Common Criteria

CC and CEM addenda

Exact Conformance, Selection-Based SFRs, Optional SFRs

Maintained by: CCDB
Unique Identifier: 013
Version: 2.0
Status: Final
Date of issue: 2021-Sep-30
Approved by: CCMC

Foreword

This is addenda to 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. As the implementation cycle for the next draft of the Common Criteria is significant, these addenda are an update to the *Exact Conformance, Selection-Based SFRs, Optional SFRs* addenda, version 0.5, dated May 2017. It incorporates feedback from trial use of the May 2017 addenda, as well as discussions of the expert group implementing ISO/IEC 15408 and 18045, which will be the next published version of the Common Criteria and Common Evaluation Methodology.

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

Technical Editor: NIAP

Document History:

V1.0, May 2017 : Initial release.

V2.0, Sep 2021: Update to incorporate trial use feedback, ISO expert feedback

Field of special use: None

Table of Contents

Table of contents

1 Introduction

1.1 Executive Summary

1 The updated CCRA introduces the cPPs as a mechanism that may be used by procurement bodies to specify their security needs. The specific cPP-related requirements in the CCRA annex K.3 can be paraphrased as: CCRA certificates that claim conformance to a cPP shall cover only the assurance requirements defined in the cPP and related Supporting Documents, and express only the security functional requirements defined in the cPP.

2 This motivates an addition to the existing strict and demonstrable types of conformance of an ST to a PP: the notion of 'exact conformance' to address the requirements stated above.

3 Unlike with strict/demonstrable conformance, an ST author claiming exact conformance to a PP cannot add or change requirements (i.e., SFRs, SARs) at their discretion. The set of requirements (SFRs and SARs) that can be used in an "exactly conformant" ST is defined in the PP or by a PP-Configuration. This type of conformance ensures that only SFRs that have been chosen and agreed to by the PP or PP-Module authors (e.g., an iTC) are included in conformant STs.

4 With the growing complexity and variety of security functionality, a given implementation may contain features that are germane to the general security problem or technology area that a cPP describes, but is not supported or addressed on all implementations of that technology. In these cases, it is desirable to express that functionality as an allowed option, where both the SFR(s) that describe the functionality as well as any associated Evaluation Activity are included in the PP, but do not have to be selected by an ST author in order to be conformant to the PP. These addenda therefore also define the notion of Optional Requirements that can be chosen by an ST author. Optional Requirements are SFRs that the ST author has the option to include or not include while maintaining adherence to exact conformance. Optional requirements can either be elective or conditional. An elective optional SFR is one that can be included or excluded from the set of requirements in the ST regardless of the functionality implemented by the TOE. A conditionally optional requirement is one that must be included in the set of requirements in the ST if the TOE implements that functionality. This allows flexibility that otherwise would not be possible in a PP or PP-Module with an exact conformance type specified in its conformance statement.

5 Certain SFRs have selections specifying a capability that, in turn, may require a complex and potentially insecure implementation. Including all of the requirements for such complex functionality inside the selection can lead to an unwieldy and unintelligible requirement; therefore, these addenda also define the notion of Selection-based Requirements that an ST author must include in a conformant ST if certain selections are made.

6 Experience in writing and using functional packages has pointed out a need for a third type of package conformance claim that allows selections in SFRs contained in a package to be added and deleted when instantiated in PPs and PP-Modules—this type of operation is not supported in the existing <package name>-conformant and <package-name>-augmented claims. The third type--<package name>-tailored—is defined in these addenda to support the necessary operations on the functional package SFRs.

7 Exact conformance does not replace nor prevent strict or demonstrable conformance from being a valid conformance statement for PPs.

8 Exact Conformance needs to be accounted for when constructing PP-Configurations, and when evaluating TOEs against PP-Configurations. These addenda provide clarification of modular requirements constructs and rules to precisely capture how to implement the Exact Conformance concept for these constructs.

9 The framework to support Exact Conformance statements, Selection-Based SFRs, and Optional SFRs is defined in Chapter 2 of this document. The additions required to CC Part 3 Assurance Requirements are defined and Chapter 3, and the evaluation methodology additions are presented in Chapter 4. Because the changes are intertwined with existing CC constructs, the presentation in the addenda show changes to the existing CC (rev 5) text in context (changes delineated in red text), rather than having solely stand-alone text.

1.2 Scope

10 This document extends the Common Criteria (CC) framework for the definition and application of "Exact Conformance" to a Protection Profile and PP-Configuration; the definition and use of Selection-Based Security Functional Requirements (SFRs); the definition and use of Optional SFRs; and the definition and use of <package name>-tailored functional package conformance. It is to be used as a complement to CC Parts 1 and 3, and the CEM, for the production and evaluation of protection profiles that include functional packages, Selection-Based SFRs, Optional SFRs, and require Exact Conformance.

1.3 Audience

11 This document is intended for PP/PP-Module authors, ST authors, and evaluators.

1.4 Normative References

12 The following references apply to this document.

13 [CC-1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 1: Introduction and general model. CCMB-2017-04-001.

14 [CC-2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 2: Security functional components. CCMB-2017-04-002.

15 [CC-3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. Part 3: Security assurance components. CCMB-2017-04-003.

16 [CEM] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 5, April 2017. Evaluation methodology. CCMB-2017-04-004.

1.5 Terms and definitions

(augments [CC-1], Section 4.1)

17 For the purpose of this document, the following terms and definitions apply. These terms should be considered as included in the list of terms in [CC-1], Section 4.1.

18 **Base PP-Module** – PP-Module specified in a different PP-Module used as a basis to build a Protection Profile Configuration

19 Note that specifying a base PP-Module in a PP-Module implicitly includes the base PP-Module's PMB.

20 **Base Protection Profile (base PP)** – Protection Profile specified in a PP-Module used as a basis to build a Protection Profile Configuration

21 **exact conformance** – hierarchical relationship between a PP or PP-Configuration and a ST where all the requirements in the ST are drawn only from the PP/PP-Configuration

22 **Protection Profile Configuration (PP-Configuration)** – ~~Protection Profile~~ implementation independent statement of security needs ~~composed of~~ for a TOE type contained in either two or more PPs, or one or more PP-Modules (and the associated PP-Module Bases (PMBs)) and, optionally, one or more PPs that are not base PPs for any PP-Module included. ~~Base Protection Profiles and Protection Profile Module~~

23 **PP-Configuration component** – a Protection Profile or PP-Module included in a PP-Configuration

24 **Protection Profile Module (PP-Module)** – implementation-independent statement of security needs for a TOE type complementary to one or more PP-Module Bases (PMBs) ~~Protection Profiles~~

25 Protection Profile Module Base (PMB) – set of base PP-Modules and base PPs specified by a PP-Module as a basis for building a PP-Configuration

26 The notion of a PMB is iterative in that the base of a PP-Module can be another PP-Module with its own base, with that base being a PP-Module with yet

another a PP-Module with its own base, etc. However, this “chain” terminates with the a PP-Module that has (at least one) PP as its base.

27 **optional Security Functional Requirement** – SFR in a PP, PP-Module, or functional package that either may be included in a conformant ST at the election of the ST author, or is to be included in a conformant ST if the TOE implements the functionality to which the SFR pertains

28 An optional SFR can contribute to the SPD stated in the PP, PP-Module, or functional package, or it may define appropriate SPD elements to be included when the optional SFR is included.

29 **selection-based Security Functional Requirement** – SFR in a PP, PP-Module, or functional package that contributes to a stated aspect of the PP’s, PP-Module’s, or functional package’s SPD that is to be included in a conformant ST if a selection choice identified in the PP/PP-Module/functional package indicates that it has an associated selection-based SFR

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

31 Note that such tailoring is considered only in the context of one package and is not considered in the context with other packages, PPs, or PP-Modules

32 Also note that the selections in the SFR may be replaced by the additional selections. Additionally, selections can only be added for packages claimed by PPs or PP-Modules. STs cannot claim <package-name>-tailored conformance to the package.

2 Addendum to CC Part 1

33 The additions required to support the concepts of exact conformance, selection-based SFRs, optional SFRs, and <package name>-tailored functional package conformance require changes throughout Part 1 of the CC. Some of the changes are related to more than one of the constructs that are being introduced, so this chapter is structured as changes to [CC-1] in sequential order.

2.1 Changes to *8.1.3, The selection operation*

(augments [CC-1], Section 8.1.3; the entire section is repeated below for context and ease of application, with the changes highlighted.)

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

35 Whenever an element in a PP contains a selection, the PP author may do one of three things:

a) leave the selection uncompleted.

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

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

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

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

38 A PP, PP-Module, or functional package may define a set of SFRs called selection-based SFRs. A set of SFRs is associated with a selection in another SFR in the PP, PP-Module, or functional package. These SFRs must be included in a PP, PP-Module, or ST if 1) a selection choice identified in the PP, PP-Module, or functional package indicates that it has an associated selection-based SFR and 2) that selection is made by the PP, PP-Module, or ST author. For a) above, a PP/PP-Module author would leave the list of selection-based SFRs unchanged. For c) above, a PP/PP-Module author would remove any selection-based SFRs from the list that correspond to the choices removed. For b) above, PP, PP-Module, and ST authors would include the appropriate selection-based SFRs in the list of SFRs for the PP/ST.

2.2 Changes to *9.2, Packages*

(changes [CC-1], Section 9.2; the first three paragraphs are repeated below for context and ease of application, with the changes highlighted.)

39 A package is a named set of security requirements. A package is either

40 - a functional package, containing only SFRs, and optionally SDP elements and objectives, or

41 - an assurance package, containing only SARs.

42 Mixed packages containing both SFRs and SARs are not allowed.

43 A package can be defined by any party and is intended to be re-usable. To this goal it should contain requirements that are useful and effective in combination. Packages can be used in the construction of larger packages, PPs, PP-Modules, and STs. At present there are no criteria for the evaluation of packages, therefore any set of SFRs or SARs can be a package.

2.3 Changes to *9.3, Protection Profiles*

(changes [CC-1], Section 9.3; the entire section is repeated below for context and ease of application, with the changes highlighted.)

44 Whereas an ST always describes a specific TOE (e.g. the MinuteGap v18.5 Firewall), a PP is intended to describe a TOE type (e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations. A detailed description of PPs is given in Annex **Fout! Verwijzingsbron niet gevonden.**.

45 In general an ST describes requirements for a TOE and is written by the developer of that TOE, while a PP describes the general requirements for a TOE type, and is therefore typically written by:

- A 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;
- A government or large corporation specifying its requirements as part of its acquisition process.

46 The PP determines the allowed type of conformance of the ST to the PP. That is, the PP states (in the PP conformance statement, see section **Fout! Verwijzingsbron niet gevonden.**) what the allowed types of conformance for the ST are:

- if the PP states that exact conformance is required, the ST shall conform to the PP in an exact manner;
- if the PP states that strict conformance is required, the ST shall conform to the PP in an exact or strict manner;

- if the PP states that demonstrable conformance is required, the ST shall conform to the PP in an exact, strict, or demonstrable manner.

