CC and CEM addenda

Exact Conformance, Selection-Based SFRs, Optional SFRs

May 2017

Version 0.5

CCDB-2017-05-xxx

Draft for Use

Foreword

This is a DRAFT addenda to the Common Criteria version 3.1 and the associated Common Evaluation Methodology for Information Technology Security Evaluation, which is approved for trial use. Upon final approval, this document will be updated to remove the "DRAFT" caveat and will then be integrated in the next versions of those documents.

Technical Editor:

Document History:

V0.5, May 2017 : Initial release, for trial use

Field of special use: None

DRAFT - For Trial Use

Table of Contents

1 INTRODUCTION 5

1.1 Executive Summary 5

1.2 Scope 6

1.3 Audience 6

1.4 Normative References 6

1.5 Terms and definitions 6

2 ADDENDUM TO CC PART 1 8

2.1 Changes to *8.1.3, The selection operation* 8

2.2 Changes to *9.3, Protection Profiles* 8

2.3 Changes to *9.5, Using Multiple Protection Profiles* 13

2.4 Changes to *10.5, Conformance Claim* 13

2.5 Changes to *A.5, Security functional requirements (SFRs)* 15

2.6 Changes to *A.9.1, Security functional requirements (SFRs)* 16

2.7 Changes to *B.2, Mandatory contents of a PP* 17

2.8 Changes to *B.5, Conformance claims (APE_CCL)* 17

2.9 Changes to *B.9, Security requirements (APE_REQ)* 17

2.10 Changes to *B.13.2, Conformance Claims* 18

2.11 Changes to *B.13.6, Security functional requirements* 19

2.12 Changes to *B.14.5, Conformance claims* 19

2.13 Changes to *B.15.1, Mandatory content of a PP-Configuration* 20

2.14 Changes to *B.15.5, Conformance claims* 20

2.15 Changes to *C.2.3, The selection operation* 22

2.16 Addition of *C.5, Optional SFRs* 22

2.17 Changes to *D.1, Introduction* 23

2.18 Addition of *D.2, Exact conformance* 24

3 ADDENDUM TO CC PART 3 29

3.1 Changes to *APE_CCL* 29

3.1.1 Changes to *APE_CCL.1.11C* 29

DRAFT - For Trial Use

3.1.2 Additions to *APE_CCL* 29

3.2 Changes to *ACE_CCL* 29
3.2.1 Additions to ACE_CCL Developer Elements 29
3.2.2 Additions to ACE_CCL Content Elements 29

3.3 Changes to *ACE_CCO* 30
3.3.1 Changes to *ACE_CCO.1.3C* 30

4 ADDENDUM TO THE CEM 31

4.1 Changes to work units associated with *APE_CCL* 31
4.1.1 Changes to work units associated with *APE_CCL.1.5C* 31
4.1.2 Changes to work units associated with *APE_CCL.1.6C* 33
4.1.3 Changes to work units associated with *APE_CCL.1.8C* 34
4.1.4 Changes to work units associated with *APE_CCL.1.9C* 34
4.1.5 Changes to work units associated with *APE_CCL.1.10C* 35
4.1.6 Changes to *APE_CCL.1.11C* and work units associated with *APE_CCL.1.11C* 36
4.1.7 Addition of *APE_CCL.1.12C* and associated work units 36
4.1.8 Addition of *APE_CCL.1.13C* and associated work units 37
4.1.9 Addition of *APE_CCL.1.14C* and associated work units 38

4.2 Changes to work units associated with *APE_REQ* 39
4.2.1 Changes to work units associated with *APE_REQ.1.2C* 39
4.2.2 Changes to work units associated with *APE_REQ.1.3C* 40
4.2.3 Changes to work units associated with *APE_REQ.2.2C* 40
4.2.4 Changes to work units associated with *APE_REQ.2.3C* 41

