CC and CEM addenda

Modular PP

March 2014

Version 1.0

CCDB-2014-03-001

Foreword

This is addenda to the the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation that will be integrated in the next versions of those documents.

Certificates issued as a result of the application of those addenda are recognized under the CCRA.

Technical Editor: ANSSI

Document History:
V1.0, March 2014 : Initial release.

Field of special use: None

Table of contents

1 Introduction

1.1 Executive summary

1 This document extends the Common Criteria (CC) framework for the definition and evaluation of modular protection profiles. It defines a methodology that allows addressing TOE's optional security features and enhances the factorisation of PP edition and evaluation tasks and the PP maintenance process by limiting the impact of PP modifications.

2 The methodology relies on two notions:

- "PP-module": CC counterpart of a set of optional security features for a certain type of TOE and has to be used together with one or more base-PP(s). This notion shall not be confused with the notion of module used in TOE decomposition for the ADV_TDS class;
- "PP-configuration": protection profile composed of standard protection profiles and PP-modules.

3 The methodology states the expected content of PP-modules and PP-configurations in Chapter 2, the new assurance class ACE for the evaluation of PP-configurations in Chapter 3 and the evaluation methodology in Chapter 4.

1.2 Scope

4 This document contains all the normative elements required to develop and evaluate modular protection profiles. It has to be used as a complement to CC Part 3 and CEM for the edition and evaluation of modular protection profiles.

1.3 Audience

5 This document is intended for PP editors, ST editors and evaluators.

1.4 Normative references

6 The following references apply to this document.

[CC-1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 1: Introduction and general model. CCMB-2009-07-001.

[CC-2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 2: Security functional components. CCMB-2009-07-002.

[CC-3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 3: Security assurance components. CCMB-2009-07-003.

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 3, July 2009. Evaluation methodology. CCMB-2009-07-004.

1.5 Terms and definitions

7 For the purpose of this document, the following terms and definitions apply.

8 This section contains only those terms which are used in a specialised way throughout the CC and do not belong to list of terms introduced in [CC-1]§4.

9 **Base Protection Profile** — protection profile used as a basis to build a Protection Profile configuration

10 **Protection Profile configuration** — protection profile composed of base Protection Profiles and Protection Profile modules

11 **Protection Profile module** — implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles

2 Addendum to CC Part 1

2.1 Protection Profiles, PP-Modules and PP-Configurations

(completes [CC-1]§9)

2.1.1 Introduction

12 To allow the definition of modular Protection Profiles that address optional TOEs' security features, this chapter introduces two constructs: PP-modules and PP-configurations, as well as the way they can be used to evaluate compliant products.

2.1.2 PP-Modules

(new)

13 A PP-module is a consistent set of elements (threats, assumptions, organisational policies, objectives and security requirements) with a unique reference.

14 Unlike Protection Profiles, PP-modules address optional security features of a given type of TOE that cannot be required uniformly for all products of this kind.

15 Each PP-module refers to at least one base Protection Profile (or PP-base) that provides the definition of the TOE type and the mandatory requirements to fulfill. The PP-module specifies the modified TOE type, completes these requirements and has to be used with the PP-bases: a PP-module may introduce new elements to the PP-bases and may also refine or interpret some of the elements of the PP-bases.

16 If the PP-module refers to several base Protection Profiles, this set of base PPs have to be used simultaneously for the evaluation and usage of the PP-module.

17 The PP-module can also refer to alternate sets of base PPs, in the case the PP-module could comply with alternate base PPs depending of the usage.

18 The evaluation of a PP-module alone is meaningless. A PP-module has to be evaluated as part of a PP-configuration, at least with its mandatory base PPs.

2.1.3 PP-Configurations

(new)

19 A PP-configuration results from the combination of at least one PP-module with its base PPs, without any additional content: a PP-configuration is much like a Protection Profile that would include all the elements from the base PPs and the PP-modules.

20 A PP-configuration can select more PPs than the base PPs of the PP-modules, but at least all of the base PPs of the referred PP-modules must be included in the PP-configuration.

21 If the PP-module defines alternate sets of base PPs, only one of these sets must be used in the PP-configuration.

22 A PP-configuration holds a unique reference and identifies all the PP components: selected base PPs and selected PP-modules.

23 A PP-configuration can only combine certified base PPs to PP-modules.

24 Evaluation rules for PP-configurations are similar to the ones for standard PPs. These rules are described in new Class ACE, in chapter 3.

2.1.4 Using PP-modules and PP-configurations in security targets

(new)

25 PP-modules are used to build specific PP-configurations on top of one or more base PPs. PP-modules are used in Security Targets only as part of well-identified PP-configurations.

26 PP-configurations are used like Protection Profiles. A Security Target can claim conformity to a PP-configuration provided this PP-configuration has been evaluated. Henceforth, the evaluation of the ST can rely on the results of the PP-configuration evaluation results as usual.

27 Note that the evaluation of a PP-configuration can arise in two situations, with no impact on the evaluation methodology:

- Independently of any product (a fortiori ST) evaluation, or
- As the first step of the evaluation of a Security Target that claims conformity with the PP-configuration. Otherwise the conformance claim is meaningless and the ST evaluation would fail in this aspect.

28 In practice, a ST that claims conformance with a non-certified PP-configuration can still be evaluated with a conformance claim against the PP-base of the PP-configuration; the elements of the ST that meet the PP-modules of the PP-configuration would be evaluated as standard additions to the PP-base, proper to the TOE.

2.2 Evaluation results

(completes [CC-1]§10)

2.2.1 Introduction

29 This chapter presents the expected results from PP-configuration evaluation and ST/TOE evaluations according to the CEM and the addendum presented in chapter 4.

30 The evaluated PP-configurations integrate the catalogue of evaluated PPs, linked to the base PPs of the PP-configurations.

31 STs may be based on packages, evaluated PPs or non-evaluated PPs, evaluated PP-configurations or non-evaluated PP-configurations, or built-in independently.

2.2.2 Results of a PP-configuration evaluation

(new)

32 CC Part 3 and the addendum in Section 3.1 contain the evaluation criteria that an evaluator is obliged to follow in order to state whether a PP-configuration is complete, consistent, and technically sound and hence suitable for use in developing an ST.