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

48 While in general a PP can claim conformance to one or more PPs, because of the nature of exact conformance it does not make sense for one PP to be exactly conformant to another PP, and so a PP cannot claim exact conformance to another PP. If an ST claims exact conformance to multiple PPs, this is allowed, but in this case all PPs must require exact conformance in their conformance statement, and all PPs must list the other PPs in their allowed-with statement.

49 See Annex D for additional information.

50 In cases where one or more PPs do not require exact conformance, if an ST claims conformance to multiple PPs, it shall conform (as described above) to each PP in the manner ordained by that PP; that is, either strictly or demonstrably. This may mean that the ST conforms strictly to some PPs and demonstrably to other PPs.

51 Note that either the ST conforms to the PP in question or it does not. The CC does not recognise “partial” conformance. It is therefore the responsibility of the PP author to ensure the PP is not overly onerous, prohibiting PP/ST authors in claiming conformance to the PP.

52 An ST is equivalent or more restrictive than a PP if:

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

or, informally, the ST shall levy the same or more, restrictions on the TOE and the same or less restrictions on the operational environment of the TOE.

53 This general statement can be made more specific for various sections of the ST:

a) **Security problem definition**: The conformance rationale in the ST shall demonstrate that the security problem definition in the ST is equivalent (or more restrictive) than the security problem definition in the PP. This means that:

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

b) **Security objectives**: The conformance rationale in the ST shall demonstrate that the security objectives in the ST is equivalent (or more restrictive) than the security objectives in the PP. This means that:

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

54 If exact conformance for protection profiles is specified then the following requirements apply:

a) **Security problem definition**:

- The ST shall contain the security problem definition of the PP including all threats, assumptions, and OSPs. It shall not include any threats, assumptions, or OSPs that are not present in the PP.

b) **Security objectives**: The ST:

- shall contain all security objectives for the TOE of the PP and may not specify additional security objectives for the TOE that are not present in the PP;
- shall contain all security objectives for the operational environment as defined in the PP and may not specify additional security objectives for the operational environment that are not present in the PP.

c) **Security requirements**: The ST shall contain all SFRs and SARs present in the PP, with the following exceptions:

- SFRs designated as optional SFRs in the PP (see Section B.9) may be excluded in an exactly conformant ST;
- SFRs designated as selection-based SFRs in the PP (see Sections 8.1.3 and B.9) must be excluded if the selection that requires their inclusion is not chosen by the ST author.

55 If strict conformance for protection profiles is specified then the following requirements apply:

a) **Security problem definition**:

- The ST shall contain the security problem definition of the PP and may specify additional threats and OSPs; it shall contain all assumptions as defined in the PP, with two possible exceptions as explained in the next two bullets;
- an assumption (or a part of an assumption) specified in the PP may be omitted from the 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 ST;
- a new assumption may be added in the 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;

b) **Security objectives**: The 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 objectives for the operational environment in the PP are security objectives for the TOE in the ST. This is called re-assigning a security objective. If a security objective is re-assigned to the TOE the security objectives rationale has to make clear which assumption or part of the assumption may not be necessary any more;
- may specify additional 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

c) **Security requirements**: The ST shall contain all SFRs and SARs in the PP, but may claim additional or hierarchically stronger SFRs and SARs. The completion of operations in the ST must be consistent with that in the PP; either the same completion will be used in the ST as that in the PP or one that makes the requirement more restrictive (the rules of refinement apply).

56 If demonstrable conformance for protection profiles is specified then the following requirements apply:

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

- 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.

57 PP evaluation is optional. Evaluation is performed by applying the APE criteria to them as listed in CC Part 3. The goal of such an evaluation is to demonstrate that the PP is complete, consistent, and technically sound and suitable for use as a template on which to build another PP or an ST.

58 Basing a PP/ST on an evaluated PP has two advantages:

- There is much less risk that there are errors, ambiguities or gaps in the PP. If any problems with a PP (that would have been caught by evaluating that PP) are found during the writing or evaluation of the new ST, significant time may elapse before the PP is corrected.

- Evaluation of the new PP/ST may often re-use evaluation results of the evaluated PP, resulting in less effort for evaluating the new PP/ST.

2.4 Changes to *9.5, Using Multiple Protection Profiles*

(augments [CC-1], Section 9.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

59 The CC also allows PPs to conform to other PPs (with the exception that a PP cannot claim exact conformance to other PPs), allowing chains of PPs to be constructed, each based on the previous one(s).

60 For instance, one could take a PP for an Integrated Circuit and a PP for a Smart Card OS, and use these to construct a Smart Card PP (IC and OS) that claims conformance to the other two. One could then write a PP on Smart Cards for Public Transport based on the Smart Card PP and a PP on Applet Loading. Finally, a developer could then construct an ST based on this Smart Cards for Public Transport PP.

2.5 Changes to *9.6, Protection Profiles, PP-Modules and PP-Configurations*

(changes [CC-1], Section 9.6; the entire section is repeated below for context and ease of application, with the changes highlighted.)

61 **9.6.1 Introduction**

62 To allow the definition of requirements in a modular ~~Protection Profiles~~ fashion that address a TOE's optional ~~TOE's~~ 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.

63 9.6.2 PP-Modules

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

65 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.

66 Each PP-Module refers to a ~~at least one~~ PP-Module Base (PMB). A PMB ~~Base Protection Profile (or Base-PP) that~~ provides the definition of the TOE type and the mandatory requirements to fulfill. The PP-Module specifies the modified TOE type, complements these requirements and has to be used with the PMB ~~Base-PPs~~: a PP-Module may introduce new elements to those in the PMB, ~~the Base-PPs~~ and may also refine or interpret some of the elements ~~of~~ in the ~~Base-PPs~~ PMB.

67 A PMB consists of

68 - One or more PPs (these are called “base PPs”)

69 - One or more PP-Modules (and their associated PMBs; these PP-Modules are referred to as “base PP-Modules”)

70 - A combination of PPs and PP-Modules (and their associated PMBs)

71 If the PP-Module refers to several base PPs and/or base PP-Modules ~~Base Protection Profiles~~, this set of ~~Base-PPs~~ base PPs/base PP-Modules have to be used simultaneously for the evaluation and usage of the PP-Module.

72 The PP-Module can also refer to alternative PMBs ~~sets of Base-PPs~~, in the case the PP-Module could comply with alternative PMBs ~~Base-PPs~~ depending of the usage.

73 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 one PMB. ~~its mandatory Base-PPs.~~

74 9.6.3 PP-Configurations

75 A PP-Configuration results from some ~~the~~ combination of ~~at least one~~ PP-Modules (and their PMBs) and ~~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~~.

76 ~~A~~ To be more specific, a PP-Configuration can consist of:~~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.~~

77 - Two or more PPs (and no PP-Modules), or

78 - One or more PP-Module (and the associated PMB(s)), and, optionally, one or more PPs that are not associated with a PP-Module.

79 If a ~~the~~ PP-Module defines alternative PMBs ~~sets of Base-PPs~~, only one of ~~these sets~~ PMBs must be used in the PP-Configuration.

80 309 A PP-Configuration holds a unique reference and identifies all of its ~~the PP~~ components: any PP-Modules, selected PMBs for any PP-Modules, and any PPs not associated with PP-Modules in the PP-Configuration~~ Base-PPs and selected PP-Modules~~.

~~81 A PP-Configuration can only combine certified Base-PPs to PP-Modules.~~

82 Evaluation rules for PP-Configurations are similar, but not identical, to the ones for ~~standard~~ PPs. These rules are described in Class ACE, in CC Part 3.

83 9.6.4 Using PP-Modules and PP-Configurations in security targets

84 PP-Modules are used to build specific PP-Configurations on top of one or more PMBs ~~Base-PPs~~. PP-Modules cannot be specified by themselves by a ST; they are used in Security Targets only as part of well-identified PP-Configurations.

85 ~~PP-Configurations are used like Protection Profiles. ~~A Security Target can claim conformity to a single 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. Unlike the case with PPs, an ST can claim conformance to only one PP-Configuration.

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

87 - Independently of any product evaluation, or

88 - 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.

89 In practice, a ST that claims conformance with a non-certified PP-Configuration can still be evaluated with a conformance claim against the Base-PP 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 Base-PP, proper to the TOE.

2.6 Changes to *10.1, Introduction*

(changes [CC-1], Section 10.1, paragraph 320; the changes are highlighted.)

90 STs may be based on packages, evaluated PPs/PP-Configurations or non-evaluated PPs/PP-Configurations - however this is not mandatory, as STs do not have to be based on anything at all.

2.7 Changes to *10.5, Conformance Claim*

(changes [CC-1], Section 10.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

91 The conformance claim indicates the source of the collection of requirements that is met by a PP, PP-Module, or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

d) describes the version of the CC to which the PP, PP-Module, or ST claims conformance.

e) describes the conformance to CC Part 2 (security functional requirements) as either:

   - **CC Part 2 conformant** - A PP, PP-Module, or ST is CC Part 2 conformant if all SFRs in that PP, PP-Module, or ST are based only upon functional components in CC Part 2, or
   - **CC Part 2 extended** - A PP, PP-Module, or ST is CC Part 2 extended if at least one SFR in that PP, PP-Module, or ST is not based upon functional components in CC Part 2.

f) describes the conformance to CC Part 3 (security assurance requirements) as either:

   - **CC Part 3 conformant** - A PP, PP-Module, or ST is CC Part 3 conformant if all SARs in that PP, PP-Module, or ST are based only upon assurance components in CC Part 3, or
   - **CC Part 3 extended** - A PP, PP-Module, or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

92 Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- *Package name Conformant* - A PP, PP-Configuration, PP-Module, or ST is conformant to a pre-defined package (e.g. EAL) if:
   - the SFRs of that PP, PP-Configuration, PP-Module, or ST are identical to the SFRs in the package, or
   - the SARs of that PP, PP-Configuration, PP-Module, or ST are identical to the SARs in the package.
- *Package name Augmented* - A PP, PP-Configuration, PP-Module, or ST is an augmentation of a predefined package if:
   - the SFRs of that PP, PP-Configuration, PP-Module, or ST contain all SFRs in the package, but have at least one additional

SFR or one SFR that is hierarchically higher than an SFR in the package.

- the SARs of that PP, PP-Configuration, PP-Module, or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

– *Package name Tailored* - A PP or PP-Module claims tailoring of a predefined functional package if:

- all constituent parts (SPD, Security Objectives, and SFRs) of that PP/PP-Module 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.

- the package contains no SARs.

93 When an ST claims conformance to a PP or PP-Configuration, it only claims conformance to packages that are claimed by the PP/PP-Configuration component if the ST augments the package over what is claimed by the PP/PP-Configuration. An ST cannot make a claim of <package name>-tailored under any conditions. A PP-Configuration itself cannot make any functional package conformance claims; all functional package conformance claims are associated with the PP-Configuration's components.

94 If the PP/PP-Configuration requires exact conformance in its conformance statement, an ST can make no package conformance claims of any kind.

95 Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

96 Finally, the conformance claim may also include two statements with respect to Protection Profiles:

a) *PP Conformant* - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.

b) *Conformance Statement* (Only for PPs and PP-Modules) - This statement describes the manner in which PPs, PP-Configurations, or STs must conform to this PP: exact, strict, or demonstrable. For exact conformance, the statement also includes an "allowed-with statement" that lists

- For PPs, the PPs allowed to be used (in an exact conformance claim by an ST or in a PP-Configuration with exact conformance type) with the PP, and PP-Modules that may be used in a PP-Configuration with this PP.