4.3 Changes to work units associated with *ACE_CCL* 41
4.3.1 Addition of *ACE_CCL.1.5C* and associated work units 41

4.4 Changes to work units associated with *ACE_CCO* 42
4.4.1 Changes to *ACE_CCO.1.3C* and associated work units 42

4.5 Changes to work units associated with *ASE_CCL* 43
4.5.1 Changes to work units associated with *ASE_CCL.1.5C* 43
4.5.2 Changes to work units associated with *ASE_CCL.1.8C* 45
4.5.3 Changes to work units associated with *ASE_CCL.1.9C* 47
4.5.4 Changes to work units associated with *APE_CCL.1.10C* 48

DRAFT - For Trial Use

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 iTC (PP or PP-Module authors) 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, as long as those Optional Requirements do not require additional Threats, Objectives, or OSPs. This allows flexibility that otherwise would not be possible in a PP or PP-Module with an exact 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 Exact conformance does not replace nor prevent strict or demonstrable conformance from being a valid conformance statement for PPs.

7 The framework to support Exact Conformance statements, Selection-Based SFRs, and Optional SFRs is defined in Chapter 2. The additions required to

DRAFT For Trial Use

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) documents in context, rather than having solely stand-alone text.

1.2 Scope

8 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); and the definition and use of Optional SFRs. 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 Selection-Based SFRs, Optional SFRs, and require Exact Conformance.

1.3 Audience

9 This document is intended for PP authors, ST authors, and evaluators.

1.4 Normative References

10 The following references apply to this document.

11 [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.

12 [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.

13 [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.

14 [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)

15 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.

16 **exact conformance** – hierarchical relationship between a PP and an ST where all the requirements in the PP also exist in the ST, but not more, which is a special case of 'strict conformance'.

DRAFT - For Trial Use

17 Exact conformance is expected to be used in cases where the PP author requires that only the functionality and assurance requirements expressed in the PP be claimed in a conformant PP-configuration, PP or ST.

18 **optional Security Functional Requirement** – An SFR in a Protection Profile that contributes to a stated aspect of the PP's security problem description, but can be included or not included in a conformant ST's list of SFRs.

19 **selection-based Security Functional Requirement** – An SFR in a Protection Profile that contributes to a stated aspect of the PP's security problem description that must be included in a conformant ST if certain PP-identified selection operations are carried out.

DRAFT - For Trial Use

2 Addendum to CC Part 1

20 The additions required to support the concepts of exact conformance, selection-based SFRs, and optional SFRs 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.)

21 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.

22 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.

23 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.

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

25 As indicated in Section B.9, a PP 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. These SFRs must be included in a PP or ST if 1) a selection choice identified in the PP indicates that it has an associated selection-based SFR and 2) that selection is made by the PP or ST author. For a) above, a PP author would leave the list of selection-based SFRs unchanged. For c) above, a PP author would remove any selection-based SFRs from the list that correspond to the choices removed. For b) above, both PP and ST authors would include the appropriate selection-based SFRs in the list of SFRs for the PP/ST.

2.2 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.)

26 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

DRAFT - For Trial Use

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 B.

27 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.

28 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 B.5) 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.

29 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.

30 While in general an ST or PP can claim conformance to multiple PPs, because of the nature of exact conformance (that is, if a PP requires exact conformance, then only those SFRs and SARs specified by that PP are allowed in the conformant ST or PP) there are additional stipulations that need to be made. If a PP requires exact conformance in its conformance statement, it must also specify which, if any, additional PPs that are allowed to be claimed by another PP or ST at the same time (in other terms, the PPs that are *allowed with* that PP). These additional PPs must also require exact conformance in their conformance statement.

31 Then, an ST can only claim exact conformance to multiple PPs where at least one PP has an exact conformance statement if 1) all PPs to which it is claiming conformance have an exact conformance requirement and 2) all PPs to which it is claiming conformance are identified by as being “allowed” by all other PPs in their conformance statement.

