled from the Evaluation Technical Report (ETR) related to a base component and its evaluation in order to provide sufficient information for a composite evaluation with such an already evaluated base component.

NOTE 1 A standard ETR usually contains proprietary information on the base component and its evaluation that cannot be made public. Such full ETR is therefore possibly not suitable for external delivery. The information that is presented in the ETR_COMP document contains a meaningful subset of the information provided in the full ETR of the base component for support of a composite evaluation.

The goal of the ETR_COMP document is to enable the composite product evaluator and the composite product evaluation authority to understand the attack paths and the tests that have been considered and performed for the base component and the effectiveness of the countermeasures implemented by the base component.

NOTE 2 The content of the ETR_COMP document strikes the right balance between protecting the proprietary information of the base component developer and/or the base component evaluator on the one hand and providing sufficient information for the composite product evaluator and the composite product evaluation authority on the other hand.

14.3.3.6.2 Procedure

The ETR_COMP is produced by the base component evaluator on the basis of the base component evaluation results and is derived from the full ETR related to the base component evaluation.

The ETR_COMP is part of the base component evaluation. The ETR_COMP is provided and validated on request of the sponsor of the base component evaluation. The report of the base component evaluation authority for the base component in particular declares the acceptance of the ETR_COMP by all parties involved in the base component evaluation (i.e. the base component evaluator, the base component evaluation authority, the base component developer and the sponsor of the base component evaluation). Such validation statement for the ETR_COMP especially covers the consistency of the ETR_COMP with the original ETR. The ETR_COMP is referenced in the report of the base component evaluation authority for the base component for further re-use.

For re-use of the ETR_COMP in a composite evaluation, the previous acceptance of the ETR_COMP by the base component evaluation authority in the framework of the base component evaluation is required. The ETR_COMP is supplied to the composite product evaluator and the composite product evaluation authority for use in the composite evaluation.

For the ETR_COMP, as being part of the base component evaluation, it is ensured by the base component evaluator and the base component evaluation authority that sufficient information is provided in the ETR_COMP considering the composite evaluation approach and the intended secure use of the base component in composite products.

In the case that security issues for the base component are found after acceptance of the ETR_COMP that are not sufficiently addressed in the ETR_COMP, then the base component evaluation authority decides about the actions to take. This may include an appropriate update of the ETR_COMP and a subsequent validation of this updated ETR_COMP.

Furthermore, as part of the base component evaluation the base component evaluator ensures that the recommendations for the base component in the related ETR_COMP are consistent and complete regarding the requirements provided in the base component's user guidance. If any inconsistencies

(including missing requirements) are found which are not solved before issuance of the evaluation authority's report for the base component, then the base component evaluation authority can add supplementary information for the dependent component developer in the evaluation authority's report for the base component.

In a composite evaluation, if the current base component itself relies on a previous composite evaluation, and if there is a direct interface between the dependent component of the current evaluation and the previous base component, then the ETR_COMP of the previous composite evaluation is also supplied to the current composite product evaluator and composite product evaluation authority.

14.3.3.6.3 Exchange of the ETR for composite evaluation

The ETR_COMP document is created and maintained by the base component evaluator. However, for a composite evaluation the base component developer is the point of contact for the dependent component developer.

The dependent component developer contacts the base component developer for delivery of the ETR_COMP to the point of contact at the composite product evaluator. The base component developer checks its confidentiality management rules to determine whether delivery is possible. If necessary, the base component developer contacts the base component evaluation authority about the intent of the delivery of the ETR_COMP.

The base component developer contacts the base component evaluator to request the delivery (using a secure method and distributing only marked versions) of the ETR_COMP to the given contact point of the composite product evaluator. If the delivery is granted, either the base component evaluator or the base component developer sends the ETR_COMP to the composite product evaluator depending on the agreements between these two parties. The ETR_COMP delivery process depends on the (usually contractual) agreement between the base component developer and the base component evaluator, which may lead to deviations from the described procedure. The ETR_COMP document is delivered also to the composite product evaluation authority using the similar exchange procedure as for its provisioning to the composite product evaluator.

If necessary, the base component evaluator and the composite product evaluator exchange additional or more detailed information. This is always under the control of the base component developer. In case of clarification the base component evaluator and the composite product evaluator are the main parties. If an additional assurance statement is required, then the base component evaluation authority is also involved in the exchange.

It is important that multi-party exchange of information considers all the identified controls for information exchange and protection.

14.3.3.6.4 Content of the ETR for composite evaluation

The information required to be provided in the ETR_COMP document includes:

a) information about the evaluated base component;

This section of the ETR_COMP shall provide formal information on the base component evaluation including:

— version information of the ETR_COMP;

— base component unambiguous identification;

— base component developer and sponsor identities;

— identities of the base component evaluator and the base component evaluation authority;

— assurance level of the base component evaluation;

— formal evaluation results such as pass/fail;

— reference to the ETR related to the base component and its evaluation.

b) information about the base component design:

This section of the ETR_COMP shall provide a high-level description of the base component and its major components based on the deliverables required by the assurance class ADV.

The intent of this section is to characterize the degree of architectural separation of the major components of the base component, to show possible technical dependencies between the base component and a dependent component using this base component, and to outline the security mechanisms of the base component covered by the base component evaluation.

c) information about the evaluated configuration of the base component:

This section of the ETR_COMP shall provide information about the evaluated configuration of the base component established on the developer's configuration list or relevant parts as needed or on a case by case basis. The base component shall unambiguously be identifiable, and this identification shall be linked to the evaluated configuration as stated in the report of the base component evaluation authority for the base component.

If applicable, generation and installation parameter settings which are security relevant for the base component shall be explained and their effect on the defence against attacks shall be outlined (for example key length, counter limits). This shall include methods for the dependent component developer and the dependent component evaluator to verify the values of these settings, in order to ensure that the expected evaluated configuration is used.

This evidence can include installation, generation and start-up procedures of the base component as outlined in the related user guidance to ensure that the base component is configured in a secure manner.

d) information on delivery procedures, the development and production sites involved and data exchange:

For supporting composite evaluation, both evaluation evidence for delivery procedures of the base component and for acceptance procedures of the dependent component, and related data to be integrated during development and production are necessary.

The ETR_COMP shall provide an overview of the sites involved in the development and production of the base component, including the role of each site and the date of the latest audit.

e) information about the penetration testing of the base component including the considered attack paths and summary of test results; information about the penetration testing of the supporting functions in the base component:

This section of the ETR_COMP shall provide information about the independent vulnerability analysis performed for the base component by the base component evaluator with the considered attack scenarios, the performed penetration testing and the reference to the corresponding rating (quotation) of the attack potential.