- For PP-Modules, the PPs (not in its PMB) and PP-Modules (not in its PMB) that are allowed to be used (in an exact conformance claim) with the PP-Modules in a PP-Configuration.

For more information on this Conformance Statement, see Annex **Fout! Verwijzingsbron niet gevonden.**.

97 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, one of exact, strict, or demonstrable, that meet the conformance statements of the ~~Base PP(s)~~PP-Configuration's components,

– if any component of a PP-Configuration has a conformance statement that requires exact conformance, then all components in that PP-Configuration must have conformance statements of exact conformance; all PPs must list all other PPs in their respective allowed-with statements; all PP-Modules must list all other PP-Modules and PPs not in the PMB in their allowed-with statement; and all PPs must list all PP-Modules in the PP-configuration in their allowed-with statements.

– an ST may claim conformance with exactly one ~~or more~~ PP-Configuration~~s~~.

2.8 Changes to *A.2, Mandatory contents of an ST*

(augments [CC-1], Section A.2, paragraph 344, item b and Figure 5.)

98 *Item b is updated as follows:*

99 b) a conformance claim, showing whether the ST claims conformance to any PPs/PP-Configurations and/or packages, and if so, to which PPs/PP-Configurations and/or packages;

100 *Figure 5 is updated to include* "PP-Configuration claim" below "PP-Claim" in the call-out for the Conformance Claims section of the figure.

2.9 Changes to *A.5, Conformance Claims (ASE_CCL)*

(augments [CC-1], Section A.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

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

– Part 2 and Part 3 of this International Standard;

– Protection Profiles (if any);

- A PP-Configuration (if any);
- Packages (if any).

102 The description of how the ST conforms to the CC consists of two items: the version of the CC that is used and whether the ST contains extended security requirements or not (see Section A.8).

103 The description of conformance of the ST to Protection Profiles means that the ST lists the Protection Profile(s) ~~packages~~ that conformance is being claimed to. For an explanation of this, see Section 10.5.

104 The description of conformance of the ST to a PP-Configuration means that the ST lists the PP-Configuration that conformance is being claimed to. For an explanation of this, see Section 10.5.

105 The description of conformance of the ST to packages means that the ST lists the packages that conformance is being claimed to. For an explanation of this, see Section 10.5.

~~106 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.~~

2.10 Changes to *A.9.1, Security functional requirements (SFRs)*

(augments [CC-1], Section A.9.1; the entire section is repeated below for context and ease of application, with the changes highlighted.)

107 The SFRs are a translation of the security objectives for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed) and be independent of any specific technical solution (implementation). The CC requires this translation into a standardised language for several reasons:

- to provide an exact description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a more exact description of the functionality of the TOE.
- to allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison.

108 The SFRs specified in an ST depend on the SFRs specified in the PP/PP-Configuration, as well as the conformance statement of the PP/PP-Configuration as outlined in Annex D. All optional and selection-based SFRs from the PP/PP-Configuration the ST claims are included in this section.

109 If the ST claims conformance to a PP or PP-Configuration, and the PP or the components of the PP-Configuration contain optional requirements, the ST may instantiate these requirements, being sure to include any required SPD-elements associated with those requirements, and complying with the categorization of the optional requirements in the PP, PP-Module, or package (elective or conditional). This may be done regardless of the conformance required by the PP or PP-Configuration. Omitting optional SFRs in a ST does not constitute "partial conformance" to a PP or PP-Configuration, and thus is allowed.

110 There is no translation required in the CC for the security objectives for the operational environment, because the operational environment is not evaluated and does therefore not require a description aimed at its evaluation. See the bibliography for items relevant to the security assessment of operational systems.

111 It may be the case that parts of the operational environment are evaluated in another evaluation, but this is out of scope for the current evaluation. For example: an OS TOE may require a firewall to be present in its operational environment. Another evaluation may subsequently evaluate the firewall, but this evaluation has nothing to do with the evaluation of the OS TOE.

2.11 Changes to *B.2, Mandatory contents of a PP*

(changes [CC-1], Section B.2, paragraph 444; only item "f", security requirements, *is changed as indicated below)*

f) *security requirements*, where a translation of the security objectives for the TOE into a standardised language is provided. This standardised language is in the form of SFRs. The set of SFRs includes optional and selection-based SFRs. Additionally this section defines the SARs;

2.12 Changes to *B.5, Conformance claims (APE_CCL)*

(changes [CC-1], Section B.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

112 This section of a PP describes how the PP conforms with other PPs and with packages. It is identical to the conformance claims section for an ST (see Section **Fout! Verwijzingsbron niet gevonden.**), with one exception: the conformance statement.

113 The conformance statement in the PP states how STs and/or other PPs must conform to that PP. The PP author selects whether "exact", "strict", or "demonstrable" conformance is required. If "exact" conformance is selected, the PP author also has the option of specifying the following information in an "allowed-with" statement:

114 A) Other PPs to which an ST can claim conformance to in combination with the subject PP and still maintain exact conformance. Note this combination

of PPs can be claimed directly in an ST, or be in a PP-Configuration that the ST claims conformance to.

115 B) PP-Modules that can specify the subject PP in its PMB for use with that PP-Module in a PP-configuration.

116 See Annex **Fout! Verwijzingsbron niet gevonden.** for more details on this.

2.13 Changes to *B.9, Security requirements (APE_REQ)*

(changes [CC-1], Section B.9; the entire section is repeated below for context and ease of application, with the changes highlighted.)

117 This section is identical to the security requirements section of an ST as explained in Section **Fout! Verwijzingsbron niet gevonden.** with the exception of the specification of optional SFRs and selection-based SFRs as outlined below. Note however that the rules for completing operations in a PP are slightly different from the rules for completing operations in an ST. This is explained in more detail in Section **Fout! Verwijzingsbron niet gevonden.**.

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

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

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

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

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

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

2.14 Changes to *B.13, Interpretation of PP-Configuration as a standard PP*

(removes [CC-1], Section B.13)

124 *PP-Configurations are distinct from standard PPs. While both are methods to state sets of SFRs and SARs used to specify security functionality and assurance to which STs can claim conformance, there are structural differences—as well as differences in how they are constructed and evaluated—such that they should not be seen as equivalent. Therefore, these addenda remove Section B.13 from Part 1.*

2.15 Changes to *B.14, Specification of PP-Modules*

(changes [CC-1], Section B.14; this is a general change throughout B.14 to avoid a minor, but pervasive, editorial change being repeated continually in these addenda.)

125 *When issued, the modular requirements construction section only allowed the specification of PPs as the base for a PP-Module. As noted above, these addenda allow the specification of PP-Modules in addition to PPs as a base for a PP-Module, and the term "PP-Module Base" (PMB) is introduced by these addenda to reflect this. Throughout this section, the term "Base-PP" is used to specify the base for a PP-Module. This clause changes the term "Base-PP" to "PMB) throughout section B.14 unless otherwise specifically noted in other sections of this addenda.*

2.16 Changes to *B.14.1, Mandatory content of a PP-Module*

(changes [CC-1], Section B.14.1 and Figure 11; the entire section is repeated below for context and ease of application, with the changes highlighted.)

126 *Figure 11 is modified in two ways. 1)* "Base-PP identification" *in the call-out for PP-Module Introduction is changed to* "PP-Module Base (PMB) Identification". *2) In the call-out for Conformance claims, add* "package claim" *after* "CC Conformance claim".

127 The content of the PP-Module is summarized below and explained in detail in sections from B.14.3 to B.14.10. A PP-Module contains:

128 - an *Introduction* that identifies the PP-Module, identifies the PP-Module Base(s) (PMB(s)) ~~Base-PP(s)~~ and states the correspondence rationale, and provides a description of the TOE within its environment that meets the descriptions underlying the PMBs ~~Base-PPs~~,

129 - a *Consistency rationale* that states the correspondence between the Module and its ~~Base-PP~~ PMB(s),

130 - a *Conformance claim* regarding the CC and packages, if any, along with inherited EAL and conformance statement,

131 - a *Security problem definition* with threats, assumptions and organisational security policies,

132 - a *Security objectives* section presenting the solution to the security problem in terms of objectives for the TOE and its operational environment,

133 - an optional *Extended functional components definition* where new functional components not included in CC Part 2 are introduced,

134 - a *Security functional requirements* section with a standardized statement of the TOE security objectives.

2.17 Changes to *B.14.3.2, Base-PP identification*

(changes [CC-1], Section B.14.3.2; the entire section is repeated below for context and ease of application, with the changes highlighted.)

135 B.14.3.2 ~~Base-PP~~ PMB identification

136 The PP-Module introduction identifies the PP-Module Base(s) (PMB(s)) ~~Base Protection Profile(s) the Module relies on~~. The identification consists of a list of ~~PP~~ references.

137 A PP-Module that requires to be used with a set of PP-Modules (and their PMBs) and Base-PPs simultaneously, say {B$_1$,...,B$_n$},will provide an identification list of the following form:

138 B~~PP~~$_1$ *AND* ... *AND* B~~PP~~$_n$ with n≥1

139 This set of PPs/PP-Modules must be closed, that is, for any PP-Module X that is in {B$_1$,...,B$_n$}, its own base PPs/PP-Modules must belong to the set {B$_1$ ... B$_n$}. This means that the set {B$_1$ ... B$_n$} must contain at least one Base-PP, because if the PP-Module had PP-Module X in its PMB, then PP-Module's X PMB would either have to be one or more Base-PPs, or another PP-Module with it's own PMB, which would eventually terminate in one or more Base-PPs.

140 It should also be noted that if the PMB identifies a PP-Module with alternative sets of PMBs (see below), the list should be annotated so that it is clear if there are any restrictions on the PMBs that are allowed to be used with that particular PP-Module.

141 The PP-Module may allow the use with alternative sets of ~~Base-PP~~PMBs, say {S$_1$,..., S$_k$}; in this case, the identification list states:

142 S$_1$ *OR* ... *OR* S$_k$, with k≥1

143 The general unfolded form of the identification of alternative sets of ~~Base-PP~~ PMBs is then:

144 *<formula below line 490 in [CC-1] deleted and replaced by:>*

145 $\{B_1,...,B_{n1}\}$ ... OR ... $\{B_1,...,B_{nk}\}$ with $k \geq 1$ and $ni \geq 1$

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

2.18 Changes to *B.14.5, Conformance claims*

(changes [CC-1], Section B.14.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

147 This section describes how the PP-Module conforms to:

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

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

149 A PP-Module inherits the conformity to SAR packages (including predefined EAL) from its PMB ~~the Base-PPs~~. The issue of PMBs with multiple components having ~~ANDed Base-PPs~~ ~~with~~ different SARs ~~EALs~~ has to be dealt with like in an ST conformant to all those components individually ~~PPs~~.