DRAFT - For Trial Use

32 The same is true for a PP claiming conformance to multiple PPs, but there is an additional stipulation in this case. The conformance statement of the PPs to which conformance is being claimed must identify the "claiming PP" as being allowed to claim that PP in its conformance statement (in other words, "*allowed to claim*").

33 See Annex D for additional information.

34 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.

35 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.

36 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.

37 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;

DRAFT - For Trial Use

- 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.

38 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.

39 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;

DRAFT - For Trial Use

- 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).

40 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.

41 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

DRAFT - For Trial Use

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.

42 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.

2.3 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.)

43 The CC also allows PPs to conform to other PPs, allowing chains of PPs to be constructed, each based on the previous one(s).

44 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.

45 However, as previously indicated, a PP that requires exact conformance has additional stipulations, such that all PPs used in chains mentioned above would require exact conformance statements and identify all PPs used in the chain to be allowed to be combined with all of the other PPs in that chain. Further, all PPs that claimed conformance to other PPs would have to be listed in those PPs' conformance statement as being allowed to claim conformance to them.

2.4 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.)

46 The conformance claim indicates the source of the collection of requirements that is met by a PP 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 or ST claims conformance.

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

DRAFT - For Trial Use

– **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or

– **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP 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 or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or

– **CC Part 3 extended** - A PP 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.

47 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 or ST is conformant to a pre-defined package (e.g. EAL) if:

– the SFRs of that PP or ST are identical to the SFRs in the package, or

– the SARs of that PP or ST are identical to the SARs in the package.

– *Package name Augmented* - A PP or ST is an augmentation of a predefined package if:

– the SFRs of that PP 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 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.

48 It should be noted that, due to the definition of exact conformance, any packages specified by the PP with a conformance statement of “exact conformance” are allowed in the conformance claim of a PP or ST only if the package conformance statement is “package name Conformant”. Packages not specified by the PP, or “package name Augmented” claims, are not allowed against PPs with an exact conformance conformance statement.

DRAFT - For Trial Use

49 Note also 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.

50 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) - This statement describes the manner in which PPs or STs must conform to this PP: exact, strict, or demonstrable. For exact conformance, the statement also includes the PPs and packages allowed be used (in an exact conformance claim) with the PP; PP-Modules that may use this PP as a base PP in a PP-configuration, as well as PPs that are allowed to claim conformance to the PP. For more information on this Conformance Statement, see Annex B.

51 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),

– if a base PP has a conformance statement of exact conformance, then all base PPs in that set of base PPs must have conformance statements of exact conformance; must allow the combination of those PPs in the conformance statements for all base PPs; and must allow all modules in the PP-configuration to be used with that base PP.

– an ST may claim conformance with one or more PP-Configurations. A conformance claim to more than one PP-configuration is allowed only if the conformance statement for the PP-configuration is strict or demonstrable.

2.5 Changes to *A.5, Security functional requirements (SFRs)*

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

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

– Part 2 and Part 3 of this International Standard;

– Protection Profiles (if any);

– Packages (if any).

DRAFT - For Trial Use

53 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).

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

55 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.

56 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. However, if the PP-configuration requires exact conformance, then the ST can only claim a single PP-configuration; it cannot be combined with other PP-configurations.

2.6 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.)

57 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.

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

59 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.

DRAFT - For Trial Use

60 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.

2.7 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;

2.8 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.)

61 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 A.5), with one exception: the conformance statement.

62 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:

63 A) Other PPs to which a PP or ST can claim conformance to in combination with the subject PP and still maintain exact conformance.

64 B) Packages to which a PP or ST can claim conformance to in combination with the subject PP and still maintain exact conformance.

65 C) PP-Modules that can specify the subject PP as a base PP for use with that PP-Module in a PP-configuration.

66 D) Other PPs that are allowed to claim conformance to the subject PP and still maintain exact conformance.

67 See Annex D for more details on this.

2.9 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.)