The information about the penetration testing shall include:

— a summary showing all of the attack methods that have been addressed during the vulnerability analysis,

— the details necessary for understanding the attack scenarios/paths that were considered,

— the assessments of the penetration tests performed and their results.

The attack scenario descriptions shall provide sufficient details to support the composite product evaluator in reproducing attacks, which require additional countermeasures in the composite product.

If a potential vulnerability of the base component has to be resolved by adhering to the base component guidance this shall be clearly outlined in the summary including a reference to a specific section in the guidance or if possible, a guidance element.

f) Observations and recommendations:

The evaluated base component user guidance shall contain all information required to use the base component in a secure way as defined in the base component ST, in particular including information on how to avoid residual vulnerabilities and unexpected behaviour. The base component evaluator shall ensure that the ETR_COMP only contains recommendations on the secure use of the base component that are also addressed as requirements in the base component user guidance. The base component evaluator shall ensure that the base component user guidance and the recommendations in the ETR_COMP are consistent and that the user guidance requirements are sufficiently specific to enable the dependent component developer to perform design compliance analysis.

However, in some cases additional detailed information beyond the base component guidance can be necessary for allowing the composite product evaluator to perform the composite evaluation such as:

— observations on the base component evaluation results (e.g. specific base component configuration for the base component evaluation);

— recommendations/stipulations for the composite product evaluator: specific information on the use of the base component evaluation results (e.g. about specific testing necessary during a composite evaluation).

Any such observation or recommendation/stipulation comes from the base component evaluator and/or the base component evaluation authority.

The ETR_COMP document is not intended to reproduce information (e.g. text copies) from other available base component evidence such as the ST and guidance. However, the composite evaluation is supported by references to the relevant sections of such base component evidence.

14.3.3.7 Reports and their validity

The results of a composite evaluation are provided to the composite product evaluation authority in the form of an ETR for the composite product. This composite product ETR shall contain, amongst other information, the final overall verdict for the composite evaluation based on the partial verdicts for each assurance component being in scope of the current composite evaluation. The usage of the composite evaluation approach shall be addressed in the composite product ETR and if applicable, in the composite product's report of the composite product evaluation authority.

As the composite product and its composite evaluation cover the base component and its related evaluation, the composite evaluation is linked to the validity and topicality of the report of the base component evaluation authority for the base component. The composite product evaluator and the composite product evaluation authority need a valid and up-to-date report of the base component evaluation authority for the base component or at a minimum the assessment of the base component evaluation authority on the status of the evaluation authority's report in question.

NOTE 1 The composite product evaluation authority generally asks for a re-assessment of the base component if the base component's ETR_COMP is not valid or not up-to-date, and therefore not suitable for re-use in the composite evaluation, in particular because of its (obsolete or insufficient) vulnerability analysis and penetration testing. This re-assessment consists of a re-evaluation of the base component focusing on a renewal of the vulnerability analysis and penetration testing (surveillance process) or as an alternative, of a confirmation statement of the base component evaluation authority.

NOTE 2 If the base component's ETR_COMP was issued before the submission of the related composite evaluation tasks and in the meantime a major change in performing state-of-the-art relevant attacks on the base component arose (e.g. a major change in the attack methods or attack ratings) then the composite product evaluation authority potentially requires a re-assessment or re-evaluation of the base component focusing in particular on the new attack issues.

NOTE 3 Rules determining the validity and topicality of reports (here in particular the base component-related report of the base component evaluation authority and the ETR_COMP) are defined by the respective evaluation scheme and can be linked to a specifically defined validity period.

NOTE 4 If the composite product evaluator detects any failures resulting from the testing of the base component (e.g. vulnerabilities due to improved attack methods or techniques), these results are communicated to the composite product evaluation authority. The composite product evaluation authority then takes appropriate steps together with the base component evaluation authority, e.g. to invoke a re-assessment or re-evaluation of the base component.

In the case that the entire composite product is set up as a chain of composite products constructed on top of each other (e.g. the base component itself is already a composite product) the validity and up-to-date aspect of each ETR_COMP and evaluation authority report used in this chain of composite products is necessary. In addition, all dependencies from a lower level ETR_COMP to a higher level ETR_COMP are in consideration when re-using the results in the composite evaluation of the entire composite product.

NOTE 5 The evaluation authority report for a product declares the acceptance of the product's evaluation and its results by the respective evaluation authority (i.e. acceptance of the related ETR by the evaluation authority is given). In particular, such report declares that the evaluation of the product was carried out according to ISO/IEC 15408.

The validity, topicality and relevance of the base component's report of the base component evaluation authority and of the ETR_COMP for the current composite product and its composite evaluation are acknowledged by the report of the composite product evaluation authority for the composite product. This includes the determination and acceptance of equivalence of single assurance components (and, hence, of assurance levels) belonging to different ISO/IEC 15408 and ISO/IEC 18405 versions, if the base component evaluation was performed in conformance to another version of ISO/IEC 15408 and ISO/IEC 18045 than the current composite evaluation.

The composite product evaluation authority issues a report for the composite product, if:

— the final overall verdict for the composite evaluation in the composite product ETR is "PASS", and

— the validity, topicality and relevance of the base component's report of the base component evaluation authority and the ETR_COMP are acknowledged for the present composite product and its composite evaluation by the composite product evaluation authority.

14.4 Requirements for evaluations using composition techniques

14.4.1 Re-use of evaluation results

When composing components into an IT product, it is possible that single components of the product have already been evaluated and that therefore already existing evaluation results for such components can be re-used. However, additional evaluation activities are usually required and performed to confirm the security assurance of the entire IT product.

The re-use of evaluation results and evidence related to such components of the IT product (TOE) require their availability for the evaluation of the entire IT product (TOE).

14.3.2 and 14.3.3 address evaluation techniques for the layered composition model. 14.3.2 describes the usage of the ACO class defined in ISO/IEC 15408-3 for composed TOEs, and in 14.3.3 an evaluation technique for composite products is provided.

The re-use of evaluation results and evidence of components of the IT product (TOE) is dependent upon:

— the composition model used for the IT product (TOE);

— the security assurance to be claimed for the entire IT product (TOE), in particular in relationship to its components and their security assurance;

— the security properties claimed for the IT product (TOE) and its components.

EXAMPLE Separation, Information Flow Control and Fault tolerance are examples of security properties.