33 The results of the evaluation shall also include a “Conformance Claim” (see Section 2.2.4).

2.2.3 Results of an ST evaluation

(completes §10.3 : evaluate the PP-configuration before the ST itself)

34 CC Part 3 and the addendum in Section 3.2 contain the evaluation criteria that an evaluator is obliged to consult in order to determine whether sufficient assurance exists that the TOE satisfies the SFRs in the ST, when this ST claims conformance with one or more PP-configurations.

35 The results of evaluation shall also include a “Conformance Claim” as defined in the next section.

2.2.4 Conformance claim

(completes §10.4)

36 Besides the standard CC conformance claim regarding the version of the CC, the CC Part 2 and Part 3, the SFR and SAR packages, and the standard PP claim,

- a PP-configuration has to provide a conformance statement applicable to the conformant STs, either *strict* or *demonstrable*, that meet the conformance statements of the base PP(s),
- a ST may claim conformity with one or more PP-configurations.

2.3 Specification of PP-modules

(new)

2.3.1 Mandatory content of a PP-module

37 Figure 1 shows the mandatory content of a PP-module.

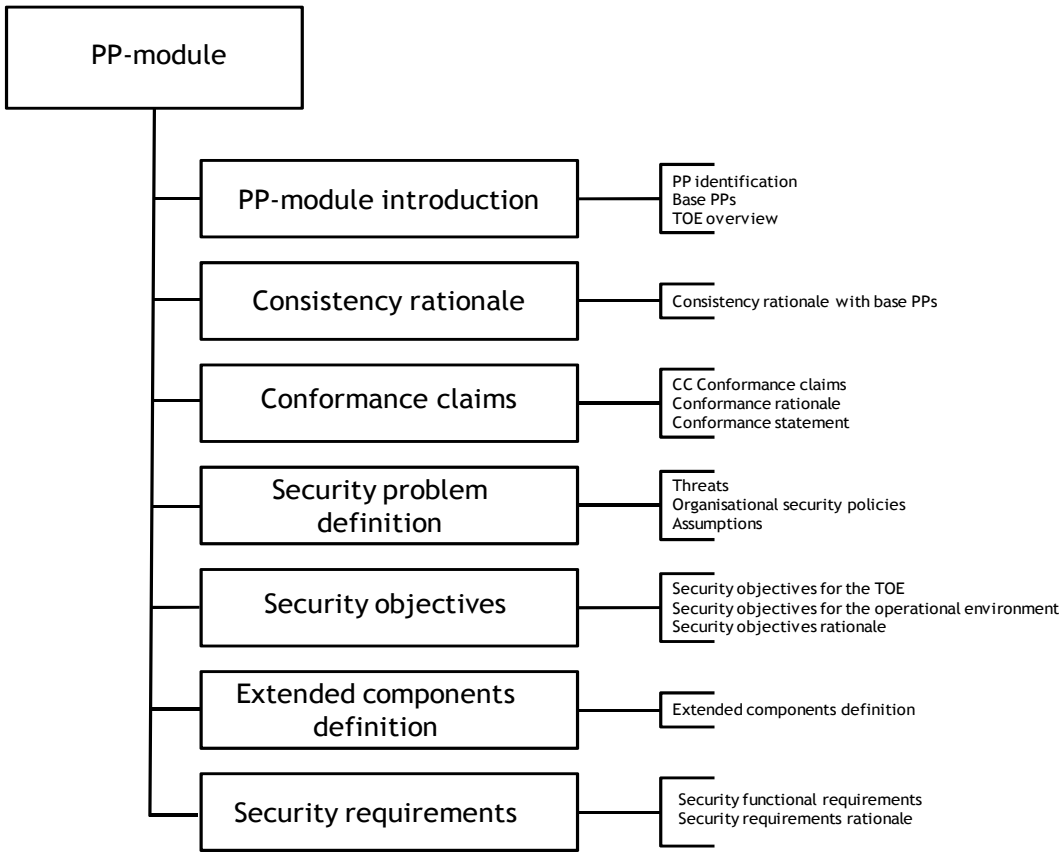

Figure 1 - PP-module content

38 The content of the PP-module is summarized below and explained in detail in Sections 2.3.3 to 2.3.10. A PP-module contains:

- an *Introduction* that identifies the PP-module, identifies the base PP(s) and states the correspondence rationale, and provides a description of the TOE within its environment that meets the descriptions underlying the base PPs,
- a *Consistency rationale* that states the correspondence between the module and its base PP(s),
- a *Conformance claim* regarding the CC, with inherited EAL and conformance statement,
- a *Security problem definition* with threats, assumptions and organisational security policies,

- a *Security objectives* section presenting the solution to the security problem in terms of objectives for the TOE and its operational environment,
- an optional *Extended functional components definition* where new functional components not included in CC Part 2 are introduced,
- a *Security functional requirements section* with a standardized statement of the TOE security objectives.

2.3.2 Using the PP-module

39 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 completes one or more base PPs and allows consumers to refer to this statement, facilitates the evaluation against it and the comparison of conformant evaluated TOEs.

2.3.3 PP-module introduction

2.3.3.1 PP-module reference

40 The PP-module introduction provides a clear and unambiguous reference that allows identifying the PP-module. A typical reference is made of the title of the PP-module, its version, their authors and the publication date.

41 The PP-module reference will be used to index the document in Protection Profiles databases.

2.3.3.2 Base PP identification

42 The PP-module introduction identifies the base Protection Profile(s) the module relies on. The identification consists of a list of PP references.

43 The PP-module may require to be used with a set of base PPs simultaneously, say $\{PP_1, \ldots, PP_n\}$; the identification list states:

PP_1 AND… *AND* PP_n, with $n \geq 1$

44 The PP-module may allow the use with alternate sets of base PPs, say $\{S_1, \ldots, S_k\}$; the identification list states:

S_1 OR … *OR* S_k, with $k \geq 1$

45 The general form of the base PP identification is then

($PP_{1,1}$ *AND*… *AND* $PP_{1,n1}$) *OR* … *OR* ($PP_{k,1}$ *AND*… *AND* $PP_{k,nk}$), with $ni \geq 1$, $k \geq 1$

46 Note that a PP-module that states an ORed-list can be replaced by as many PP-modules as elements in the list. That is, the ORed-list is a means to avoid managing similar PP-modules for different usages, which does not introduce any complexity to the security specification itself.