DRAFT - For Trial Use

68 This section is identical to the security requirements section of an ST as explained in Section A.9 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 8.1.

69 The PP may identify a set of SFRs as optional SFRs. These SFRs can be included in a conforming PP or ST—even if the conformance statement of the containing PP requires exact conformance.

70 The PP may identify a set of selection-based SFRs. For each SFR (or set of SFRs) identified as selection-based, the PP author additionally ensures that the PP clearly indicates the dependencies between a particular selection in an SFR included in the PP and the selection-based SFR(s) that should be included if that selection is chosen by another PP or ST author.

2.10 Changes to *B.13.2, Conformance Claims*

(changes [CC-1], Section B.13.2; the entire section is repeated below for context and ease of application, with the changes highlighted.)

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

– The conformance to the PP(s) whose conformance is claimed in the Base-PP(s).

– The conformance to SAR packages (including predefined EAL) from the Base-PPs. The issue of ANDed Base-PPs with different EALs has to be dealt with like in an ST conformant to all those PPs (meaning that the ST has to claim the level of the minimum EAL of all the Base-PPs).

– The conformance statement (exact, strict, or demonstrable) from the Base-PPs. The issue of ANDed Base-PPs with different conformance statements has to be dealt with like in an ST conformant to all those PPs.

72 Note that a Base-PP with exact conformance is not allowed to be combined with Base-PPs with other types of conformance.

73 If the PP-Module inherits a conformance claim from a set of base PPs of exact conformance, then the PP-Module also may list in its conformance statement a set of other PP-Modules that are allowed to be specified in a PP-Configuration with that PP-Module (in combination with the base PPs requiring exact conformance). 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.

DRAFT - For Trial Use

2.11 Changes to *B.13.6, Security functional requirements*

(changes [CC-1], Section B.13.6; the entire section is repeated below for context and ease of application, with the changes highlighted.)

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

– all the SFRs from the PP-Module(s) of the PP-Configuration.

– all the SFRs from the Base-PP(s) except those which are refined in the PP-Module(s). This may include selection-based and optional SFRs from the Base-PP(s).

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

2.12 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.)

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

– Part 2 of the Common Criteria: CC version and extended security requirements,

– SFR packages.

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

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

79 A PP-Module inherits the conformance statement (exact, strict, or demonstrable) from the Base-PPs. The issue of ANDed Base-PPs with different conformance statements has to be dealt with like in an ST conformant to all those PPs.

80 Note that a Base-PP with exact conformance is not allowed to be combined with Base-PPs with other types of conformance.

81 If the PP-Module inherits a conformance claim from a set of base PPs of exact conformance, then the PP-Module also may list in its conformance statement a set of other PP-Modules that are allowed to be specified in a PP-Configuration with that PP-Module (in combination with the base PPs requiring exact conformance). This is to maintain the exact conformance

DRAFT - For Trial Use

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.

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

(changes [CC-1], Section B.15.1 paragraph 531; only the Conformance Statement *item is changed as indicated below.)*