150 A PP-Module inherits the conformance statement (exact, strict, or demonstrable) from its PMB ~~the Base-PPs~~. The issue of PMBs with multiple components having ~~ANDed Base-PPs~~ ~~with~~ different conformance statements has to be dealt with like in an ST conformant to all those components individually ~~PPs~~.

151 Note that if one PMB component requires exact conformance, then it is not allowed to be combined with PMB components with other types of conformance.

152 If the PP-Module inherits a conformance claim from a PMB of exact conformance, then the PP-Module also may list in its allowed-with statement (contained in the conformance statement section) a set of other PP-Modules that are allowed to be specified in a PP-Configuration with that PP-Module (excluding PP-Modules that are in its PMB). This is to maintain the exact conformance concept of the authors of a set of requirements (in this instance, those that are in the PP-Module) having control over what other requirements are specified in combination with the requirements that they wrote when claiming conformance to that PP-Module. Similarly, the allowed-with statement will list any PPs that are not in its PMB that are allowed to be used in a PP-Configuration that requires exact conformance.

2.19 Changes to *B.14.9, Security functional requirements*

(augments [CC-1], Section B.14.9; the following text is added to the end of section B.14.9; that is, after paragraph 525. This makes the specification of optional and selection-based requirements consistent between PP-Modules and PPs.)

153 PP-Modules may specify optional SFRs and selection-based SFRs in the same manner as is done in PPs; see section B.9.

2.20 Changes to *B.15.1, Mandatory content of a PP-Configuration*

(changes [CC-1], Section B.15.1 paragraph 531; only the Components statement *and* Conformance Statement *items are changed as indicated below.)*

- a *Components statement* that identifies the non-Base PPs, 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 exact, strict, or demonstrable,

2.21 Changes to *B.15.2, Using the PP-Configuration*

(changes [CC-1], Section B.15.2; the entire section is repeated below for context and ease of application, with the changes highlighted.)

154 PP-Configurations are security statements that cover specific needs of groups of users, consumers, organisations, etc. A PP-Configuration is used by these groups to state their needs in a manner such that a conformant TOE will provide a solution for the stated need. An ST can claim conformance to a single PP-Configuration. A PP-Configuration cannot be used as the PMB for a PP-Module, and cannot be used simultaneously in a conformance claim with a PP by an ST. ~~Any PP-Configuration can be used exactly as a standard Protection Profile, as explained in Section B.13.~~

2.22 Changes to *B.15.4, PP-Configuration components statement*

(changes [CC-1], Section B.15.4; the entire section is repeated below for context and ease of application, with the changes highlighted.)

155 The *Components statement* identifies the non-Base PPs, Base-PPs and the PP-Modules that compose the PP-Configuration.

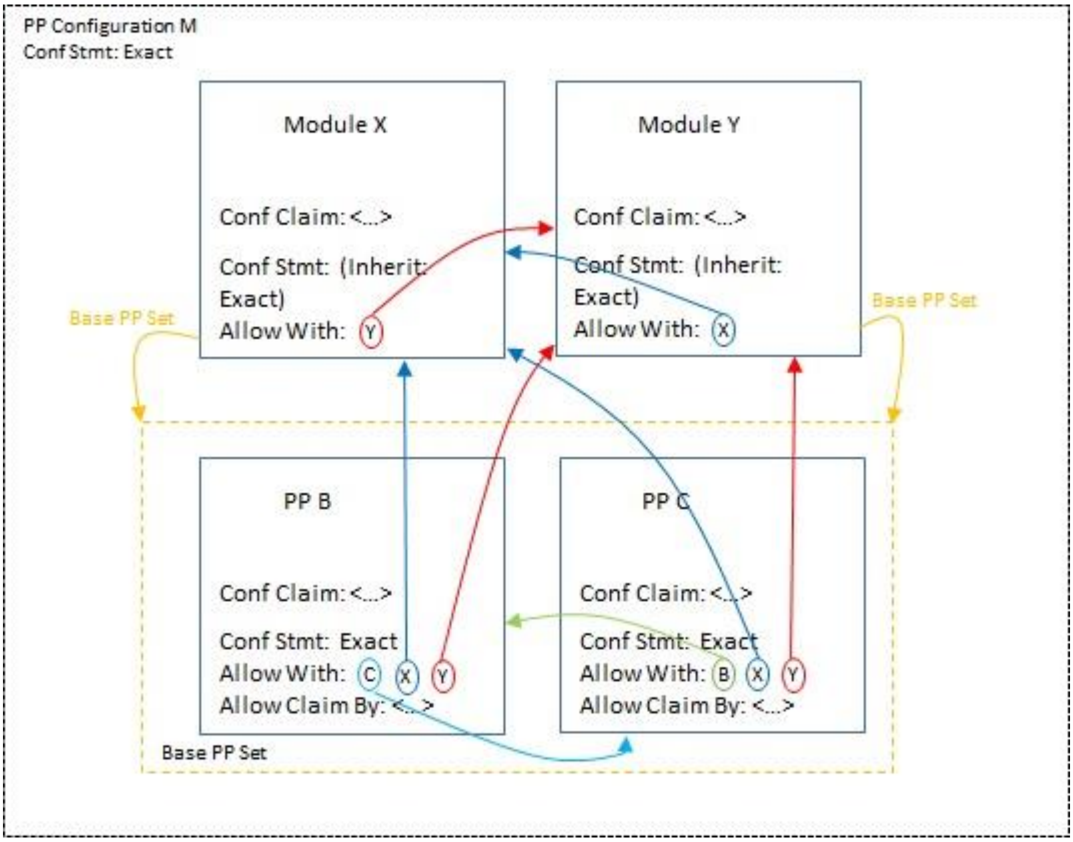
156 The Components statement must include at least all Base-PPs and base PP-Modules referenced in the PP-Modules. If the PP-Module specifies alternative

PMBs ~~sets of Base-PPs~~, only one of these sets must be referred to in the PP-Configuration. This is iterative; if a PMB contains a PP-Module that itself specifies alternative PMBs, only one can be specified in the PP-Configuration.

2.23 Changes to *B.15.5, PP-Configuration conformance statement*

(changes [CC-1], Section B.15.5; the entire section is repeated below for context and ease of application, with the changes highlighted.)

157 The *Conformance statement* specifies whether the conformance to this PP-Configuration has to be exact, strict, or demonstrable. If any component in the PP-Configuration requires exact conformance, then all PP-configuration components must be of exact conformance type. Further, all non-base-PPs, base-PPs, and PP-modules in the PP-configuration must allow all other PP-Configuration components in their respective allowed-with statements (the exception is that if a component is in the PMB of a PP-Module, that component does not need to listed in the allowed-with statement of that PP-Module). This is illustrated in the following example:

158 

159 In this example a PP-Configuration (named "M") specifies exact conformance in its conformance statement to PP-Modules X and Y. PP-Modules X and Y both have two PPs (both requiring exact conformance) listed as their PMB: PP B and PP C. The following statements (shown in the diagram) must be true for this to be an evaluable PP-Configuration with a conformance statement of "exact conformance":

1. The PP-Modules inherit the conformance statement from their base PPs, so their conformance statement is exact conformance.

2. The PP-Configuration must require exact conformance since the PP-Modules require exact conformance.

3. PP B must specify in its conformance statement that it is allowed to be used with PP C, PP-Module X, and PP-Module Y.

4. PP C must specify in its conformance statement that it is allowed to be used with PP B, PP-Module X, and PP-Module Y.

5. PP-Module X must specify in its conformance statement that it is allowed to be used with PP-Module Y.

6. PP-Module Y must specify in its conformance statement that it is allowed to be used with PP-Module X.

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

2.24 Changes to *B.15.6, PP-Configuration SAR statement*

(changes [CC-1], Section B.15.6; the following text is added at the end of this section (after paragraph 539).)

161 While in general the SAR statement can be different than that contained in the PP-Configuration's components if the PP-Configuration specifies demonstrable or strict conformance, this is not allowed for PP-Configurations of exact conformance type.

2.25 Changes to *C.2.3, The selection operation*

(changes [CC-1], Section C.2.3; the entire section is repeated below for context and ease of application, with the changes highlighted.)

162 As described in section **Fout! Verwijzingsbron niet gevonden.** the selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

163 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 authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of ..."

164 Section 8.1.3 also describes the notion of a selection-based SFR. The following is an example of such an SFR.

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

166 *Application Note:*

167 *In the first 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 are chosen corresponding to their selection are included in the ST.*

168 ***Appendix B*** *(of the example PP)*

169 *The following SFRs are included in the ST if the ST author selects "IPsec" in FTP_ITC.1.1:*

170 *FCS_IPSEC_EXT.1 […]*

2.26 Addition of *C.5, Optional SFRs*

(new; this section follows section C.4 in [CC-1])

171 **C.5 Optional SFRs**

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

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

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

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

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

177 It should be noted that since and ST can claim conformance to PPs with a strict or demonstrable conformance claim and add SFRs to the ST (over those

specified in the PP), optional requirements in those PPs may be unnecessary. However, if claiming conformance to a PP that requires exact conformance, optional requirements are a useful method to allow constrained flexibility (under control of the PP author) in the specification of functionality than an ST can claim conformance to.

2.27 Changes to *D.1, Introduction*

(changes [CC-1], Section D.1; the entire section is repeated below for context and ease of application, with the changes highlighted.)

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

179 Note that it is also possible for a PP to be used as a template for another PP. That is PPs can claim conformance to other PPs. This case is completely similar to that of an ST vs. a PP. For clarity this Annex describes only the ST/PP case, but it holds also for the PP/PP case.

180 The CC does not allow any form of partial conformance, so if a PP is claimed, the PP or ST must fully conform to the referenced PP or PPs (note that in the case of optional or selection-based SFRs, the inclusion or exclusion of these types of SFRs as outlined in the CC is still considered "full conformance"). There are however three types of conformance ("exact", "strict", and "demonstrable") and the type of conformance allowed is determined by the PP. That is, the PP states (in the PP conformance statement, see section **Fout! Verwijzingsbron niet gevonden.**) what the allowed types of conformance for the ST are. As indicated in Section 9.5, if a PP specifies exact conformance, then the ST can only claim conformance to that PP, either by itself or in combination with other explicitly-identified PPs that also require exact conformance. The distinction between strict and demonstrable conformance when such conformance statements are contained in multiple PPs to which an ST is claiming conformance is applicable to each PP to which an ST may claim conformance on an individual basis. This may mean that the ST conforms strictly to some PPs and demonstrably to other PPs. An ST is only allowed to conform to a PP in a demonstrable manner, if the PP explicitly allows this, whereas an ST can always conform with exact or strict conformance to any PP requiring demonstrable or strict conformance.

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

182 Conformance to a PP means that the PP or ST (and if an ST is of an evaluated product, the product as well) meets all requirements of that PP.

183 Published PPs will normally require demonstrable conformance. This means that STs claiming conformance with the PP must offer a solution to the generic security problem described in the PP, but can do so in any way that is equivalent or more restrictive to that described in the PP. "Equivalent but more restrictive" is defined at length within the CC, but in principle it means that

the PP and ST may contain entirely different statements that discuss different entities, use different concepts etc., provided that overall the ST levies the same or more restrictions on the TOE, and the same or less restrictions on the operational environment of the TOE.