2.3.3.3 TOE overview

47 The *TOE overview* of the PP-module may complete the TOE overviews of the base PPs, provided the supplements do not contradict the base PPs:

- The *TOE type* of the PP-module can be the same of the base PPs or introduce specificities that meet the purpose of the PP-module.
- The PP-module can introduce additional *usage and major security features* to those stated in the base PPs.
- The PP-module can specify particular *non-TOE HW, SW and FW* compliant with the statement in the base PPs.

48 The possibility of supplementing the *TOE overview* of one or more base PPs in a PP-module has the same meaning as the supplements of a ST regarding the *TOE overview* of a PP or the supplements of a PP that is conformant to another PP.

49 The statement of the *TOE overview* in a PP-module is necessary whenever the *TOE overview* of the base PPs present different characteristics that need to be consolidated.

50 The PP-module may provide as many specific TOE overviews as alternate sets of base PPs.

2.3.4 Consistency rationale

51 The PP-module has to provide a consistency rationale with respect to its base PPs.

52 If the PP-module specifies alternate sets of base-PPs, the PP-module must provide as many conformance claims as the number of alternate set of base-PPs.

53 If the PP-module specifies alternate sets of base-PPs, the PP-module must provide as many consistency rationales as the number of alternate set of base-PPs.

54 The consistency analysis must be performed on the TOE type, the SPD, the objectives and the security functional requirements. At the end, the goal is to demonstrate that a TOE can meet the TOE types descriptions provided in the base-PP(s) and in the PP-module and that can satisfy all the base-PPs and the PP-module security functional requirements.

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

56 The consistency rationale may use correspondence tables between SPD/objectives/SFRs in the PP-module and SPD/objectives/SFRs in the base PPs together with textual justifications whenever needed.

57 Note that the consistency at the SFR level implies the consistency of the union of objectives and the union of SPDs provided that the PP-module does not change the assumptions and objectives for the environment of the base-PP(s). Indeed, assume that both SFR and SFR' are consistent sets, then:

- For PP-base: SFR $\Rightarrow$ OBJ_TOE $\Rightarrow \neg$ T and OSP_TOE
- For PP-module: SFR' $\Rightarrow$ OBJ_TOE' $\Rightarrow \neg$ T' and OSP_TOE'
- Then SFR and SFR' $\Rightarrow$ OBJ_TOE and OBJ_TOE' $\Rightarrow \neg$ T and $\neg$ T' and OSP_TOE and OSP_TOE'
- Assume the consistency of (SFR and SFR') has been demonstrated.
- Assume (OBJ_TOE and OBJ_TOE') leads to contradiction (FALSE), then (SFR and SFR') also does which contradicts the previous consistency assessment.

2.3.5 Conformance claims

58 This section describes how the PP-module conforms to:

- Part 2 of the Common Criteria: CC version and extended security requirements,
- SFR packages.

59 A PP-module cannot claim conformance to any PP, PP-module or PP-configuration.

60 A PP-module inherits the conformity to SAR packages (including predefined EAL) from the base PPs. The issue of ANDed-base PPs with different EALs has to be dealt with like in a ST conformant to all those PPs.

61 A PP-module inherits the conformance statement (*strict* or *demonstrable*) from the base PPs. The issue of ANDed-base PPs with different conformance statements has to be dealt with like in a ST conformant to all those PPs.

2.3.6 Security problem definition

62 This section defines the security problem addressed by the PP-module. It can contain assumptions, threats and organisational security policies.

63 A PP-module defines the security problem in relationship with the security problem of the base PPs and the definition of the TOE and its environment provided in the PP-module's *Introduction*.

64 Each element of the SPD may either come from a base PP or be entirely new. Let E be an element of the SPD of a PP-module, one of the following cases holds:

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

65 Note that the interpreted / refined elements can be dealt with as new elements without any impact on the meaning of the SPD.

66 Note that as for STs, a PP-module can introduce assumptions provided they cover aspects that are outside the scope of the base PPs.

2.3.7 Security objectives

67 This section defines the security objectives for the TOE and for the TOE's operational environment.

68 A PP-module defines the security objectives in relationship with its security problem and with the security objectives of the base PPs.

69 Each security objective may either come from a base PP or be entirely new. Let O be an objective of a PP-module, one of the following cases holds:

- O belongs to an identified base PP; the PP-module may only contain a reference to the objective in the base PP,
- O results from the interpretation or refinement of an objective of the same kind (for the TOE or for the TOE operational environment) of a base PP,
- O is a new objective introduced by the PP-module.

70 Note that the interpreted / refined objectives can be dealt with as new objectives without any impact on the meaning of the whole set of objectives.

71 As for STs, a PP-module can introduce new objectives for the TOE operational environment only provided they address aspects that are outside the scope of the base PPs.

72 In the opposite, if this is the purpose of the PP-module, some security objectives for the environment of the base PPs could become security objectives for the TOE in the PP-module.

73 This section also defines the rationale between the SPD and the security objectives of the PP-module, which consists of a mapping that traces the SPD of the PP-module to their security objectives as well as a justification demonstrating that the tracing is effective, as specified in [CC-Part1] §B.7. Moreover, the mapping has to show not only that all the assumptions, threats and organisational security policies are covered but also that there is no useless security objective.

74 It may happen that some security objectives of the PP-module cover also elements of the SPD of the base PPs that do not belong to the SPD of the PP-module itself. This information is not required, but can be provided in application notes.

2.3.8 Extended functional components definition

75 This section is identical to the standard PP and ST extended components section specified in [CC-Part1] §A.8, applied to functional components only.

2.3.9 Security functional requirements

76 This section defines the security functional requirements for the TOE in relationship with the set of TOE security objectives in the PP-module and with the security functional requirements of the base PPs.

77 Each security functional requirement may either come from a base PP or be entirely new. Let R be a security functional requirement of a PP-module, one of the following cases holds:

- R belongs to an identified base PP; the PP-module may only contain a reference to the requirement in the base PP,
- R results from the interpretation or refinement of a SFR of a base PPs,
- R is a new requirement introduced by the PP-module.

78 Note that the interpreted / refined requirements can be dealt with as new ones without any impact on the meaning of the whole set of requirements.