14.4.2 Composition evaluation issues

14.4.2.1 Composition rationale

When composing an IT product (TOE) from components using a composition model as described in 14.2 and using composition techniques for its evaluation, a composition rationale shall be provided for the evaluation of the IT product (e.g. in the ST of the composite/composed product). This includes analysis of at least:

— the composition model used for the IT product (TOE);

— the security assurance to be claimed for the entire TOE, in particular in relationship to its components and their security assurance;

— the interfaces and dependencies of the components and their functionality;

— the composability of the security function policies and OSPs of the components;

— the preservation of security properties of the components;

— for the embedded composition model, aspects of correctness.

14.4.2.2 Vulnerability analysis

The IT product composed from components using a composition model as described in 14.2 and using composition techniques for its evaluation shall undergo a vulnerability analysis, in accordance with the AVA class given in ISO/IEC 15408-3 taking the proposed EAL for the IT product into account. Although it is possible to re-use the vulnerability analysis results from the components additional vulnerability analysis activities for the entire IT product (TOE) shall be designed and performed.

The vulnerability analysis shall be designed in consideration of the analysis of the IT product with its components.

14.4.2.3 Testing

The IT product composed from components using a composition model as described in 14.2 and using composition techniques for its evaluation shall undergo additional testing, using the ATE class given in ISO/IEC 15408-3. Although it is possible to re-use the testing evaluation results from the components additional tests for the entire IT product (TOE) shall be designed and performed.

The testing shall be designed in consideration of the analysis of the IT product and its components.

14.4.2.4 Use of the ACO class for composed TOEs

ISO/IEC 15408-3 describes the ACO class which provides security assurance components that are intended to be used in support of the evaluation of composed TOEs.

ISO/IEC 15408-5 provides a family of pre-defined assurance packages for composed TOEs [composed assurance packages (CAP)] which balance the level of assurance obtained with the cost and feasibility of acquiring such assurance for composed TOEs.

The CAPs are designed to provide assurance that the composition was performed correctly, to a specified rigour, and in consideration of the proposed EAL for the composed IT product.

14.4.2.5 Use of the composite evaluation technique for composite products

ISO/IEC 15408-3 describes the COMP families in different assurance classes, which provide security assurance components that are intended to be used in support of the evaluation of composite products.

These COMP families are set up as assurance families that appropriately supplement other already existing assurance families defined in ISO/IEC 15408-3 in order to address the composite-specific evaluation aspects and issues.

The COMP families are designed to provide assurance that the composition was performed correctly, to a specified rigour, and in consideration of the proposed EAL for the composite product.

Use of the composite evaluation technique for the evaluation of a composite product requires an already evaluated base component accompanied by a corresponding ETR_COMP and a valid report of the base component evaluation authority.

14.5 Evaluation by composition and multi-assurance

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

Evaluation by composition addresses TOEs with a supply and/or integration chain that potentially involves multiple parties, where each party takes care of the evaluation of the security functionality they develop. The ISO/IEC 15408 series standardizes two approaches for the reuse of evaluation results in an evaluation process:

a) composed evaluation allows to obtain a composed assurance level for a TOE from the individual assurance levels of its interacting sub-TOEs;

b) composite evaluation allows to obtain an EAL for a layered TOE, in an incremental way where the base layer is evaluated first, then the integrated dependent and base layers are evaluated by reusing the evaluation results of the base layer.

Multi-assurance evaluation focuses on TOEs where different assurance needs apply to different parts of the security functionality (the sub-TSFs) while ensuring a global assurance level for the entire TOE. Before the introduction of multi-assurance, such needs would have forced a sponsor to undergo several evaluations of the same TOE for different STs. Using this concept, the ISO/IEC 15408 series standardizes and optimizes this process.

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

In practice, multi-assurance and evaluation by composition can be used together in an evaluation.

Annex A
(normative)

Specification of packages

A.1 Goal and structure of this annex

The goal of this annex is to give further information about the specification of packages.

NOTE ISO/IEC 15408-3 does not define evaluation criteria for packages since packages are not separately evaluated. Evaluation of packages is implicit once a package is incorporated into a PP, PP-Module or ST.

A.2 Package families

A.2.1 General

Figure A.1 shows the structure of a package family. Each part is discussed below.

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 endeavours 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 the ISO/IEC 15408 series that is used.

The package may also be given a short name.