184 The case for modular requirements construction (PP-Configurations and PP-Modules) is similar, but distinct from that for PPs.

185 A PP-Module inherits its conformance from its PMB. If all PMB components specify a single conformance type, then the PP-Module requires that conformance type as well. If one PMB component specifies exact conformance, then all PMB components must specify exact conformance, and the PP-Module itself will require exact conformance in its conformance statement. If the PMB components have a mix of conformance types (demonstrable and strict), then that will be resolved when the PP-Module is included in a PP-Configuration to which an ST claims conformance, and is evaluated the same as an ST claiming conformance to multiple PPs with different conformance types.

186 The configuration type for a PP-Configuration is handled in exactly the same manner as for a PP-Module, with the PP-Configuration components (which each has a conformance type) determining the conformance type of the PP-Configuration in the same manner.

2.28 Addition of *D.2, Exact conformance*

(new; this section follows section D.1 in [CC-1] to keep the hierarchical notion of exact, strict, then demonstrable conformance. This will also cause the current sections D.2 and D.3 in [CC-1] to be renumbered D.3 and D.4.)

187 **D.2 Exact conformance**

188 Exact conformance is oriented to the PP/PP-Module/PP-Configuration-author who requires evidence that the requirements in the PP/PP-Module/PP-Configuration are met, and that the ST is an instantiation of exactly those requirements (SFRs) without including additional functionality. In essence, the ST specifies that the TOE does what is required without making additional claims.

189 The CC allows a PP to claim conformance to another PP. With respect to Exact conformance this presents somewhat of a problem, since one could say if a PP is exactly conformant to another PP, then the PPs are identical. The intent of this construct in the CC is to allow PPs to build on one another. This type of construct can now be accomplished with PP-Modules and Base-PPs. Because of this, if a PP requires Exact Conformance, then it cannot be specified in another PP’s conformance claim statement.

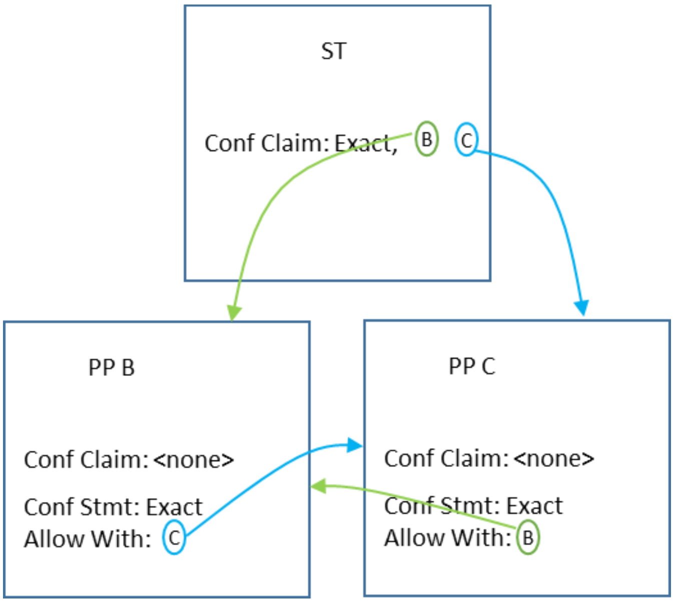
190 The CC allows an STs to claim conformance to multiple PPs, and a PP-Configuration can contain a combination of non-Base-PPs, Base-PPs, and PP-Modules. In the case where a PP requires exact conformance, this has the potential to circumvent the intent behind exact conformance, which gives the

PP author more control over the functionality and assurance provided for conformant STs than either strict or demonstrable conformance does. For example, if an ST can claim conformance to PP A (which requires exact conformance) and to PP B (which requires demonstrable conformance) at the same time, this would pull in SFRs which PP A's author did not explicitly approve to be used in combination with PP A's functionality when an ST claims conformance to PP A. Similarly, if a PP-Configuration contains PP-Module A (with a PMB of PP B), then if PP-Module A adds functionality to that specified by PP B, there is the same type of issue mentioned for the multiple PP case.

191 To address this issue, the conformance statement in the PP (see section B.5) and PP-Module (see section B.14.5) may also an allowed-with statement, which is a statement of which PPs and PP-Modules an ST, PP-Configuration, PP-Module, or PP author may simultaneously claim conformance to with the subject PP or PP-Module All identified PPs/PP-Modules/PP-Configurations must require exact conformance in their conformance statement, and must also list the subject PPs (and all other PPs being claimed) in their conformance statement (the exception being that a PP-Module does not list any PPs or PP-Modules that are part of its PMB).

192 Two examples are given to clarify these concepts; one for an ST claiming conformance to multiple PPs, and another for an ST claiming conformance to a PP-Configuration that contains multiple components.

193 In the first example, suppose PP B's authors wanted to allow STs to claim conformance it, and also to allow conformance claims to it in combination with PP C. This situation is pictured in the following diagram.



194 Then the following would have to be true:

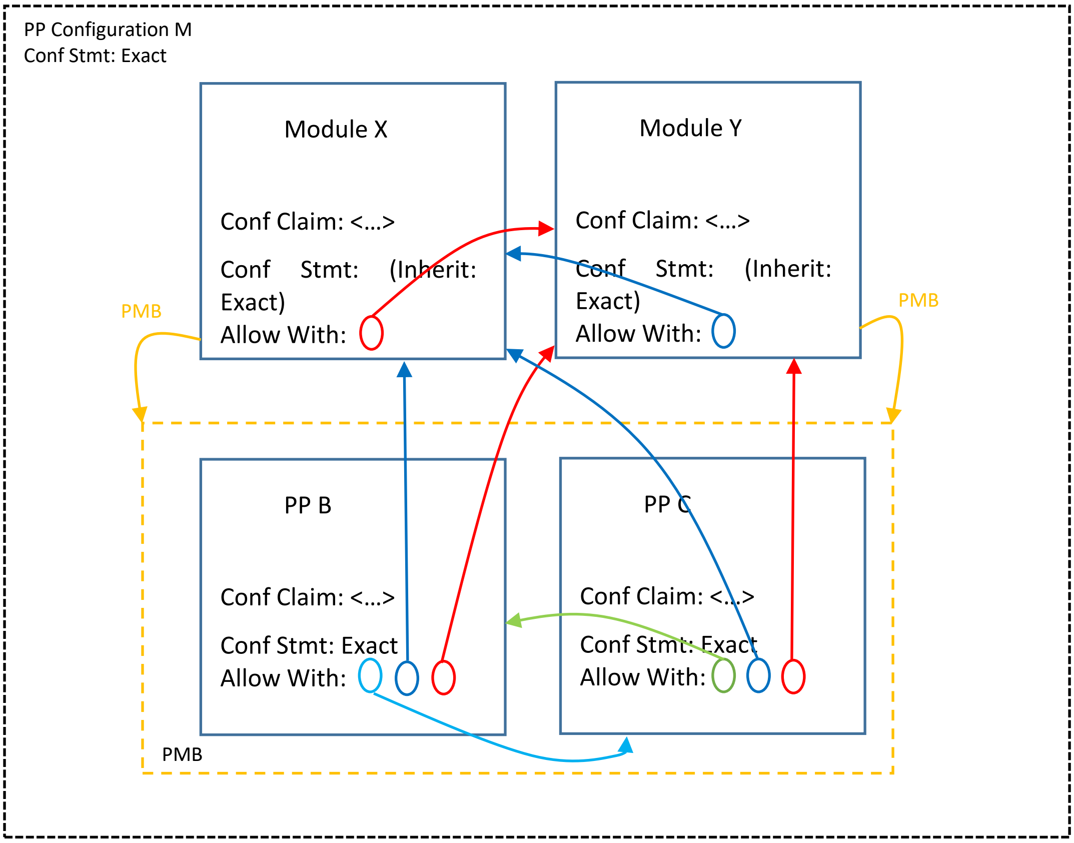
1. PPs B and C would all have to specific exact conformance in their conformance statement.

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

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

195 If any of these statements did not hold, then the ST could not claim (exact) conformance to PPs B and C.

196 In the second example, suppose an organization wishes to specify a PP-Configuration (M) that consisted of two PP-Modules: X and Y. These PP-Module specified the same PMB, consisting of the two PPs B and C. This is depicted in the following diagram:



197 The following statements (shown in the diagram) must be true for this to be an evaluable PP-Configuration with a conformance statement of "exact conformance":

1. The PP-Modules inherit the conformance statement from their base PPs, so their conformance statement is exact conformance.

2. The PP-Configuration must require exact conformance since the PP-Modules require exact conformance.

3. PP B must specify in its conformance statement that it is allowed to be used with PP C, PP-Module X, and PP-Module Y.

4. PP C must specify in its conformance statement that it is allowed to be used with PP B, PP-Module X, and PP-Module Y.

5. PP-Module X must specify in its conformance statement that it is allowed to be used with PP-Module Y.

6. PP-Module Y must specify in its conformance statement that it is allowed to be used with PP-Module X.

198 A typical example of the use of exact conformance is where the a technical community has agreed on a set of requirements and activities necessary to gain assurance with respect to the implementation of those requirements (and have specified such in the PP and supporting documents), but has not agreed on the need for, validity of, or specific methodology interpretations necessary for gaining assurance in, functionality that is not specified in the PP.

3 Addendum to CC Part 3

199 In order to implement and verify the concept of <package name>-tailored conformance and exact conformance in [CC-3], changes to and additions of elements need to be made for the families presented in this chapter. No changes are necessary in [CC-3] in order to implement selection-based and optional SFRs.

3.1 Changes to *APE_CCL*

3.1.1 Changes to *APE_CCL.1.6C*

(changes [CC-3] APE_CCL.1.6C; changes to existing element are highlighted)

APE_CCL.1.6C **The conformance claim shall describe any conformance of the PP to a package as ~~either~~ one of package-conformant, ~~or~~ package-augmented, or package-tailored.**

3.1.2 Changes to *APE_CCL.1.11C*

(changes [CC-3] APE_CCL.1.11C; changes to existing element are highlighted)

APE_CCL.1.11C **The conformance statement shall describe the conformance required of any PPs/STs to the PP as exact-PP, strict-PP, or demonstrable-PP conformance.**

3.1.3 Additions to *APE_CCL*

(changes [CC-3] APE_CCL with additional (new) content elements)

APE_CCL.1.12C **The conformance statement shall identify the set of PPs (if any) to which, in combination with the PP under evaluation, exact conformance is allowed to be claimed.**

APE_CCL.1.13C **The conformance statement shall identify the set of PP-modules (if any) that are allowed to be used with the PP under evaluation in a PP-Configuration.**

3.2 Changes to *ACE_INT*

3.2.1 Changes to ACE_INT.1.1C

(changes [CC-3] ACE_INT.1.1C; changes to existing element are highlighted)

ACE_INT.1.1C **The PP-Module introduction shall uniquely identify ~~all the Base-PPs~~ one or more PMBs, either in combination and as alternative sets, on which the PP-**

Module relies, including their logical structuring and relationship to the PP-Module according to CC Part 1, section B.14.3.2.