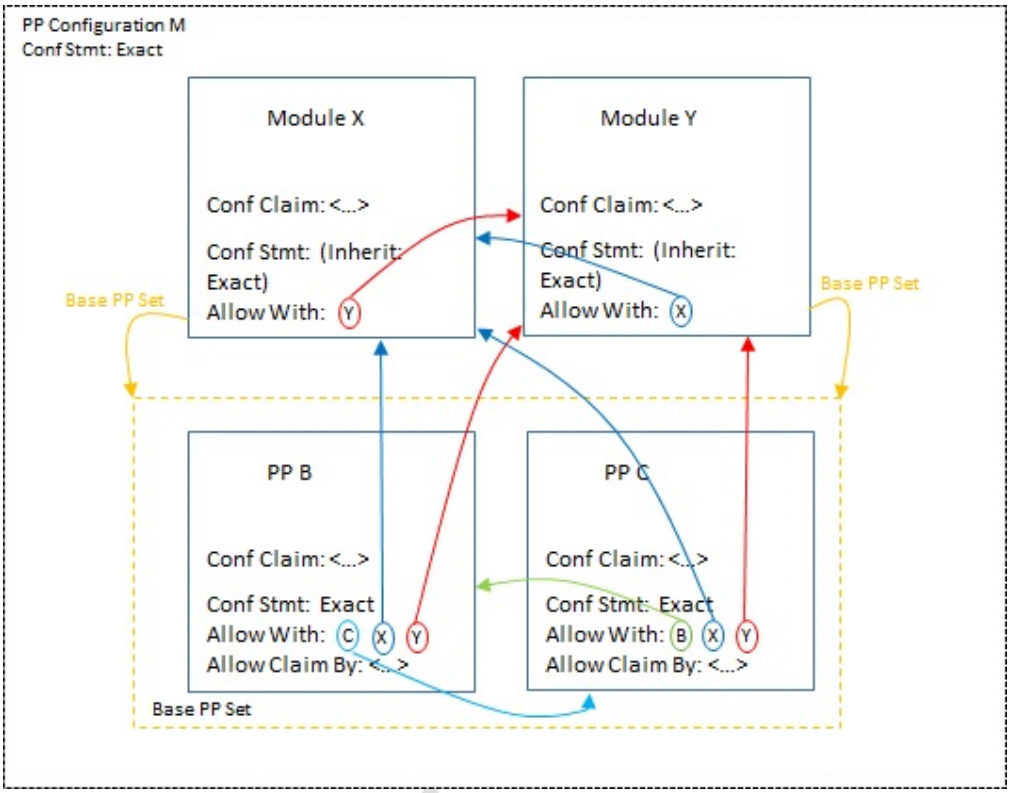
– a *Conformance statement*, that specifies whether the conformance to this PP-Configuration has to be exact, strict, or demonstrable,

2.14 Changes to *B.15.5, Conformance claims*

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

82 The *Conformance statement* specifies whether the conformance to this PP-configuration has to be exact, strict, or demonstrable. If a base PP (and therefore PP-module) in the PP-configuration has an exact conformance statement, then all base PPs (and PP-modules) in the PP-configuration must have exact conformance statements. Further, all base PPs and PP-modules in the PP-configuration must allow all other base PPs and PP-modules to be combined in their respective conformance statements. This is illustrated in the following example:

DRAFT - For Trial Use



83

84 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 set of base PPs: 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.

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

DRAFT - For

2.15 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.)

86 As described in section 8.1.3 the selection operation occurs where a given component contains an element where a choice from several items has to be made by the PP/ST author.

87 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 ...”

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

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

90 *Application Note:*

91 *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.*

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

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

94 *FCS_IPSEC_EXT.1 […]*

2.16 Addition of *C.5, Optional SFRs*

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

95 **C.5 Optional SFRs**

96 Optional SFRs are specified in the Protection Profile as SFRs that address some aspect of the Security Problem Definition for that PP, but supplement other (non-optional) SFRs in the PP. Therefore, it is left to the ST author’s discretion whether to include such SFRs in an ST or not, depending on whether the TOE supports the functionality specified.

97 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.

DRAFT - For Trial Use

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.

2.17 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.)

98 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.

99 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.

100 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 B.5) 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.

101 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.

102 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.

103 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

DRAFT - For Trial Use

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.

2.18 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.)

104 **D.2 Exact conformance**

105 Exact conformance is oriented to the PP-author who requires evidence that the requirements in the PP 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 in the PP without making additional claims.