79 This section also defines the rationale between the SFRs and the TOE security objectives of the PP-module, which consists of a mapping that traces the TOE objectives of the PP-module to one or more SFRs and a justification demonstrating that the tracing is effective, as specified in [CC-Part1] §B.9. Moreover, the mapping must fulfill the conditions specified in Section 2.3.10 and has to show not only that all the objectives for the TOE are covered but also that there is no useless security functional requirement.

80 It may happen that some SFRs of the PP-module cover also TOE security objectives of the base PPs that do not belong to the PP-module itself. This information is not required, but can be provided in application notes.

2.3.10 Guidance for inclusion of elements from base-PP

81 In order to limit the amount of information contained in the PP-module, the editor may apply the following rules.

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

83 Let *P* be a PP-module with *Q* amongst its base PPs. *P* has to satisfy the following condition:

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

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

85 That is, a PP-module would not contain portions of base PPs unless they are required to fulfill new needs. Here, interpreted/refined elements are considered new.

2.4 Specification of PP-configurations

2.4.1 Mandatory content of a PP-configuration

86 The content of the PP-configuration is summarized below and explained in detail in Sections 2.4.3 and 2.4.4. A PP-configuration contains:

- a *Reference* that identifies the PP-configuration,
- a *Components statement* that identifies the base PPs and the PP-modules composing the PP-configuration,
- a *Conformance statement*, that specifies whether the conformance to this PP-configuration has to be strict or demonstrable,
- a *SAR statement*, specifying the EAL or SAR package applicable to the PP-configuration.

2.4.2 Using the PP-configuration

87 PP-configurations are security statements that cover specific needs of groups of users, consumers, organisations, etc. Any PP-configuration can be used exactly as a standard Protection Profile, as explained in Section 2.6.

2.4.3 PP-configuration reference

88 The PP-configuration reference provides a clear and unambiguous identification, usually made of a title, version number, sponsor and the publication date.

89 The PP-configuration reference will be used to index the document in Protection Profiles databases.

2.4.4 PP-configuration components

90 The *Components statement* identifies the base PPs and the PP-modules that compose the PP-configuration.

91 The *Components statement* must include at least all base PPs referenced in the PP-modules. If the PP-module specifies alternate sets of base-PPs, only one of these sets must be referred to in the PP-configuration.

2.4.5 PP-configuration conformance

92 The *Conformance statement* specifies whether the conformance to this PP-configuration has to be strict or demonstrable.

93 Any ST that claims conformance to the PP-configuration shall conform to the kind of conformance claimed in the PP-configuration.

2.4.6 PP-configuration SAR statement

94 The *SAR statement* specifies the set of SAR (potentially predefined EAL) applicable to any product evaluation with a ST that claims conformance to this PP-configuration.

2.4.7 Evaluation of a PP-configuration

95 The assurance components for PP-configuration evaluation, defined in Chapter 3, are the following: ACE_INT.1, ACE_CCL.1, ACE_SPD.1, ACE_ECD.1, ACE_OBJ.1, ACE_REQ.1, ACE_MCO.1 and ACE_CCO.1.

2.5 Specification of Security Targets

(completes §A, "Conformance claim")

96 A Security Target can use PP-configurations in the same way as standard Protection Profiles. That is, the *Conformance claim* of a ST can contain a *PP claim* that identifies the PP-configurations the ST is conformant with.

97 All the other content of a ST remains unchanged with respect to the descriptions provided in [CC-Part1] §A.

2.6 Interpretation of PP-configuration as a standard PP

98 Once evaluated, a PP-configuration can be interpreted and used in the same way as a standard Protection Profile. This chapter explains how to combine the content of the base-PP(s) and PP-module(s) of a PP-configuration so as to interpret it as a standard PP.

2.6.1 TOE type

99 The TOE type of a PP to interpret in the same way as the PP-configuration would be constituted of the TOE type of the base-PP(s) with the additions introduced in the PP-module(s) TOE types. The evaluation of the PP-configuration ensures that it forms a consistent TOE type.

2.6.2 Conformance claims

100 The Conformance claims of a PP to interpret in the same way as the PP-configuration would contain:

- The conformance to the PP(s) whose conformance is claimed in the base PP(s).
- The conformance to SAR packages (including predefined EAL) from the base PPs. The issue of ANDed-base PPs with different EALs has to be dealt with like in a ST conformant to all those PPs.
- The conformance statement (strict or demonstrable) from the base PPs. The issue of ANDed-base PPs with different conformance statements has to be dealt with like in a ST conformant to all those PPs.

2.6.3 Security problem definition

101 The SPD of a PP to interpret in the same way as the PP-configuration would contain the union of the elements from the base-PP(s) and PP-module(s) of the PP-configuration.

2.6.4 Security objectives

102 The security objectives of a PP to interpret in the same way as the PP-configuration would contain the union of the security objectives from the base-PP(s) and PP-module(s) of the PP-configuration.

2.6.5 Extended functional components definition

103 The extended functional components of a PP to interpret in the same way as the PP-configuration would contain all extended functional components from the base-PP(s) and PP-module(s) of the PP-configuration.

2.6.6 Security functional requirements

104 The set of SFRs of a PP to interpret in the same way as the PP-configuration would contain:

- all the SFRs from the PP-module(s) of the PP-configuration.
- all the SFRs from the base-PP(s) except those which are interpreted or refined in the PP-module(s).

105 The consistency analysis performed on PP-configuration during evaluation shall ensure this set is valid.

3 Addendum to CC Part 3

106 Evaluating a PP-configuration is required to demonstrate that the PP-configuration is sound and consistent. These properties are necessary for the PP-configuration to be suitable for use as the basis for writing an ST or another PP or PP-configuration.

107 The class ACE is defined for the evaluation of a PP-configuration composed of one or more PPs and one PP-module.

108 This Chapter should be used in conjunction with Annexes B and C in CC Part 1, as these Annexes clarify the concepts used here and provide many examples.

109 This standard does not define low assurance PP-configuration evaluation package. There is only one assurance package for PP-configuration evaluation, equivalent to Standard PP evaluation package.