3.2.2 Changes to ACE_INT.1.2C

(changes [CC-3] ACE_INT.1.2C; changes to existing element are highlighted)

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~~PMB(s).**

3.3 Changes to *ACE_CCL*

3.3.1 Additions to ACE_CCL Developer Elements

(changes [CC-3] ACE_CCL with additional (new) developer element)

ACE_CCL.1.2D **The developer shall provide a conformance statement.**

3.3.2 Additions to ACE_CCL Content Elements

(changes [CC-3] ACE_CCL with additional (new) content elements)

ACE_CCL.1.5C **The conformance claim shall describe any conformance of the PP-Module to a functional package as either package-name-conformant, package-name-augmented or package-name-tailored.**

ACE_CCL.1.6C **The conformance statement shall identify the set of PPs and PP-Modules to which, in combination with the PP-Module under evaluation, exact conformance is allowed to be claimed in a PP-Configuration.**

3.4 Changes to *ACE_MCO*

3.4.1 Changes to *ACE_MCO.1 (all elements)*

(changes [CC-3] ACE_MCO.1. All elements are affected.)

200 *Each element in ACE_MCO only identifies "Base-PP(s)" as being bases for PP-Modules. These addenda adds the construct of PP-Modules (and their PMBs) as being allowed bases for a PP-Module, and so all elements need to modified in order to accommodate this. In each element, change "Base-PP" to "PMB".*

3.5 Changes to *ACE_CCO*

3.5.1 Changes to *ACE_CCO.1.3C*

(changes [CC-3] ACE_CCO.1.3C; changes to existing element are highlighted)

ACE_CCO.1.3C **The conformance statement shall specify the required conformance to the PP-Configuration as one of exact, strict, or demonstrable. The**

conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the PP-Configuration and its underlying components ~~Base-PP(s) and PP-Module~~ claim conformance.

3.5.2 Changes to *ACE_CCO.1.5C*

(changes [CC-3] ACE_CCO.1.5C; changes to existing element are highlighted)

ACE_CCO.1.5C **The ~~Base-PP~~ elements (PP-Module(s) and PP(s)) of the PMB(s) on which the PP-Modules relies shall be~~long the Protection Profiles~~ identified in the components statement of the PP-Configuration.**

3.6 Changes to *ASE_CCL*

3.6.1 Changes to *ASE_CCL.1.5C*

(changes [CC-3] ASE_CCL.1.5C; changes to existing element are highlighted)

ASE_CCL.1.5C **The conformance claim shall identify a PP-Configuration, or all PPs and security requirement packages to which the ST claims conformance.**

3.6.2 Changes to *ASE_CCL.1.7C, ASE_CCL.1.8C, ASE_CCL.1.9C, ASE_CCL.1.10C*

(changes [CC-3] ASE_CCL.1.7C through ASE_CCL.1.10C; the following change is made for all of those elements.)

201 *ASE_CCL.1.7C through ASE_CCL.1.10C are written to only apply to claims of an ST against a PP. These need to be changed to specify claims of conformance against a PP-Configuration as well. In each element, change "in the PPs" to "in the PP-Configuration or the PPs".*

3.6.3 Additions to *ASE_CCL.1*

(changes [CC-3] ASE_CCL with additional (new) content elements)

ASE_CCL.1.11C **The conformance claim shall describe any conformance of the ST to a PP as PP-Conformant.**

ASE_CCL.1.12C **The conformance claim shall describe any conformance of the ST to a PP-Configuration as PP-Configuration-Conformant.**

ASE_CCL.1.12C **The conformance claim for PP(s) or a PP-Configuration shall be exact, strict, or demonstrable.**

4 Addendum to the CEM

202 The additions required to support the concepts of exact conformance, selection-based SFRs, optional SFRs, and <package-name>-tailored conformance require changes to and additions of several work units throughout the [CEM]. This chapter presents these changes, grouped first by the family, then by the particular element and associated work units.

4.1 Changes to work units associated with *APE_CCL*

4.1.1 Changes to work units associated with *APE_CCL.1.5C*

(changes [CEM] work units associated with APE_CCL.1.5C. Changes to the existing element are highlighted.)

APE_CCL.1-6a The evaluator ***shall check*** that the conformance claim contains a PP claim that identifies all PPs for which the PP claims conformance.

203 If the PP does not claim conformance to another PP, this work unit is not applicable and therefore considered to be satisfied.

204 The evaluator ensures that the conformance statement for the PP, and the conformance statement for any PP to which the PP is claiming conformance, does not specify exact conformance is required.

205 The evaluator determines that any referenced PPs are unambiguously identified (e.g. by title and version number, or by the identification included in the introduction of that PP).

206 The evaluator is reminded that claims of partial conformance to a PP are not permitted.

4.1.2 Changes to work units associated with *APE_CCL.1.6C*

(changes [CEM] work unit APE_CCL.1-8; for context, the entire work unit is reproduced with the changes highlighted.)

APE_CCL.1.6C ***The conformance claim shall describe any conformance of the PP to a package as ~~either~~ one of package-conformant, ~~or~~ package-augmented, or package-tailored.***

APE_CCL.1-8 The evaluator ***shall check*** that, for each identified package, the conformance claim states a claim of ~~either~~ one of package-name conformant, ~~or~~ package-name augmented, or package-name tailored.

207 If the PP does not claim conformance to a package, this work unit is not applicable and therefore considered to be satisfied.

208 If the package conformance claim contains package-name conformant, the evaluator determines that:

a) If the package is an assurance package, then the PP contains all SARs included in the package, but no additional SARs.

b) If the package is a functional package, then the PP contains all SFRs included in the package, but no additional SFRs.

209 If the package conformance claim contains package-name augmented, the evaluator determines that:

a) If the package is an assurance package, then the PP contains all SARs included in the package, and at least one additional SAR or at least one SAR that is hierarchical to a SAR in the package.

b) If the package is a functional package, then the PP contains all SFRs included in the package, and at least one additional SFR or at least one SFR that is hierarchical to a SFR in the package.

210 If the package conformance claim contains package-name tailored, the evaluator determines that:

a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP);

b) the PP may have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package;

c) the PP shall have at least one additional (not present in the SFR in the package) selection item in one of the SFRs in the functional package.

d) In the case of package-name tailored, the evaluator additionally examines the selection (and other selections in that requirement) to ensure that the requirement still meets its security objective (or the associated SPD element in the low assurance approach) with the addition of (and potentially deletion of) the selection item.

4.1.3 Changes to *APE_CCL.1.11C* and associated work units

(changes [CEM] statement of APE_CCL.1.11C to correspond to [CC-3], and changes work unit APE_CCL.1-13; for context, the entire text is reproduced with the changes highlighted.)

APE_CCL.1.11C ***The conformance statement shall describe the conformance required of any PPs/STs to the PP as exact-PP, strict-PP, or demonstrable-PP conformance.***

APE_CCL.1-13 The evaluator ***shall check*** that the PP conformance statement states a claim of exact-PP, strict-PP, or demonstrable-PP conformance.

4.1.4 Addition of *APE_CCL.1.12C* and associated work units

(adds [CEM] statement of APE_CCL.1.12C to correspond to [CC-3], and adds associated (new) work units.)

APE_CCL.1.12C ***The conformance statement shall identify the set of PPs (if any) to which, in combination with the PP under evaluation, exact conformance is allowed to be claimed.***

APE_CCL.1-14 The evaluator ***shall check*** the conformance statement to determine it contains an allowed-with statement that lists the set of PPs to which, in combination with the PP being evaluated, an exact conformance claim (in an ST or PP) is allowed.

211 If the PP does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

212 If the PP does not allow claims of exact conformance to it in combination with any other PPs, then no list of PPs is required and this work unit is considered satisfied.

213 There are no other actions for the evaluator other than determining that the list is present.

4.1.5 Addition of *APE_CCL.1.13C* and associated work units

(adds [CEM] statement of APE_CCL.1.13C to correspond to [CC-3], and adds associated (new) work units.)

APE_CCL.1.13C ***The conformance statement shall identify the set of PP-modules (if any) that are allowed to be used with the PP under evaluation in a PP-Configuration.***

APE_CCL.1-16 The evaluator ***shall check*** the conformance statement to determine it lists the set of PP-modules that are allowed to be used with the PP when the PP is a component in a PP-configuration with the PP-Module.

214 If the PP does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

215 If the PP does not allow any PP-module to be used with the PP in a PP-Configuration, then the evaluator confirms that no PP-modules are listed.

216 There are no other actions for the evaluator other than determining that the list is present (or absent).

4.2 Changes to work units associated with *APE_REQ*

4.2.1 Changes to work units associated with *APE_REQ.1.2C*

(changes [CEM] work unit APE_REQ.1-3; for context, the entire work unit is reproduced with the changes highlighted.)

APE_REQ.1-3 The evaluator ***shall examine*** the PP to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.

217 The evaluator determines that the PP defines all:

- (types of) subjects and objects that are used in the SFRs;
- (types of) security attributes of subjects, users, objects, information, sessions and/or resources, possible values that these attributes may take and any relations between these values (e.g. top_secret is “higher” than secret);
- (types of) operations that are used in the SFRs, including the effects of these operations;
- (types of) external entities in the SFRs;
- SFRs that are to be treated as *optional* SFRs. The PP may define optional requirements in one of two categories. Each category is specified explicitly by the PP.

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

  The second category of optional requirements is conditional. If the TOE implements the described functionality then the optional requirement shall be included in the ST. If the TOE does not implement the functionality covered by the optional requirement, then the requirement is not included in the ST.
- Optional requirements can be written in response to SPD-elements that exist in the PP, or SPD-elements that are specifically associated with the requirement. The evaluator determines that such associations are identified in the PP. Low Assurance PPs do not have security objectives for optional requirements that have associated SPD elements, while regular PPs include security objectives for the associated SFRs and SPD elements.

- other terms that are introduced in the SFRs and/or SARs by completing operations, if these terms are not immediately clear, or are used outside their dictionary definition.

218 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no misunderstanding may occur due to the introduction of vague terms. This work unit should not be taken into extremes, by forcing the PP writer to define every single word. The general audience of a set of security requirements should be assumed to have a reasonable knowledge of IT, security and Common Criteria.

219 All of the above may be presented in groups, classes, roles, types or other groupings or characterisations that allow easy understanding.

220 The evaluator is reminded that these lists and definitions do not have to be part of the statement of security requirements, but may be placed (in part or in whole) in different sections. This may be especially applicable if the same terms are used in the rest of the PP.

4.2.2 Changes to work units associated with *APE_REQ.1.3C*

(changes [CEM] work unit APE_REQ.1-4; for context, the entire work unit is reproduced with the changes highlighted.)

APE_REQ.1-4 The evaluator ***shall check*** that the statement of security requirements identifies all operations on the security requirements.

221 The evaluator determines that all operations are identified in each SFR or SAR where such an operation is used. This includes both completed operations and uncompleted operations. Identification may be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

222 If the PP defines *selection-based* SFRs, the evaluator determines that the PP clearly identifies the dependencies between the selection in an SFR and the selection-based SFR(s) to be included in the PP/ST should that selection be chosen by the PP/ST author.