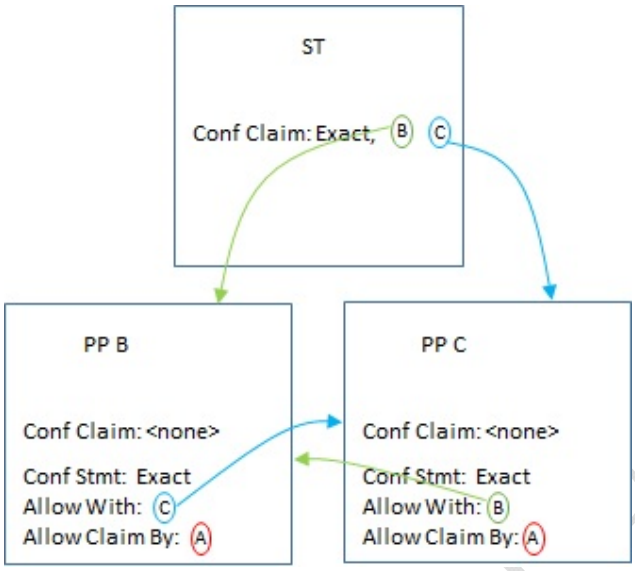
106 The CC allows STs and PPs to claim conformance to multiple PPs. In the case where a PP requires exact conformance, this has the potential to circumvent the intent behind exact conformance, which gives the PP author more control over the functionality and assurance provided for conformant STs than 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.

107 To address this issue, the conformance statement in the PP (see section B.5) may also include two statements: a statement of which PPs an ST or PP author may simultaneously claim conformance to with the subject PP (the *allowed with* statement); and a statement of which PPs are allowed to claim conformance to the subject PP (the *allowed to claim* statement). All identified PPs must require exact conformance in their conformance statement, and must also list the subject PPs (and all other PPs being claimed) in their conformance statement.

108 Two examples are given to clarify these concepts; one for an ST claiming conformance to multiple PPs, and another for a PP wishing to claim conformance to multiple PPs.

109 For the ST 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.

DRAFT For Trial Use



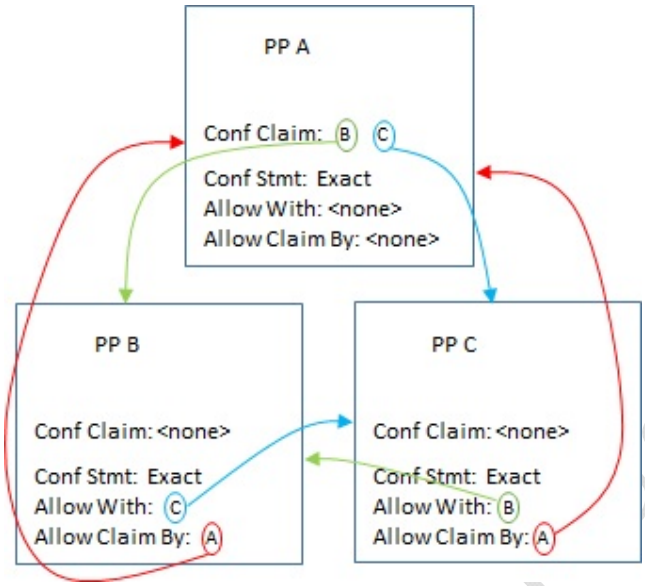
110 Then the following would have to be true:

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.

111 If any of these statements did not hold, then the ST could not claim (exact) conformance to PPs B and C. Note that PPs B and C also all a conformance claim to them by PP A, but that is not relevant for determining ST conformance.

112 The PP example is similar. For this example, PP A wishes to claim conformance to PP B and PP C. Since PP B and PP C require exact conformance, in order for PP A to claim conformance to them, it too must require exact conformance in its conformance statement. This situation is pictured below.