110 Figure 2 shows the families within this class, and the hierarchy of components within the families.

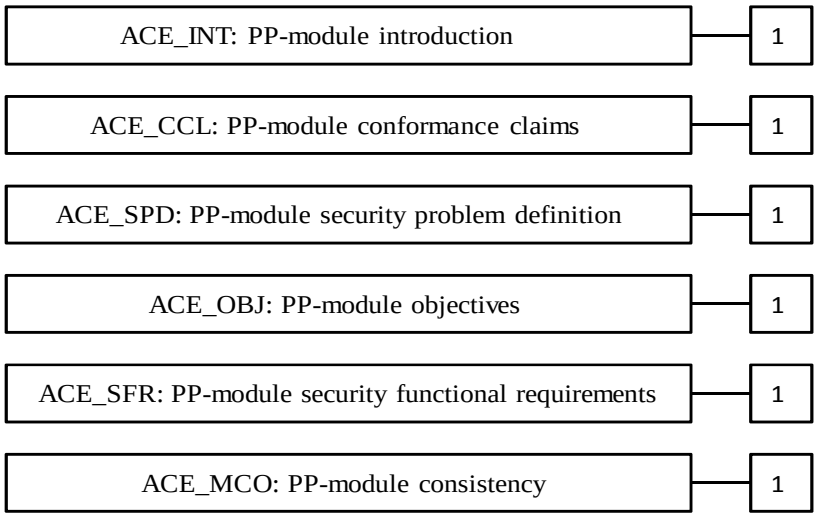

Figure 2 - ACE: Protection Profile configuration evaluation class decomposition

3.1 Class ACE: Protection Profile Configuration evaluation

111 The ACE class is based on APE.

3.1.1 PP-module introduction (ACE_INT)

3.1.1.1 Objectives

112 The objective of this family is to describe the TOE in a narrative way.

113 The objective of this sub-activity is to determine whether the PP-module is correctly identified, and whether the PP-module reference and TOE overview are consistent with each other.

ACE_INT.1 PP-module introduction

Dependencies: No dependency

Developer action elements:

ACE_INT.1.1D **The developer shall provide a PP-module introduction.**

Content and presentation elements:

(All content and presentation elements of APE_INT.1 hold).

ACE_INT.1.1C **The PP-module introduction shall uniquely identify all the base-PPs on which the PP-module relies.**

ACE_INT.1.2C **The TOE overview shall identify the differences introduced by the PP-module with respect to the TOE overview of its base PP(s).**

Evaluator action elements:

ACE_INT.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

3.1.2 PP-module conformance claims (ACE_CCL)

3.1.2.1 Objectives

114 The objective of this family is to determine the validity of the conformance claim. Unlike standard protection profiles, a PP-module cannot claim conformance to another PP or PP-module, nor to CC Part 3 or any SAR package.

ACE_CCL.1 PP-module Conformance claims

Dependencies: ACE_INT.1 PP-module introduction
ACE_ECD.1 Extended functional components definition
ACE_REQ.1 Stated security requirements

Developer action elements:

ACE_CCL.1.1D **The developer shall provide a conformance claim.**

Content and presentation elements:

ACE_CCL.1.1C **The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the PP-module claims conformance.**

ACE_CCL.1.2C **The CC conformance claim shall describe the conformance of the PP-module to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.**

ACE_CCL.1.3C **The conformance claim shall identify all security functional requirement packages to which the PP-module claims conformance.**

ACE_CCL.1.4C **The CC conformance claim shall be consistent with the extended components definition.**

Evaluator action elements:

ACE_CCL.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

3.1.3 PP-module Security problem definition (ACE_SPD)

(All content and presentation elements of APE_SPD.1 hold).

3.1.4 PP-module Security objectives (ACE_OBJ)

(All content and presentation elements of APE_OBJ.2 hold).

3.1.5 PP-module Extended components definition (ACE_ECD)

3.1.5.1 Objectives

115 Extended security functional requirements are requirements that are not based on components from CC Part 2, but are based on extended components: components defined by the PP-module author.

116 Evaluation of the definition of extended functional components is necessary to determine that they are clear and unambiguous, and that they are necessary, i.e. they may not be clearly expressed using existing CC Part 2 components.

ACE_ECD.1 PP-module Extended components definition

Dependencies: No dependencies

Developer action elements:

ACE_ECD.1.1D **The developer shall provide a statement of security functional requirements.**

ACE_ECD.1.2D **The developer shall provide an extended functional components definition.**

Content and presentation elements:

ACE_ECD.1.1C **The statement of security functional requirements shall identify all extended security functional requirements.**

ACE_ECD.1.2C **The extended functional components definition shall define an extended functional component for each extended security functional requirement.**

ACE_ECD.1.3C **The extended functional components definition shall describe how each extended functional component is related to the existing CC Part 2 components, families, and classes.**

ACE_ECD.1.4C **The extended functional components definition shall use the existing CC Part 2 components, families, classes, and methodology as a model for presentation.**

ACE_ECD.1.5C **The extended functional components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.**

Evaluator action elements:

ACE_ECD.1.1E **The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.**

ACE_ECD.1.2E **The evaluator *shall confirm* that no extended functional component may be clearly expressed using existing components.**

3.1.6 PP-module security requirements (ACE_REQ)

3.1.6.1 Objectives

117 The SFRs form a clear, unambiguous and well-defined description of the expected security behaviour of the TOE.

118 Evaluation of the security functional requirements is required to ensure that they are clear, unambiguous and well-defined.