4.2.3 Changes to work units associated with *APE_REQ.2.2C*

(changes [CEM] work unit APE_REQ.2-3; for context, the entire work unit is reproduced with the changes highlighted.)

APE_REQ.2-3 The evaluator ***shall examine*** the PP to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.

223 The evaluator determines that the PP defines all:

- (types of) subjects and objects that are used in the SFRs;

- (types of) security attributes of subjects, users, objects, information, sessions and/or resources, possible values that these attributes may take and any relations between these values (e.g. top_secret is "higher" than secret);

- (types of) operations that are used in the SFRs, including the effects of these operations;

- (types of) external entities in the SFRs;

- SFRs that are to be treated as *optional* SFRs. The PP may define optional requirements in one of two categories. Each category is specified explicitly by the PP.

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

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

- Optional requirements can be written in response to SPD-elements that exist in the PP, or SPD-elements that are specifically associated with the requirement. The evaluator determines that such associations are identified in the PP. Low Assurance PPs do not have security objectives for optional requirements that have associated SPD elements, while regular PPs include security objectives for the associated SFRs and SPD elements.

- other terms that are introduced in the SFRs and/or SARs by completing operations, if these terms are not immediately clear, or are used outside their dictionary definition.

224 The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no misunderstanding may occur due to the introduction of vague terms. This work unit should not be taken into extremes, by forcing the PP writer to define every single word. The general audience of a set of security requirements should be assumed to have a reasonable knowledge of IT, security and Common Criteria.

225 All of the above may be presented in groups, classes, roles, types or other groupings or characterisations that allow easy understanding.

226 The evaluator is reminded that these lists and definitions do not have to be part of the statement of security requirements, but may be placed (in part or in

whole) in different sections. This may be especially applicable if the same terms are used in the rest of the PP.

4.2.4 Changes to work units associated with *APE_REQ.2.3C*

(changes [CEM] work unit APE_REQ.2-4; for context, the entire work unit is reproduced with the changes highlighted.)

APE_REQ.2-4 The evaluator ***shall check*** that the statement of security requirements identifies all operations on the security requirements.

227 The evaluator determines that all operations are identified in each SFR or SAR where such an operation is used. This includes both completed operations and uncompleted operations. Identification may be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

228 If the PP defines *selection-based* SFRs, the evaluator determines that the PP clearly identifies the dependencies between the selection in an SFR and the selection-based SFR(s) to be included in the PP/ST should that selection be chosen by the PP/ST author.

4.3 Changes throughout Class ACE section

4.3.1 General modification throughout section 10

(modifies [CC-3] section 10; this is a general change throughout section 10 to avoid a minor, but pervasive, editorial change being repeaded continually in these addenda.)

229 *When issued, the modular requirements construction section only allowed the specification of PPs as the base for a PP-Module. As noted above, these addenda allow the specification of PP-Modules in addition to PPs as a base for a PP-Module, and the term "PP-Module Base" (PMB) is introduced by these addenda to reflect this. Throughout this section, the term "Base-PP" is used to specify the base for a PP-Module. This clause changes the term "Base-PP" to "PMB) throughout section 10 unless otherwise specifically noted in other sections of this addenda. This includes inputs to the evaluation activities; where "its Base-PP(s)" is specified, for instance, it should be read as "its PMB components (PP-Modules(s), Base-PP(s))."*

4.4 Changes to Class ACE Introduction

4.4.1 Modification of *section 10.1*

(modifies [CC-3] section 10.1)

230 *PP-Configurations are distinct from standard PPs. While both are methods to state sets of SFRs and SARs used to specify security functionality and assurance to which STs can claim conformance, there are structural differences—as well as differences in how they are constructed and evaluated—such that they should not be seen as equivalent. Text starting on*

in paragraph 312 depends on the treatment of a PP-Configuration as a "standard PP", which is clarified as not being allowed by these addenda. Therefore, these addenda remove paragraphs 312 through 313, including Figure 6.

4.5 Changes to work units associated with *ACE_INT*

4.5.1 Modification of *ACE_CCL.1.1C* and associated work units

(changes [CEM] statement of ACE_CCL.1.1C to correspond to [CC-3], and modifies associated work units.)

ACE_INT.1.1C ***The PP-Module introduction shall uniquely identify ~~all the Base PPs~~ one or more PMBs, either in combination and as alternative sets, on which the PP-Module relies, including their logical structuring and relationship to the PP-Module according to CC Part 1, section B.14.3.2.***

ACE_CCL.1-1 The evaluator shall check that the PP-Module introduction identifies the PMBs ~~Base PP(s)~~ on which the PP-Module relies. This can consist of a single PP or PP-Module (with its PMB), or multiple PPs and/or PP-Modules (with associated PMBs) that must be used all together, or alternate sets of PMBs, one of which is used when the PP-Module is instantiated in a PP-Configuration.

4.6 Changes to work units associated with *ACE_CCL*

4.6.1 Addition of *ACE_CCL.1.5C* and associated work units

(adds [CEM] statement of ACE_CCL.1.5C to correspond to [CC-3], and adds associated (new) work units.)

ACE_CCL.1.5C ***The conformance claim shall describe any conformance of the PP-Module to a functional package as either package-name-conformant, package-name-augmented or package-name-tailored.***

ACE_CCL.1-5 The evaluator ***shall check*** that, for each identified package, the conformance claim states a claim of one of package-name conformant, package-name augmented, or package-name tailored.

231 If the PP-Module does not claim conformance to a package, this work unit is not applicable and therefore considered to be satisfied.

232 If a PP-Module or PP in the PP-Module's PMB claims conformance to a package and the PP-Module does not further modify the package, the evaluator ensures that the PP-Module does not also claim conformance to that package.

233 The evaluator determines that any packages claimed by a PP-Module are functional packages.

234 If the package conformance claim contains package-name conformant, the evaluator determines that:

a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP-Module (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP-Module);

235 If the package conformance claim contains package-name augmented, the evaluator determines that:

a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP-Module (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP-Module); except

b) the PP-Module contains at least one additional SFR or at least one SFR that is hierarchical to a SFR in the package.

236 If the package conformance claim contains package-name tailored, the evaluator determines that:

a) all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP-Module (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP-Module);

b) the PP may have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package;

c) the PP shall have at least one additional (not present in the SFR in the package) selection item in one of the SFRs in the functional package.

237 In the case of package-name tailored, the evaluator additionally examines the selection (and other selections in that requirement) to ensure that the requirement still meets its security objective (or the associated SPD element in the low assurance approach) with the addition of (and potentially deletion of) the selection item.

4.6.2 Addition of *ACE_CCL.1.6C* and associated work units

(adds [CEM] statement of ACE_CCL.1.6C to correspond to [CC-3], and adds associated (new) work units.)

ACE_CCL.1.6C ***The conformance statement shall identify the set of PPs and PP-Modules to which, in combination with the PP-Module under evaluation, exact conformance is allowed to be claimed in a PP-Configuration.***

ACE_CCL.1-6 The evaluator ***shall check*** the conformance statement to determine it lists the set of PP-modules that can be specified in the components statement of a PP-Configuration that includes the PP-module.

238 If the PP-Module does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

239 If the PP-module does not allow its use (in a PP-configuration) with other PP-Modules, then there will be no other PP-Modules identified in the PP-Module's allowed-with statement, and the evaluator ensures the PP-Configuration contains no other PP-Modules in the PP-Configuration's components statement. The only exception to this is if the PP-Module contains another PP-Module in its PMB; in this case, while the PP-Module in the PMB will be listed in the PP-Configuration's components list, it does not need to be listed in the PP-Module's allowed-with list since it's implicitly allowed by virtue of it being in the PMB.

240 Note that the reverse is not true. If PP-Module A specifies PP-Module B in its PMB (which incidentally brings in PP-Module B's PMB), then PP-Module B will have to list PP-Module A in its allowed-with statement.

241 If the PP-configuration's components statement does include other PP-Modules, then the evaluator ensures that all PP-Modules listed in the components statement are included in the PP-Module's allowed-with statement.

ACE_CCL.1-7 The evaluator ***shall check*** the conformance statement to determine it lists the set of PPs that can be specified in the components statement of a PP-Configuration that includes the PP-module.

242 If the PP-Module does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

243 If the PP-module does not allow its use (in a PP-configuration) with PPs that are not its PMB, then there will be no other PPs identified in the PP-Module's allowed-with statement, and the evaluator ensures the PP-Configuration contains no other PPs in the PP-Configuration's components statement.

244 If the PP-Configuration's components statement does include other PPs, then the evaluator ensures that all PPs listed in the components statement are included in the PP-Module's allowed-with statement.

4.7 Changes to work units associated with *ACE_CCO*

4.7.1 Changes to *ACE_CCO.1.3C* and associated work units

(changes [CEM] statement of APE_CCO.1.3C to correspond to [CC-3]; changes work unit ACE_CCO.1-3; and adds (new) work unit ACE_CCO.1-3a (to maintain the Rev 5 numbering). For context, the entire text is reproduced with the changes highlighted.)

ACE_CCO.1.3C ***The conformance statement shall specify the required conformance to the PP-Configuration as one of exact, strict, or demonstrable. The conformance claim shall contain a CC conformance claim that identifies the version of***

the CC to which the PP-Configuration and its underlying components ~~Base-PP(s) and PP-Module~~ claim conformance.

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

245 The evaluator shall check that the conformance claim contains a CC conformance claim that identifies the version of the CC to which the PP-Configuration and its underlying components ~~Base-PP(s) and PP-Module~~ claim conformance.

246 The evaluator shall examine the PP-Configuration conformance claim to determine the compatibility between all CC versions that are related to the PP-Configuration and its underlying components ~~Base-PP(s) and PP-Module~~.

247 If at least one of the Protection Profiles identified in the PP-Configuration components statement requires exact conformance, then the PP-Configuration conformance statement shall also require exact conformance (and all other components in the PP-Configuration must require exact conformance). If none of the PPs identified in the PP-Configuration components statement requires exact conformance but at least one requires strict conformance, then the PP-Configuration conformance statement shall also require strict conformance.

248 CC versions used in a PP-Configuration and its underlying components ~~Base-PP(s) and PP-Module~~ have to be compatible. If compatibility is not obvious, guidance from the certification scheme should be asked.

ACE_CCO.1-3a The evaluator ***shall examine*** the PP-Configuration components statement to determine that, for each PP, all PP-Modules specified in the components statement are listed as allowed to be used with that PP.

249 If the PP-configuration does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

250 The evaluator examines each PP in the PP-Configuration components statement. For each PP, the evaluator determines that each PP-Module listed in the PP-Configuration components statement is also listed in the PP's allowed-with statement.

4.8 Changes to work units associated with *ASE_CCL*

4.8.1 Changes to work units associated with *ASE_CCL.1.5C*

(changes [CEM] work units associated with ASE_CCL.1.5C. Modifies work unit ASE_CCL.1-6; the entire text is included with changes highlighted. Adds work units ASE_CCL.1-6a and ASE_CCL.1-7a. The letter after the number is used to uniquely identify the changes made by this addendum without changing the existing number in the [CEM].)