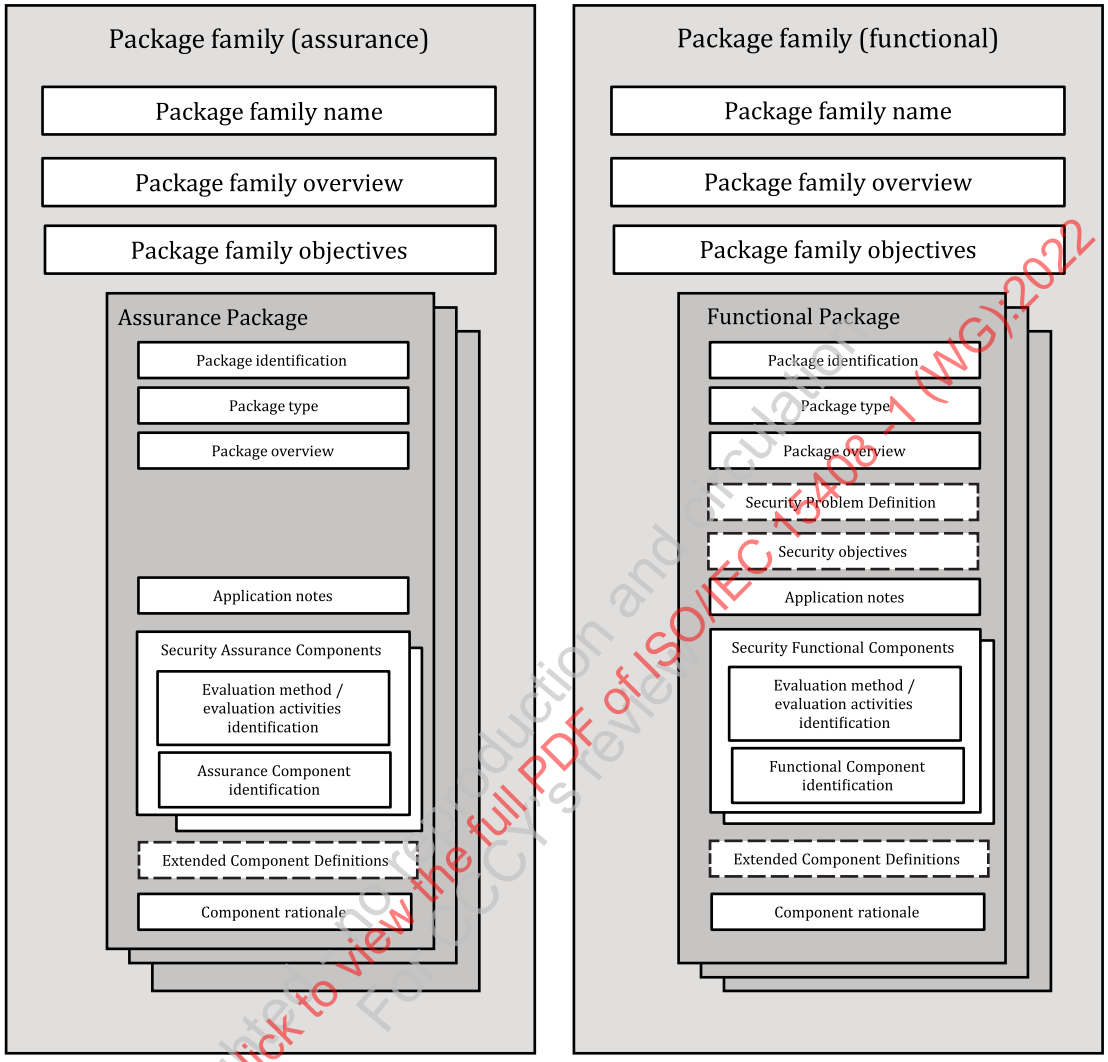

Figure A.1 — Structure of a package family with assurance or functional packages

EXAMPLE Evaluation Assurance Level 1 is also known as “EAL 1”.

NOTE For those packages defined in ISO/IEC 15408-5, items b) to e) are implicit in the edition information of ISO/IEC 15408-5.

A.3.1.2 Package type

A package is identified as one of the following types:

a) Functional package; or

b) Assurance package.

A.3.1.3 Package overview

Packages contain a section giving a high-level overview and the intent of the package.

A.3.1.4 Application notes

Application notes are optional with the following exceptions:

— for functional packages, any additional audit and management requirements relating to the SFRs included in the package shall be specified in the Application notes section;

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

Functional packages may also specify components that have dependencies that are not satisfied by the package, but are expected to be satisfied by another package, PP, PP-Module, or ST that uses the package.

EXAMPLE A package that contains the specification for a cryptographic protocol (e.g. TLS), where the higher-level SFR components are specified in the package, but the cryptographic primitives are not.

In this case an optional list of the dependent components may be provided in the application notes section of the functional package and may include further information such as any required selections/assignments for those SFRs.

NOTE Users of packages include authors of PPs, PP-Modules, other packages and STs, integrators, and evaluators.

A.3.1.5 Components (either SFRs or SARs)

The security requirements included in the package are given. This section also provides the rationale for the selection of the requirements.

The security requirements may be selection-based. See 8.2.4.2. Optional SFRs (and supporting SPD-elements and objectives, as required) are also allowed to be specified in functional packages.

A.3.2 Optional contents of a package

A.3.2.1 Security problem definition (SPD) (Functional Packages)

Assurance packages do not contain this section.

Functional packages may include this section.

This section includes any SPD-elements which describe the security problem addressed by the functional package. SPD-elements associated with optional SFRs may be defined in this section. Application notes shall be used to identify the security objectives (if applicable) and SFRs to which the optional SPD-elements are associated.

A.3.2.2 Security objectives (Functional Packages)

Assurance packages shall not contain this section.

Functional packages may include this section.

In the case of a functional package used for Direct Rationale PPs/PP-Modules/STs TOE security objectives shall not be included.

The security objectives section of a functional package presents any additional TOE security objectives or security objectives for the operational environment derived from the SPD. Security objectives for the TOE associated with optional SFRs may be defined in this section, if applicable. Application notes shall be used to identify the SPD-elements and SFRs to which the optional security objectives are associated.

A.3.2.3 Application notes

The inclusion of application notes in a package is optional. See A.3.1.4.

The application notes section may also contain information of particular interest to users of the package. The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention is needed.

A.3.2.4 Extended components definition(s)

A package may contain extended components. In this case, packages contain a section giving the extended component definitions.

A.3.2.5 Evaluation methods/activities

Packages may include evaluation methods/ activities that have been derived from ISO/IEC 18045. Where evaluation methods / activities are included, a conformance statement or statements shall be included in the security requirements section of the package, see 9.4. Evaluation methods/ activities may be provided either in the package document or may reference external documents.

Annex B
(normative)

Specification of Protection Profiles (PPs)

B.1 Goal and structure of this annex

The goal of this annex is to summarize the structure and expected content of a PP.

NOTE 1 This annex does not define the requirements for evaluation of PPs. The PP evaluation criteria are found in the APE class given in ISO/IEC 15408-3.

NOTE 2 This annex does not give the requirements for the specification of PP-Configurations and PP-Modules. These are found in Annex C.

This annex consists of the following major parts:

a) *the specification of a PP*

This is summarized in B.2. and includes:

— *how to use a PP;*

— *how not to use a PP.*

b) *what a PP shall contain*

This is summarized in B.3 and is described in more detail in B.3.2 to B.3.7 that describe the mandatory contents of the PP, the interrelationships between these contents, and provide examples.

c) *claiming conformance with standards*

B.4 describes how a PP author can claim that the TOE is to meet a particular standard.

d) *Direct Rationale PPs*

Direct Rationale PPs are PPs in which the threats and OSPs in the SPD are mapped directly to the SFRs and possibly to security objectives for the operational environment. They are described in detail in B.5.

B.2 Specification of a PP

B.2.1 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.

Although this does not preclude other uses, a PP is 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.

B.2.2 How not to use a PP

Two roles, among many, that a PP does not fulfil are:

— a complete specification;

A PP is designed to be a security specification and not a general specification. Unless security-relevant, properties such as interoperability, physical size, and weight, required voltage etc. should not be part of a PP. This means that in general a PP is a part of a complete specification, but not a complete specification itself.

— A specification of a single product.

Unlike a ST, a PP is designed to describe a certain type of IT product, and not a single product. When only a single product is described, it is better to use a ST for this purpose.

B.3 Mandatory contents of a PP

B.3.1 General

There are two types of PP. Firstly, the "regular" PP which is a PP that contains the full contents as described in in B.3.2 to B.3.7. Secondly, in some cases a PP author can write a Direct Rationale PP which has different contents compared to PPs that contain security objectives for the TOE. Direct Rationale PPs, and the reasons and circumstances in which they are used are described in detail in B.5. All other parts of this annex assume a PP with full contents.