ACE_REQ.1 PP-module security requirements

Dependencies: ACE_ECD.1 PP-module extended security functional components definition
ACE_OBJ.1 PP-module security objectives

Developer action elements:

ACE_REQ.1.1D **The developer shall provide a statement of security functional requirements.**

ACE_REQ.1.2D **The developer shall provide a security requirements rationale.**

Content and presentation elements:

ACE_REQ.1.1C **The statement of security requirements shall describe the SFRs that hold on the TOE.**

ACE_REQ.1.2C **All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs shall be defined.**

ACE_REQ.1.3C **The statement of security functional requirements shall identify all operations on the security functional requirements.**

ACE_REQ.1.4C **All operations shall be performed correctly.**

ACE_ECD.1.5C **Each dependency of the security functional requirements shall either be satisfied, or the security functional requirements rationale shall justify the dependency not being satisfied.**

ACE_REQ.1.6C **The security functional requirements rationale shall trace each SFR back to the security objectives for the TOE.**

ACE_REQ.1.7C **The security functional requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.**

Evaluator action elements:

ACE_REQ.1.1E **The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.**

ACE_REQ.1.2E **The evaluator *shall confirm* that no extended functional component may be clearly expressed using existing components.**

3.1.7 PP-module consistency (ACE_MCO)

3.1.7.1 Objectives

119 The objective of this family is to determine the validity of the PP-module.

ACE_MCO.1 PP-module consistency

Dependencies: ACE_INT.1 PP-module introduction
ACE_SPD.1 PP-module conformance claim
ACE_OBJ.1 PP-module security objectives
ACE_REQ.1 PP-module security functional requirements

Developer action elements:

ACE_MCO.1.1D **The developer shall provide a *consistency rationale* of the PP-module with respect to its base-PP(s) identified in the PP-module introduction. If the PP-module specifies alternate sets of base-PPs, the developer shall provide as many consistency rationales as the number of alternate set of base-PPs.**

Content and presentation elements:

ACE_MCO.1.1C **The consistency rationale shall demonstrate that the TOE type of the PP-module is consistent with the TOE type(s) in the base-PPs identified in the PP-module introduction.**

ACE_MCO.1.2C **The consistency rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the base-PPs identified in the PP-module introduction.**

ACE_MCO.1.3C **The consistency rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the base-PPs identified in the PP-module introduction.**

ACE_MCO.1.4C **The consistency rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the base-PPs identified in the PP-module introduction.**

Evaluator action elements:

ACE_MCO.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. If the PP-module specifies alternate sets of base-PPs, the evaluator shall perform this action for each consistency rationale with its related base-PPs in the alternate set of base-PPs of the PP-module.**

3.1.8 PP-configuration consistency (ACE_CCO)

3.1.8.1 Objectives

120 The objective of this family is to determine the well-formedness and the consistency of the PP-configuration.

ACE_CCO.1 PP-Configuration consistency

Dependencies: ACE_INT.1 PP-module introduction
ACE_REQ.1 PP-module security functional requirements
ACE_MCO.1 PP-module consistency

Developer action elements:

ACE_CCO.1.1D **The developer shall provide the *reference* of the PP-configuration.**

ACE_ CCO.1.2D **The developer shall provide a *components statement*.**

ACE_ CCO.1.3D **The developer shall provide a *conformance statement*.**

ACE_ CCO.1.4D **The developer shall provide a *SAR statement.***

Content and presentation elements:

ACE_CCO.1.1C **The PP-configuration reference shall uniquely identify the PP-configuration**

ACE_CCO.1.2C **The components statements shall uniquely identify the protection profiles and the PP-modules that compose the PP-configuration.**

ACE_ CCO.1.3C **The conformance statement shall specify the kind of conformity of the PP-configuration, either strict or demonstrable.**

ACE_ CCO.1.4C **The *SAR statement* shall specify the set of SAR or predefined EAL that applies to this PP-configuration.**

ACE_CCO.1.5C **The base-PP(s) on which the PP-modules relies shall belong the protection profiles identified in the *components statement* of the PP-configuration.**

Evaluator action elements:

ACE_CCO.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

ACE_CCO.1.2E **The evaluator shall check that the PP-configuration made up of all the protection profiles and PP-modules identified in the *components statement* of the PP-configuration is consistent.**

3.2 Class ASE: Security target evaluation

121 There is no new assurance component for the evaluation of a security target compliant with a PP-configuration. Each of the components in ASE_CCL.1 that apply to a standard PP also applies to a PP-configuration. Indeed, in order to assess the conformity of a security target to a PP-configuration, the PP-configuration has to be interpreted as a standard PP, following guidance given in 2.6.

4 Addendum to CEM

122 All base-PP(s) referenced in the PP-module must be evaluated before the evaluation of a PP-configuration.

123 One possibility for evaluating a PP-configuration is to flatten all the components of the PP(s) and PP-modules composing the PP-configuration and evaluating the resulting PP as a standard PP.

124 Another possibility for evaluation of a PP-configuration composed of several PP-modules proceeds PP-module by PP-module. Considering a PP-configuration composed of the protection profiles P_i and the PP-modules M_j, evaluation of the PP-configuration proceeds with the following steps, illustrated in Figure 3:

1. first evaluating independently all Protection Profiles Pi;
2. evaluating the PP-configuration C_1 composed of the PP-module M_1 with the Protection Profiles P_i;
3. evaluating the PP-configuration C_{i+1} composed of the PP-module M_{i+1} with the PP-configuration C_i considered as a standard PP (cf. Section 2.6);
4. iterating the step 3 for all the PP-modules.

125 Steps 2 and 3 are themselves performed in two steps:

a. Evaluation of the PP-module with its base-PP(s) (ACE_MCO.1)
b. Extension of the evaluation (consistency assessment) to the other elements of the PP-configuration (ACE_CCO.1).

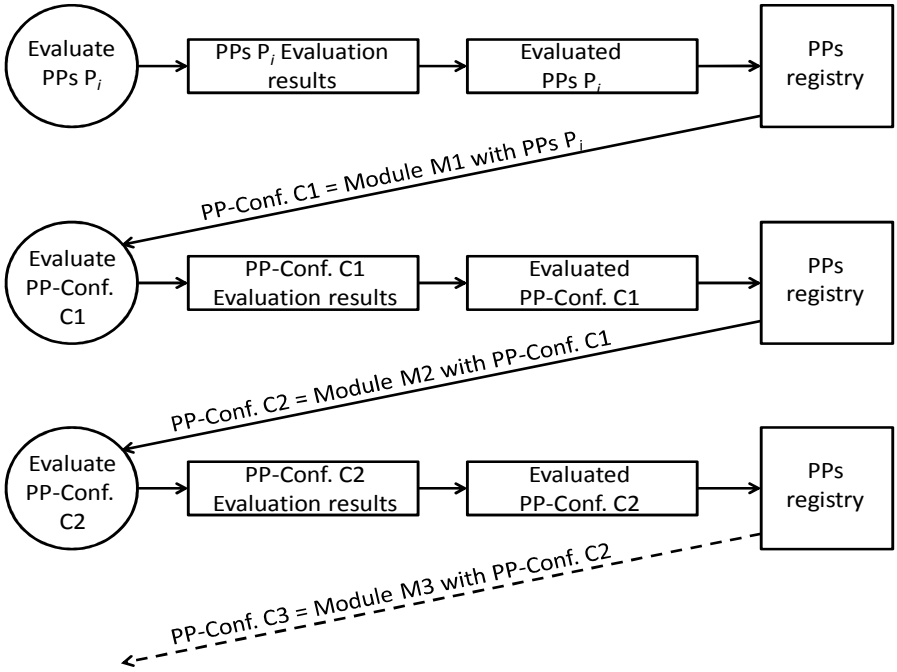

Figure 3 - Evaluation of a PP-configuration

4.1 Class ACE: Protection Profile Configuration evaluation

126 The ACE evaluation methodology is based on APE's. The common parts are not duplicated in this document but referred to.