ACE_CCL1.5C ***The conformance claim shall identify a PP-Configuration, or all PPs and security requirement packages to which the ST claims conformance.***

ASE_CCL.1-6 The evaluator ***shall check*** that the conformance claim contains a PP claim that identifies all PPs for which the ST claims conformance.

251 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore considered to be satisfied.

252 The evaluator determines that any referenced PPs are unambiguously identified (e.g. by title and version number, or by the identification included in the introduction of that PP). Only those PPs to which the ST claims exact, strict, or demonstrable conformance are allowed to be identified in the conformance claim section that means claiming partial conformance to a PP or PP-configuration is not permitted.

253 Therefore, conformance to a PP requiring a composite solution may be claimed in an ST for a composed TOE. Conformance to such a PP would not have been possible during the evaluation of the component TOEs, as these components would not have satisfied the composed solution. This is only possible in the instances where the “composite” PP permits use of the composition evaluation approach (use of ACO components).

254 The ST for a composed TOE will identify the STs of the component TOEs from which the composed ST is comprised. The composed TOE is essentially claiming conformance to the STs of the component TOEs.

ASE_CCL.1-6a The evaluator ***shall check*** that, for each PP to which the ST claims conformance, the conformance statement of that PP allows all other PPs in the conformance claim to be allowed to be claimed with that PP.

255 If the ST does not claim conformance to a PP, or claims conformance to only one PP, this work unit is not applicable and therefore considered to be satisfied.

256 If the ST is not claiming exact conformance to a PP, this work unit is not applicable and therefore considered to be satisfied.

257 The evaluator determines that the allowed-with statement of the PP to which conformance is being claimed lists each of the PPs identified in the conformance claim section of the ST. Note that this is only applicable in cases where that PP requires exact conformance and the ST claims exact conformance.

APE_CCL.1-7a The evaluator ***shall check*** that if the ST claims conformance to a PP-Configuration, it does not also claim conformance to another PP-Configuration or any PP.

4.8.2 Changes to work units associated with *ASE_CCL.1.8C*

(changes [CEM] work unit ASE_CCL.1-10. Due to the length of the work unit, the entire work unit is not reproduced here. Instead, insert the following as the third numbered paragraph of the work unit (that is, between existing paragraphs 408 and 409.))

258 If exact conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether:

a) the threats in the ST are identical (no fewer threats, no additional threats) to the threats in the PP to which conformance is being claimed. If exact conformance is being claimed to more than one PP, then the set of threats in the ST must be identical the union of the threats in all PPs to which conformance is being claimed.

b) the OSPs in the ST are identical (no fewer OSPs, no additional OSPs) to the OSPs in the PP to which conformance is being claimed. If exact conformance is being claimed to more than one PP, then the set of OSPs in the ST must be identical the union of the OSPs in all PPs to which conformance is being claimed.

b) the assumptions in the ST are identical (no fewer assumptions, no additional assumptions) to the assumptions in the PP to which conformance is being claimed. If exact conformance is being claimed to more than one PP, then the set of assumptions in the ST must be identical to the union of the assumptions in all PPs to which conformance is being claimed, with the following possible exception;

– an assumption (or part of an assumption) from a PP can be omitted, if all security objectives for the operational environment addressing this assumption (or part of an assumption) are replaced by security objectives for the TOE that are identical to (taken from) another of the PPs to which the ST is claiming conformance;

When examining an ST in these circumstances (assumptions from one PP are replaced by security objectives on the TOE from one of the other PPs) the evaluator shall carefully determine that the condition given above is fulfilled. The following discussion gives an example:

– An ST is claiming exact conformance to two PPs. As determined in previous work units, both of these PPs require exact conformance in their conformance statements, and both PPs list the other as being “allowed with” the PP in a conformance claim by an ST. One PP to which the ST claims conformance contains an assumption stating that the operational environment prevents unauthorised modification or interception of data sent to an external interface of the TOE. This may be the case if the TOE accepts data in clear text and without integrity protection at this interface and is assumed to be located in a secure operational environment, which will prevent attackers from accessing these data. The assumption will then be mapped in the PP to some objective for the operational environment stating that the data interchanged at this interface are protected by adequate measures in the operational environment. Suppose there is another PP that specifies that conformant TOEs must protect data sent over the TOEs external interfaces, and has appropriate threats and security objectives addressing this threat. The ST author can then replace the assumption and security objective for the environment related to the protection of data over the external interfaces of the TOE from one PP with the security objective stating that the TOE itself protects these data, for example by providing a secure channel for encryption and integrity protection of all data transferred via this interface from the other PP; the corresponding objective and assumption for the operational environment from the other PP is thus omitted from the ST. This is also called re-assigning of the objective, since the objective is re-assigned from the operational environment to the TOE. Note, that this TOE is still secure in an operational environment fulfilling the omitted assumption and therefore still fulfils the PP. Further, the set of threats and objectives in the ST is still no broader than the union of threats and objectives in the PPs to which it is claiming exact conformance.

4.8.3 Changes to work units associated with *ASE_CCL.1.9C*

(changes [CEM] work unit ASE_CCL.1-11. Due to the length of the work unit, the entire work unit is not reproduced here. Instead, insert the following as the second numbered paragraph of the work unit (that is, between existing paragraphs 413 and 414.))

259 If exact conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether:

- The ST contains all security objectives for the TOE of the PP to which conformance is being claimed. Note that in the exact conformance case, it is not allowed for the ST under evaluation to have additional security objectives for the TOE. If conformance is being claimed to more than one PP, the set of security objectives for the TOE must be identical to the union of the security objectives for the TOE in the PPs to which conformance is being claimed.
- The security objectives for the operational environment in the ST are identical to the security objectives for the operational environment in the PP to which conformance is being claimed. If conformance is being claimed to more than one PP, the set of security objectives for the operational environment must be identical to the union of the security objectives for the operational environment in the PPs to which conformance is being claimed with the possible exception as follows.
- a security objective for the operational environment (or part of such security objective) from one PP can be replaced by the same (part of the) security objective for the TOE from another PP.

4.8.4 Changes to work units associated with *APE_CCL.1.10C*

(changes [CEM] work unit APE_CCL.1-12; for context, the entire work unit is reproduced with the changes highlighted.)

ASE_CCL.1-12 The evaluator ***shall examine*** the ST to determine that it is consistent, as defined by the conformance statement of the PP, with all security requirements in the PPs for which conformance is being claimed.

260 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore considered to be satisfied.

261 If exact conformance is required by the PP to which conformance is being claimed then no conformance claim rationale is required. Instead, the evaluator determines that the statement of security requirements in the PP to which conformance is being claimed is exactly reproduced in the ST, with the following allowances:

- an SFR from the PP may be iterated or refined in the ST,
- SFRs identified as optional in the PP to which conformance is being claimed may or may not be included in the ST.
- all SFRs that are defined in the PP to which conformance is being claimed as selection-based upon a particular selection shall be included if and only if that selection on which inclusion is based is present in the ST. If a selection is not chosen by the ST author, then the selection-based SFRs associated with that selection are not included in the ST.
- There are no additional security requirements (SFRs or SARs) that are included in the ST that are not also present in the PP.
- In the case where exact conformance is being claimed to multiple PPs, the evaluator determines there are no additional security requirements included in the ST that are not in at least one of the PPs, and that all of the requirements (with the allowances described above) in all of the PPs have been included in the ST.

262 If strict conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether the statement of security requirements in the ST is a superset of or identical to the statement of security requirements in the PP to which conformance is being claimed (for strict conformance).

263 If demonstrable conformance is required by the PP to which conformance is being claimed, the evaluator examines the conformance claim rationale to determine that it demonstrates that the statement of security requirements of the ST is equivalent or more restrictive than the statement of security requirements in the PP to which conformance is being claimed.

264 For:

- SFRs: The conformance rationale in the ST shall demonstrate that the overall set of requirements defined by the SFRs in the ST is equivalent (or more restrictive) than the overall set of requirements defined by the SFRs in the PP. This means that all TOEs that would meet the requirements defined by the set of all SFRs in the ST would also meet the requirements defined by the set of all SFRs in the PP;

- SARs: The ST shall contain all SARs in the PP, but may claim additional SARs or replace SARs by hierarchically stronger SARs. The completion of operations in the ST must be consistent with that in the PP; either the same completion will be used in the ST as that in the PP or a completion that makes the SAR more restrictive (the rules of refinement apply).

265 For a composed TOE, the evaluator will consider whether the security requirements of the composed TOE are consistent with that specified in the STs for the component TOEs. This is determined in terms of demonstrable conformance. In particular, the evaluator examines the conformance rationale to determine that:

a) The statement of security requirements in the dependent TOE ST relevant to any IT in the operational environment is consistent with the statement of security requirements for the TOE in the base TOE ST. It is not expected that the statement of security requirements for the environment within in the dependent TOE ST will cover all aspects of the statement of security requirements for the TOE in the base TOE ST, as some SFRs may need to be added to the statement of security requirements in the composed TOE ST. However, the statement of security requirements in the base should support the operation of the dependent component.

b) The statement of security objectives in the dependent TOE ST relevant to any IT in the operational environment is consistent with the statement of security requirements for the TOE in the base TOE ST. It is not expected that the statement of security objectives for the environment within in the dependent TOE ST will cover all aspects of the statement of security requirements for the TOE in the base TOE ST.

c) The statement of security requirements in the composed is consistent with the statements of security requirements in the STs for the component TOEs.

266 If demonstrable conformance is required by the PP to which conformance is being claimed, the evaluator examines the conformance claim rationale to determine that it demonstrates that the statement of security requirements of the ST is at least equivalent to the statement of security requirements in the PP, or component TOE ST in the case of a composed TOE ST.

4.8.5 Additions to *ASE_CCL.1* and associated work units

(adds [CEM] statement of ASE_CCL.1.11C, ASE_CCL.1.12C, and ASE_CCL.1.13C to correspond to [CC-3], and adds associated (new) work units.)

ASE_CCL.1.11C ***The conformance claim shall describe any conformance of the ST to a PP as PP-Conformant.***

ACE_CCL.1-12 The evaluator ***shall check*** the conformance claim to ensure that any claim of conformance to a PP is specified as PP-Conformant.

267 If the ST does not claim conformance to a PP, this work unit is not applicable and therefore considered to be satisfied.

ASE_CCL.1.12C ***The conformance claim shall describe any conformance of the ST to a PP-Configuration as PP-Configuration-Conformant.***

ACE_CCL.1-13 The evaluator ***shall check*** the conformance claim to ensure that any claim of conformance to a PP-Configuration is specified as PP-Configuration-Conformant.

268 If the ST does not claim conformance to a PP-Configuration, this work unit is not applicable and therefore considered to be satisfied.

ASE_CCL.1.12C ***The conformance claim for PP(s) or a PP-Configuration shall be exact, strict, or demonstrable.***

ACE_CCL.1-13 The evaluator ***shall check*** the conformance claim to ensure that any claim of conformance to PP(s) or a PP-Configuration is specified as exact, strict, or demonstrable.

269 If the ST does not claim conformance to PP(s) or a PP-Configuration, this work unit is not applicable and therefore considered to be satisfied.

270 The evaluator determines that the conformance claim in the ST matches the conformance statement in the PP(s) or PP-Configuration.