Figure B.1 shows the content for a PP that is given in ISO/IEC 15408-3. Figure B.1 may also be used as a structural outline of the PP, though alternative structures are allowed. For instance, if the security requirements rationale is particularly bulky, it can be included in an appendix of the PP instead of in the security requirements section. The separate sections of a PP and the contents of those sections are briefly summarized below and explained in much more detail in B.3.2 to B.3.7.

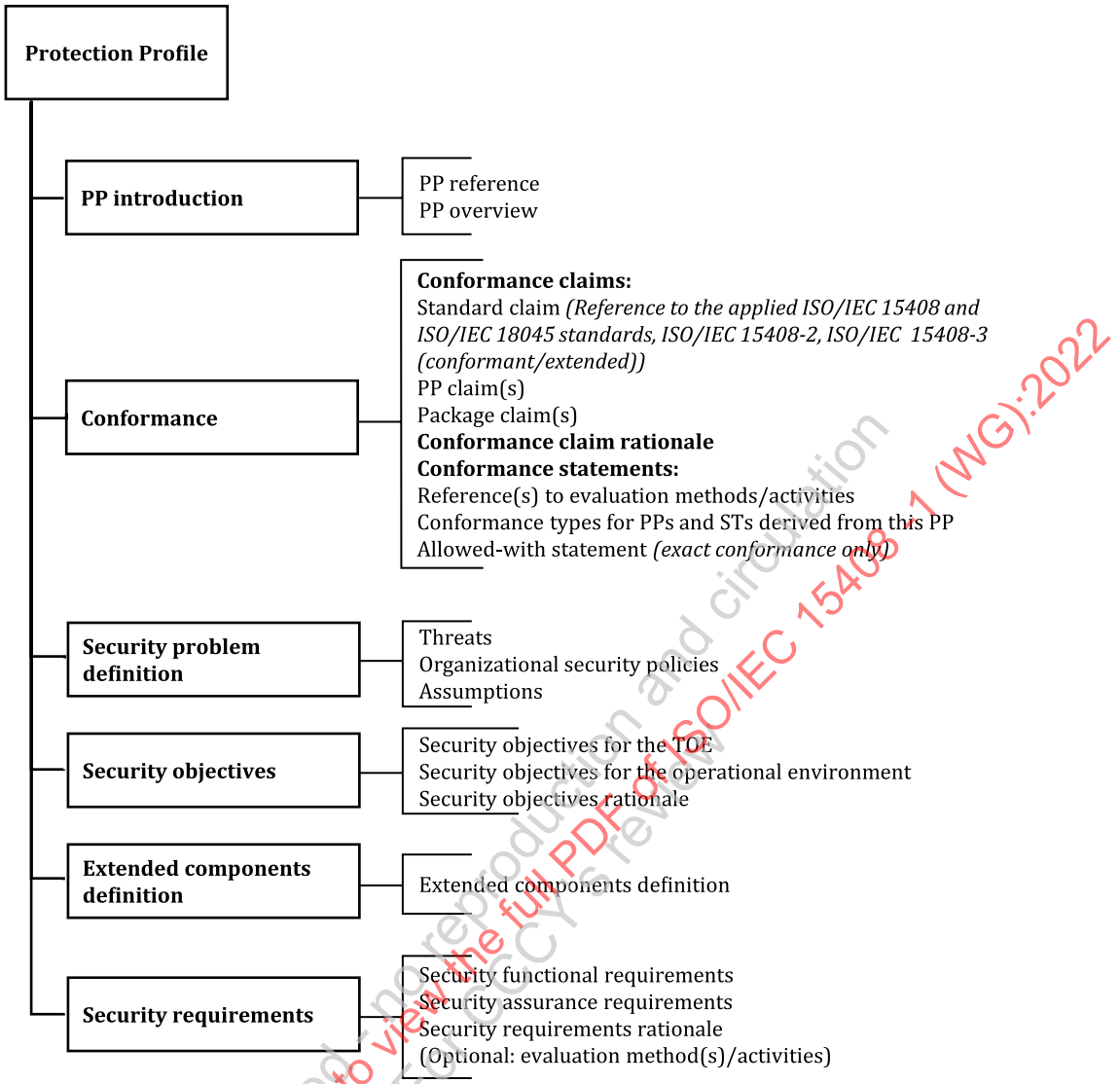

Figure B.1 — Contents of a Protection Profile

A PP contains:

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

b) *conformance claims*, showing:

- which edition of relevant parts of the ISO/IEC 15408 series is applicable;
- conformance to ISO/IEC 15408-2 and ISO/IEC 15408-3 (conformant or extended);
- whether the PP claims conformance to any other PPs and/or packages, and if so, to which ones and the type of conformance claimed.

c) *A conformance statement, containing*:

- reference to any evaluation method(s) and/or activities that have been derived from ISO/IEC 18045;

  NOTE Detail of any evaluation methods/activities can optionally be included in the PP, or in an associated supporting document.

— in the case of exact conformance, the allowed-with statement, indicating the PPs and PP-Modules that can be used in conjunction with the PP, appears in this section of the PP.

— the type of conformance demanded of STs and other PPs derived from it.

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(s)*, 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;

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.

B.3.2 PP introduction (APE_INT)

B.3.2.1 General

The PP introduction describes the TOE in a narrative way on two levels of abstraction:

a) the PP reference, which provides identification material for the PP;

b) the TOE overview, which briefly describes the TOE.

B.3.2.2 PP reference

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

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

EXAMPLE An example of a PP reference is “Atlantean Navy CablePhone Encryptor PP, version 2b, Atlantean Navy Procurement Office, April 1, 2020”.

The reference should be unique so that it is possible to tell different PPs and different versions of the same PP apart. The PP reference facilitates indexing and referencing the PP and its inclusion in PP catalogues.

B.3.2.3 PP overview

B.3.2.3.1 General

The PP overview is aimed at potential consumers of a TOE type who are looking through catalogues of PPs that can support the specification of their security needs.

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

The typical length of a PP overview is several paragraphs.

To this end, the PP overview briefly describes the usage of the TOE and its major security features, identifies the TOE type, and identifies any major non-TOE hardware/software/firmware available to the TOE.

B.3.2.3.2 Usage and major security features of a TOE type

The description of the usage and major security features of the TOE type is intended to give a very general idea of what the TOE is capable of, and what it can be used for. This section is written for PP authors, TOE developers, or potential TOE consumers, describing TOE type usage and major security features in terms of business operations, using language that TOE consumers can understand.

EXAMPLE An example of this is "The Atlantean Navy CablePhone Encryptor is an encryption device that allows confidential communication between ships across the Atlantean Navy CablePhone system. To this end it allows at least 1024 different users and support at least 500 Mb/s encryption speed. It allows both bilateral communication between ships and broadcast across the entire network."