4.1.1 PP-module introduction (ACE_INT)

4.1.1.1 Evaluation of sub-activity (ACE_INT.1)

4.1.1.1.1 Objectives

127 The objective of this sub-activity is to determine whether the PP-module is correctly identified, and whether the base-PP(s) and TOE overview are consistent with each other.

4.1.1.1.2 Input

128 The evaluation evidence for this sub-activity is:

a. the PP-module;

b. its base-PP(s).

4.1.1.2 Action ACE_INT1.1E

(All actions of APE_INT1.1E hold).

ACE_INT.1.1C **The PP-module introduction shall uniquely identify all the base-PP(s) on which the PP-module relies.**

ACE_INT.1-1 The evaluator ***shall check*** that the PP-module introduction identifies the base-PP(s) on which the PP-module relies.

ACE_INT.1.2C **The TOE overview shall identify the differences introduced by the PP-module with respect to the TOE overview of its base PP(s).**

ACE_INT.1-2 The evaluator ***shall check*** that the TOE overview identifies the differences introduced by the PP-module with respect to the TOE overview of its base PP(s).

4.1.2 PP-module conformance claims (ACE_CCL)

4.1.2.1 Evaluation of sub-activity (ACE_CCL.1)

4.1.2.1.1 Objectives

129 The objective of this sub-activity is to determine the validity of various conformance claims. These describe how the PP-module conforms to the CC Part 2 and SFR packages.

4.1.2.1.2 Input

130 The evaluation evidence for this sub-activity is:

a. the PP-module;

b. the SFR package(s) that the PP claims conformance to.

4.1.2.2 Action ACE_CCL1.1E

ACE_CCL.1.1C **The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the PP-module claims conformance.**

ACE_CCL.1-1 The evaluator ***shall check*** that the conformance claim contains a CC conformance claim that identifies the version of the CC to which the PP-module claims conformance.

131 The evaluator determines that the CC conformance claim identifies the version of the CC that was used to develop this PP-module. This should include the version number of the CC and, unless the International English version of the CC was used, the language of the version of the CC that was used.

ACE_CCL.1.2C The CC conformance claim shall describe the conformance of the PP-module to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ACE_CCL.1-2 The evaluator ***shall check*** that the CC conformance claim states a claim of either CC Part 2 conformant or CC Part 2 extended for the PP-module.

ACE_CCL.1.3C The conformance claim shall identify all security functional requirement packages to which the PP-module claims conformance.

APE_CCL.1-4 The evaluator ***shall examine*** the CC conformance claim for CC Part 2 to determine that it is consistent with the extended components definition.

132 If the CC conformance claim contains CC Part 2 conformant, the evaluator determines that the extended components definition does not define functional components.

133 If the CC conformance claim contains CC Part 2 extended, the evaluator determines that the extended components definition defines at least one extended functional component.

ACE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ACE_CCL.1-4 The evaluator ***shall examine*** the CC conformance claim for CC Part 2 to determine that it is consistent with the extended components definition.

134 If the CC conformance claim contains CC Part 2 conformant, the evaluator determines that the extended components definition does not define functional components.

135 If the CC conformance claim contains CC Part 2 extended, the evaluator determines that the extended components definition defines at least one extended functional component.

4.1.3 PP-module security problem definition (ACE_SPD)

(All content and presentation elements of APE_SPD.12 evaluation methodology hold).

4.1.4 PP-module security objectives (ACE_OBJ)

(All content and presentation elements of APE_OBJ.2 2 evaluation methodology hold).

4.1.5 PP-module security functional requirements (ACE_REQ)

(All content and presentation elements of APE_REQ.2 evaluation methodology hold without considering the SAR part which is empty in PP-modules).

4.1.6 PP-module consistency (ACE_MCO)

4.1.6.1 Evaluation of sub-activity (ACE_MCO.1)

4.1.6.1.1 Objectives

136 The objective of this sub-activity is to determine the consistency of the PP-module regarding its base-PP(s).

4.1.6.1.2 Input

137 The evaluation evidence for this sub-activity is:

1. the PP-module;
2. its base-PP(s).

4.1.6.2 Action ACE_MCO.1.1E

ACE_MCO.1.1C The consistency rationale shall demonstrate that the TOE type of the PP-module is consistent with the TOE type(s) in the base-PPs identified in the PP-module introduction.

ACE_MCO.1-1 The evaluator ***shall examine*** the consistency rationale to determine that the TOE type of the PP-module is consistent with all the TOE types of the base-PP(s).

138 The relation between the types may be simple: a PP-module may consider a TOE that provides additional security functionality regarding, or more complex: a TOE that provides a given security functionality in a specific way.

ACE_MCO.1.2C The consistency rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the base-PPs identified in the PP-module introduction.

ACE_MCO.1-2 The evaluator shall examine the PP-module consistency rationale to determine that it demonstrates that the statement of security problem definition of the PP-module is consistent with the statements of security problem definition stated in its base-PPs.

139 In particular, the evaluator examines the consistency rationale to determine that:

1. the statements of threats, assumptions and OSPs in the PP-module do not contradict those from the base-PP(s).

2. the statement of assumptions in the PP-module addresses aspects out of scope of the base-PP, in which case, the addition of elements is allowed.