B.3.2.3.3 TOE type

The TOE overview identifies the general type of a TOE addressed by the PP, such as: firewall, VPN-firewall, smart card, crypto-modem, intranet, web server, database, web server, mobile device, and database, etc. The TOE type definition often includes a characterization of the TOE software and hardware boundaries.

EXAMPLE This example of TOE type description is drawn from the Security IC Protection Profile: "The Target of Evaluation (TOE) is a security integrated circuit (security IC) which is composed of a processing unit, security components, I/O ports (contact, contactless, or similar interfaces like USB, MMC) and volatile and non-volatile memories (hardware). The TOE can also include IC Developer/Manufacturer proprietary IC Dedicated Software as long as it is delivered by the IC Manufacturer. (...) All other software running on the Security IC is called Security IC Embedded Software and is not part of the TOE."

B.3.2.3.4 Available non-TOE hardware/software/firmware

While some TOEs do not rely upon other IT, many TOEs, notably software TOEs, rely on additional, non-TOE, hardware, software and/or firmware. In the latter case, the PP overview is required to identify the non-TOE hardware/software/firmware.

As a PP is not written for a specific product, in many cases only a general idea can be given of the available hardware/software/firmware. In some other cases, more specific information can be provided.

EXAMPLE 1 An example where more specific information is provided would be a requirements specification for a specific consumer where the platform is already known.

EXAMPLE 2 Examples of hardware/software/firmware identifications include:

— none (for a completely stand-alone TOE);

— a standard PC with a dual core 2.10 GHz or faster processor and 4GB or more RAM, running the Yaiza operating system for professionals, version 53.0 Update 6b, c, or 7, or version 54.0;

— a standard 64-bit server with a 2xQuad-Core core processor and 16GB or more RAM, running the Yaiza operating system, server edition version 7.0 Update 6d, and the WonderMagic 12.0 Graphics card with the 1.01 WM Driver Set;

— a CleverCard SB17067 integrated circuit;

— a CleverCard SB17067 integrated circuit running v12.0 of the QuickOS smart card operating system;

— the Yaiza mobile-OS 3.1.6 on smartphone and tablet devices using the FP9 processor.

B.3.3 Conformance claims and conformance statement (APE_CCL)

B.3.3.1 General

The conformance claims section of a PP describes how the PP:

— states the applicable edition of the relevant parts of ISO/IEC 15408 series;

— conforms with ISO/IEC 15408-2 and ISO/IEC 15408-3 (i.e. conformant or extended);

— claims other PPs (if any);

— claims packages (if any);

The description of how the PP conforms to the ISO/IEC 15408 series consists of two items: the edition of the relevant part of ISO/IEC 15408 series that is used and whether the PP contains extended security requirements or not (see 10.3 and D.3.6).

The description of conformance claimed by the PP to other PPs means that the PP lists any other PPs to which conformance is being claimed to. The type of conformance being claimed is also identified. For an explanation of this, see 10.3.

The description of conformance of the PP to packages means that the PP lists the packages to which conformance is being claimed. For an explanation of this, see 10.3.

NOTE 1 See C.2.2.5 for the use of conformance claims in PP-Modules.

NOTE 2 See B.5.2 for the use of conformance claims in Direct Rationale PPs.

The conformance statement section of a PP describes how the PP:

— references any evaluation method(s) and/or activities derived from ISO/IEC 18405;

— may be used in conjunction with other PPs and PP-Modules in PP-Configuration. In the case of exact conformance, the conformance statement is required.

In the conformance statement, the references to the evaluation methods/ activities means that the PP provides references to the evaluation method(s) and/or activities to be used during an evaluation based on a ST claiming conformance to the PP. These evaluation methods and activities may be included directly in the PP or may be found in a referenced supporting document. It is not necessary to reproduce the text of these evaluation methods and activities in the PP. See 10.3.

If evaluation methods/ evaluation activities that have been derived from ISO/IEC 18045 are to be used to evaluate the PP then these shall be identified with the relevant security requirement section by including a statement in the following form:

"This PP requires the use of evaluation methods/ evaluation activities defined in <reference(s)>."

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 document containing the PP or to one or more separate documents.

NOTE 3 As outlined in 13.5, in some cases, evaluation schemes do not always approve the use of particular EMs/EAs.

The conformance type in the PP states how STs and/or other PPs shall conform to that PP. The PP author selects whether "exact", "strict" or "demonstrable" conformance is required.

B.3.3.2 Exact conformance

If exact conformance is selected, the PP author shall, where applicable, specify the following information in the allowed-with statement in the conformance claims section of the PP:

— other PPs that may be used, either by a ST based on this PP, or used in a PP-Configuration, with this PP;

— PP-Modules that may specify this PP in that PP-Module's PP-Module Base, or that may be present in a PP-Configuration that also includes the PP.

NOTE 1 If neither of the above options is exercised, then a ST can claim exact conformance to only the PP by itself.

NOTE 2 A PP cannot claim exact conformance to another PP.

B.3.4 Security problem definition (SPD) (APE_SPD)

See 7.1 for information and requirements for the SPD, including threats, assumptions and organizational security policies (OSPs).

B.3.5 Security objectives (APE_OBJ)

See 7.2 for information and requirements for the security objectives including security objectives for the TOE and security objectives for the operational environment.

NOTE In the case of Direct Rationale, security objectives for the TOE are not included.

B.3.6 Extended components definition (APE_ECD)

In many cases the security requirements in a PP are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3, see B.3.7. However, in some cases, there can be requirements in a PP that are not based on components in ISO/IEC 15408-2 or ISO/IEC 15408-3. In these cases, new components, i.e. extended components, shall be defined, and the definition provided in the Extended Components Definition section. For more information on this, see 8.4.

NOTE This subclause is intended to contain only the extended components and not the extended requirements which are based on the extended components. The extended requirements are included in the security requirements section as described in B.3.7 and are then for all purposes treated identically to the requirements that are based on components given in ISO/IEC 15408-2 or ISO/IEC 15408-3.

B.3.7 Security requirements (APE_REQ)

B.3.7.1 General

The security requirements consist of two groups of requirements:

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

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

These two groups are discussed in 7.3.

B.3.7.2 Including requirements in a PP

For a PP with strict conformance to another PP, all the requirements in this PP shall be included, and additional requirements may be included in the conformant PP.

For a PP with demonstrable conformance to another PP, all requirements in this PP shall be included, or a rationale explaining how they are otherwise met shall be provided in the conformant PP.

The following types of discretionary requirement may be included in PPs in all (exact, strict and demonstrable) conformance types:

If a PP contains optional requirements, a conformant PP may instantiate these requirements, being sure to include any required SPD-elements associated with those requirements. This may be done regardless of the conformance required by the PP. Omitting optional SFRs does not constitute “partial conformance” to a PP, and thus is allowed.

B.4 Referring to other standards in a PP

In some cases, a PP author needs to refer to an external standard, such as a particular cryptographic standard or protocol. The ISO/IEC 15408 series allows two ways of doing this:

a) as an OSP (or part of it);

EXAMPLE 1 There exists a government standard defining how passwords shall be chosen, this can be stated as an OSP in a PP. This can lead to an objective for the environment (e.g. if users of the TOE need to choose passwords accordingly), or it can lead to security objectives for the TOE and then to appropriate SFRs (likely of the FIA class), if the TOE generates passwords. In both cases the rationale of the PP author needs to make plausible that the security objectives for the TOE and the SFRs are suitable to fulfil the OSP. The evaluator will examine if this is in fact plausible (and can decide to look into the standard for this), if the OSP is implemented by SFRs, as explained below.

b) as a technical standard used in a refinement of a component or security requirement.

EXAMPLE 2

> FCS_CKM.1.1 Refinement: "The [selection: TSF, TOE platform] shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm
>
> [selection:
>
> RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: [selection:
>
> FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
>
> ANSI X9.31-1998, Section 4.1];
>
> ECC schemes using "NIST curves" P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
>
> FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1
>
>]".

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

NOTE The PP author is reminded that referring to a standard in SFRs can impose a significant burden on a developer developing a TOE that meets the PP (depending on the size and complexity of the standard and the assurance required), and that it can be more suitable to require alternative (non-CC related) ways to assess conformance to that standard.

B.5 Direct Rationale PPs

B.5.1 General

Writing a PP includes consideration of the STs that will be written with the PP as a basis. As noted in D.4, in some cases it is desired to write a PP that supports the specification of Direct Rationale STs.

The intention of the Direct Rationale PP is to minimize the level of indirection between the SPD, any security objectives for the operational environment, and the SFRs.

In some situations, it is appropriate to omit the definition of the TOE security objectives. In this case the SFRs enhanced with natural language descriptions and the objectives for the environment directly map the SPD.

A Direct Rationale PP consists of:

a) a PP introduction, consisting of a PP reference and a TOE overview;

b) the conformance claim;

c) security objectives for the operational environment;

d) the SFRs and the SARs (including the extended components definition) and the security requirements rationale (only if the dependencies are not satisfied).

The content of a Direct Rationale PP is shown in Figure B.2.

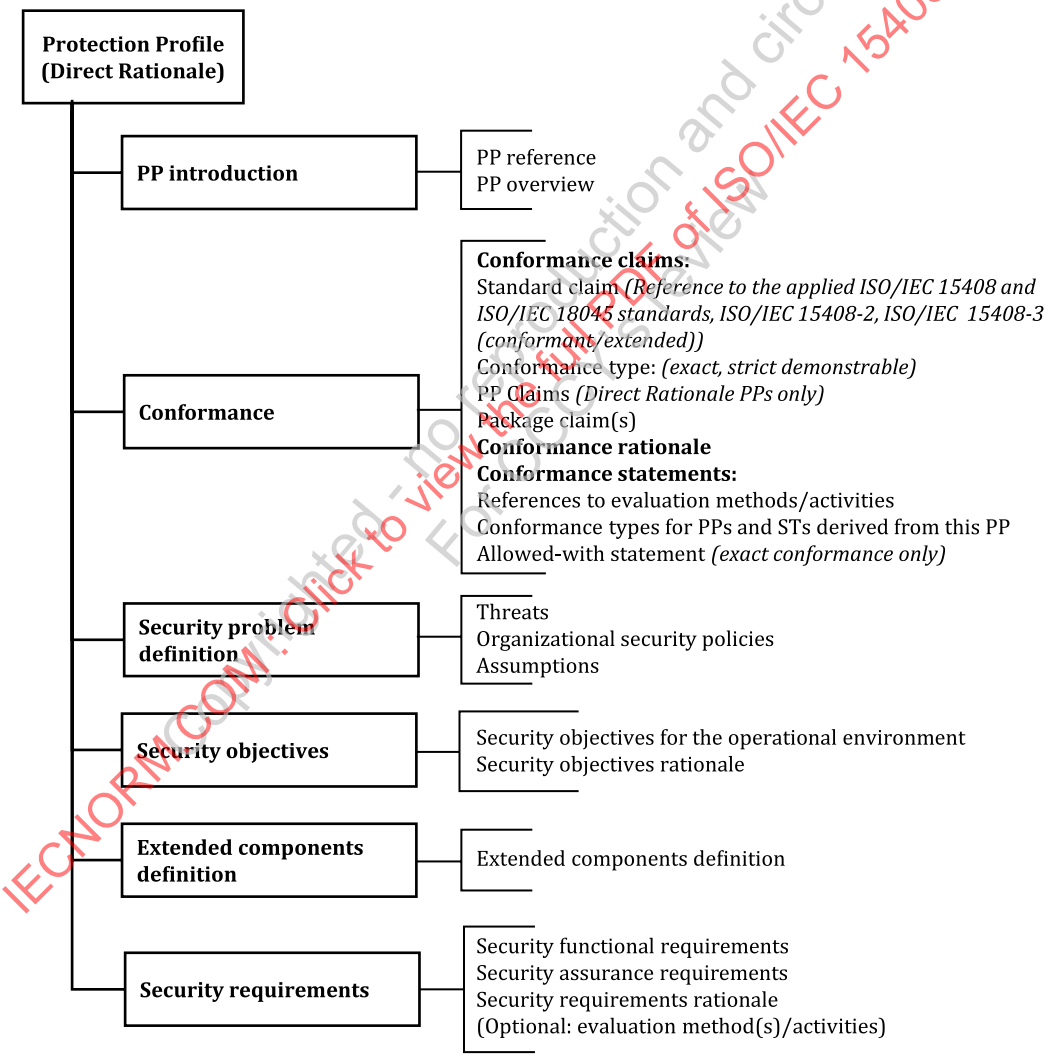

Figure B.2 — Contents of a Direct Rationale PP

B.5.2 Conformance claims (APE_CCL) for Direct Rationale PPs

A Direct Rationale PP shall only claim conformance to another Direct Rationale PP.

A regular PP may claim conformance with a Direct Rationale PP.