ACE_MCO.1.3C **The consistency rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the base-PPs identified in the PP-module introduction.**

ACE_MCO.1-3 The evaluator ***shall examine*** the consistency rationale to determine that the statement of security objectives of the PP-module is consistent with the statement of security objectives of its base-PP(s).

140 In particular, the evaluator examines the consistency rationale to determine that:

1. the statements of the security objectives for the TOE and the security objectives for the operational environment in the PP-module do not contradict those from the base-PPs.

2. the statement of the security objectives for the operational environment in the PP-module addresses aspects out of scope of the base-PP, in which case, the addition of elements is allowed.

ACE_MCO.1.4C **The consistency rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the base-PPs identified in the PP-module introduction.**

ACE_MCO.1-4 The evaluator ***shall examine*** the consistency rationale to determine that the statement of security requirements of the PP-module is consistent with the statement of security requirements of its base-PPs, that is, the SFRs of the PP-module either complete or refine the SFRs of the base-PP(s) and that no contradiction arises from the whole set of SFRs of the PP-module and the base-PP(s).

4.1.7 PP-configuration consistency (ACE_CCO)

4.1.7.1 Evaluation of sub-activity (ACE_CCO.1)

4.1.7.1.1 Objectives

141 The objective of this sub-activity is to determine whether the PP-configuration and its components are correctly identified.

142 The objective of this sub-activity is also to determine the consistency of the PP-configuration regarding the whole set of protection profiles and PP-modules.

143 For the consistency analysis required by this activity, the application notes of the CEM, Section 9.2.1 (Re-using the evaluation results of certified PPs), is applicable to determine which parts of the base-PPs are to be re-evaluated during the evaluation of PP-configuration

4.1.7.1.2 Input

144 The evaluation evidence for this sub-activity is:

1. the PP-configuration reference;
2. the PP-configuration components statement;
3. the PP(s) and PP-modules identified in the components statement.

4.1.7.2 Action ACE_CCO.1.1E

ACE_CCO.1.1C The PP-configuration reference shall uniquely identify the PP-configuration.

ACE_CCO.1-1 The evaluator ***shall examine*** the PP-configuration reference to determine that it uniquely identifies the PP-configuration.

145 The evaluator determines that the PP-configuration reference identifies the PP-configuration itself, so that it may be easily distinguished from other PPs, PP-configurations and PP-modules, and that it also uniquely identifies each version of the PP-configuration, e.g. by including a version number and/or a date of publication.

146 The PP-configuration should have some referencing system that is capable of supporting unique references (e.g. use of numbers, letters or dates).

ACE_CCO.1.2C The components statements shall uniquely identify the protection profiles and the PP-modules that compose the PP-configuration.

ACE_CCO.1-2 The evaluator ***shall examine*** the PP-configuration components statement to determine that it uniquely identifies the protection profiles and PP-modules contained in the PP-configuration.

147 The protection profiles should have been certified and available for use in security targets.

ACE_ CCO.1.3C The conformance statement shall specify the kind of conformity of the PP-configuration, either strict or demonstrable.

ACE_CCO.1-3 The evaluator ***shall examine*** the PP-configuration conformance statement to determine that it specifies the kind of conformity required: strict or demonstrable.

148 If at least one of the protection profiles identified in the PP-configuration components statement claims strict conformance, then the PP-configuration conformance claim has to state strict conformance also.

ACE_ CCO.1.4C The *SAR statement* shall specify the set of SAR or predefined EAL that applies to this PP-configuration.

ACE_CCO.1-4 The evaluator ***shall examine*** the PP-configuration SAR statement to determine that it specifies a well-formed package of SAR. The SAR package can be build in with components from CC Part 3 or can refer to a specific SAR package stated in one of the protection profiles composing the PP-configuration.

149 If the set of SAR comes from CC Part 3 then the evaluator shall check that it is well-formed: it is closed by dependencies or the SAR statements provide a sound discarding rationale.

150 The evaluator shall check that the set of SAR of the PP-configuration is consistent with respect to the SARs of each of the protection profiles contained in the PP-configuration: for any SAR component in each of the Protection Profile, the PP-configuration provides either the same component or a higher component in the family hierarchy. If the SAR component in the protection profile is a refinement of a standard component, then the correspondent SAR component in the PP-configuration has to include these refinements. If two protection profiles refine the same SAR component, the evaluator shall check that the refinements are not contradictory and that the corresponding SAR component in the PP-configuration meets both.

ACE_CCO.1.5C The base-PP(s) on which the PP-module relies shall belong to the protection profiles identified in the *components statement* of the PP-configuration.

ACE_CCO.1-2 The evaluator ***shall check*** that the base-PP(s) of the PP-module are included in the set of PP(s) selected for the PP-configuration.

4.1.7.3 Action ACE_CCO.1.2E

ACE_CCO.1-5 The evaluator shall check that the PP-configuration made up of all the protection profiles and PP-modules identified in the components statement of the PP-configuration is consistent. That is, the evaluator shall check that no contradiction arises from the whole set of protection profiles and PP-modules included in the PP-configuration.

151 The evaluator can organise this work in many ways; the actual organisation may depend on the will to derive evaluation results for more than one PP-configuration at a time.

152 For instance, the evaluator can process in two steps as follows:

1. Assess the consistency of the set of protection profiles composing the PP-configuration,

2. Then proceed with the assessment of the PP-configuration consistency incrementally, by adding one PP-module at a time.

153 An alternative is to proceed incrementally but mixing PPs and PP-modules or to flatten the definition of the PP-configuration (cf. section 2.6) and to assess the consistency of the whole set of elements.

154 Any incremental consistency analysis step where C is a subset of the PP-configuration and X is a PP or a PP-module that has to be added to C consists in:

- assessing that the SPD, the objectives and the SFRs of X do not contradict the statements in C;

- the assumptions and objectives for the environment in X either are the same as in C or address security aspects that are out of the scope of C.

155 Note that if X is a PP-module, C contains all its base-PP(s) and ACO_MCO.1 has succeed for X, then the consistency analysis step has to be performed with respect to the components of C different from these base-PP(s) only.

4.2 Class ASE: Security target evaluation

156 The evaluation methodology of ASE_CCL.1 applies to PP-configurations. Indeed, in order to assess the conformity of a security target to a PP-configuration, the PP-configuration has to be interpreted as a standard PP, following guidance given in 2.6.