B.5.3 Security Objectives (APE_OBJ) for Direct Rationale PPs

A Direct Rationale PP has the following differences with respect to security objectives when compared to a PP that contains security objectives for the TOE:

— security objectives for the TOE are not included. The security objectives for the operational environment shall still be described;

— a security objectives rationale is included only for the security objectives for the operational environment since there are no TOE security objectives in the PP;

— Security Requirements (APE_REQ) for Direct Rationale PPs.

A security requirements rationale that directly maps the SFRs and any security objectives for the operational environment to the SPD-elements is included. It is recommended that this part of the security requirements rationale is located directly under each of the threats, OSPs and assumptions in the SPD section. As in regular PPs, the security requirements rationale also needs to justify any SFR dependencies that are not satisfied; this part of the rationale is typically located after the definition of the SFRs.

B.6 Optional contents of a PP

PPs may include evaluation methods/ activities that are derived from ISO/IEC 18405. Evaluation methods/ activities that are associated with the PP are referenced in the conformance statement section of the PP. See 10.3.

If the PP author decides to include any evaluation method(s) and/or activities in the PP then they may be described either in a (separate) supporting document, or in the security requirements section of the PP along with the relevant security requirement.

Annex C
(normative)

Specification of PP-Modules and PP-Configurations

C.1 Goal and structure of this annex

The goal of this annex is to summarize the structure and expected content of PP-Modules and PP-Configurations.

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

C.2 Specification of PP-Modules

C.2.1 Using a PP-Module

A PP-Module is a security statement of a group of users or developers, regulators, administration, or any other entity that meets specific consumer needs. A PP-Module complements one or more PPs and optionally other PP-Modules, which are referred to as that PP-Module's "PP-Module Base", and allows consumers to refer to this statement, facilitates the evaluation against it and the comparison of conformant evaluated TOEs. A PP-Module can only be used within a PP-Configuration that includes this PP-Module Base.

NOTE A base PP is a PP that is required by a PP-Module. A base PP-Module is a PP-Module that along with its PP-Module Base is required by another PP-Module.

C.2.2 Mandatory contents of a PP-Module

C.2.2.1 General

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

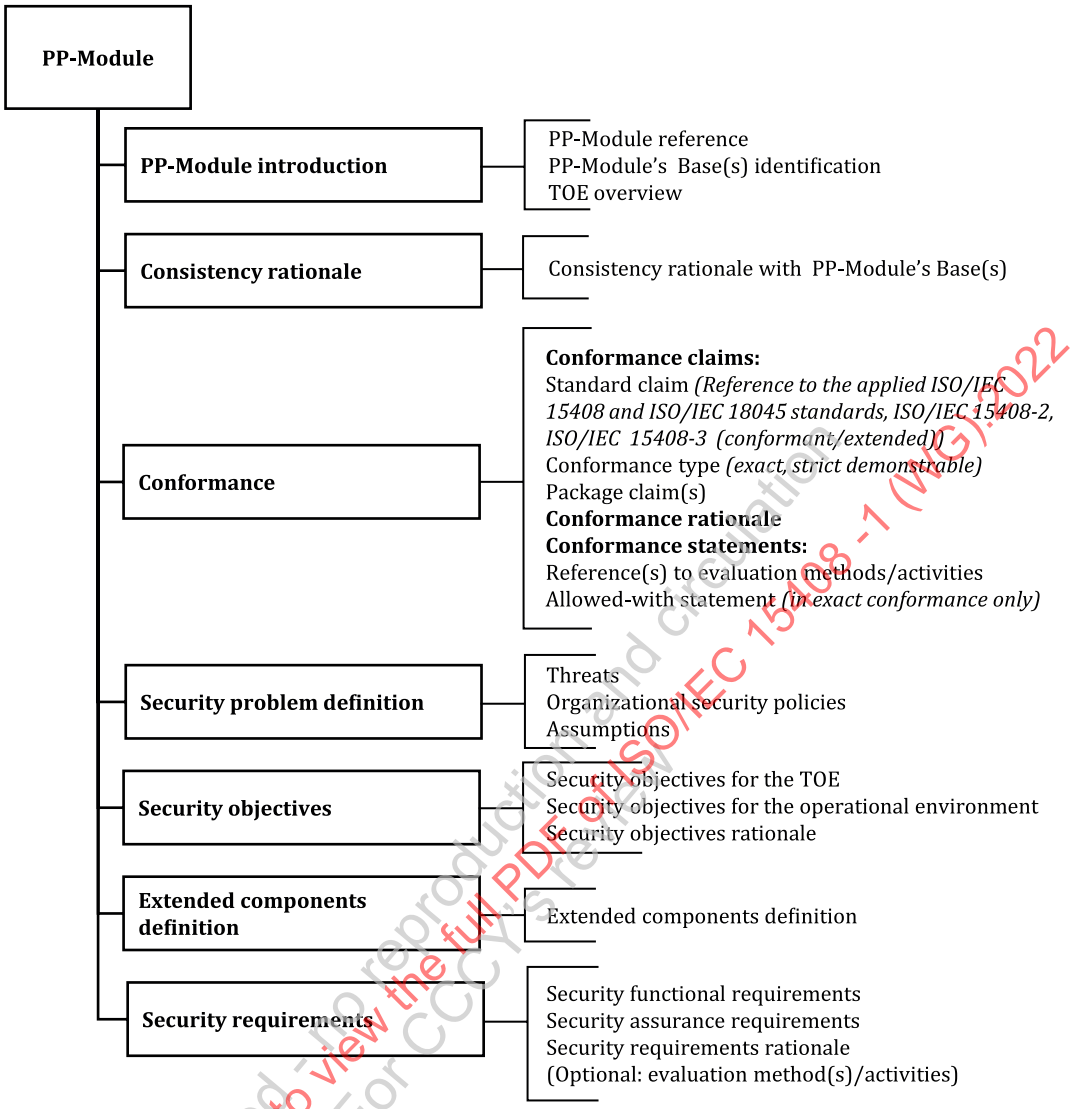

Figure C.1 — Contents of a PP-Module

The content of a PP-Module is summarized below and explained in detail in C.2.2.2 to C.2.3. A PP-Module contains:

— an *Introduction* which identifies the PP-Module, identifies the PP-Module Base which it is based on and provides a description of the TOE within its environment that meets the descriptions underlying the PP-Module Base;

— a *consistency rationale* that states the correspondence between the PP-Module and its PP-Module Base;

— a *conformance claim* regarding the edition of the ISO/IEC 15408 series, the conformance statement and for the case of exact conformance the allowed-with statements;

— a *security problem definition* with threats, assumptions, and OSPs;

— 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;