DRAFT For Trial Use



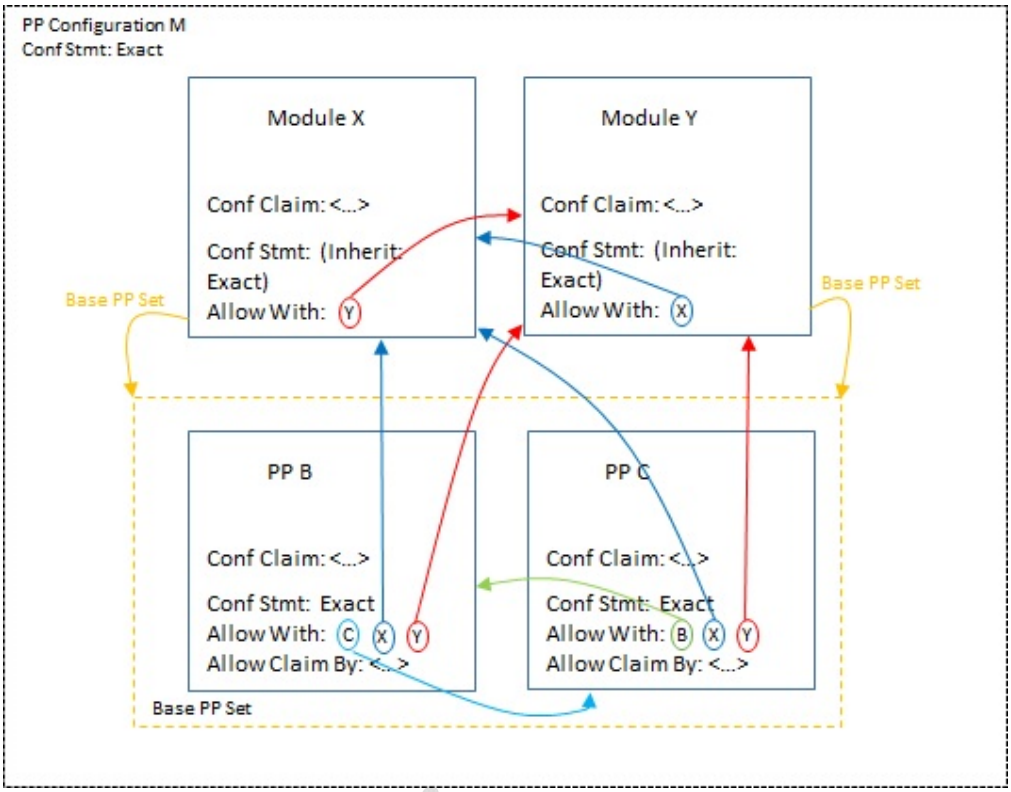
113 Then the following would have to be true:

1. PPs A, 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.
4. PP A would have to be listed as a PP that was allowed to be claimed by both B and C in PP B's and C's conformance statement.

114 If any of these statements did not hold, then PP A could not claim (exact) conformance to PPs B and C.

115 This concept is also extend to PP-modules and PP-configurations. A PP-module can identify a set of base PPs; if one of the base PPs in a set requires exact conformance, then all base PPs require exact conformance. In order to ensure that the requirement sets of the modules are allowed for use with the base PP, each base PP will identify (in its conformance statement) any PP-modules that are allowed to specify it as a base PP for use in a PP-configuration. Further, PP-modules will also specify what other PP-modules may be used in combination in a PP-configuration. The following example illustrates this:

DRAFT - For Trial Use



116 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 set of base PPs: 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.

117 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

DRAFT - For

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.

DRAFT - For Trial Use

3 Addendum to CC Part 3

118 In order to implement and verify the concept of exact conformance in [CC-3], changes to and additions of elements need to be made for the APE_CCL, ACE_CCL, and ACE_CCO families. These are 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.1.11C*

(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.**

3.1.2 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 packages and other PPs 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 that are allowed to specify the PP under evaluation as a base PP.**

APE_CCL.1.14C **The conformance statement shall identify the set of other PPs that can claim exact compliance to the PP under evaluation.**

3.2 Changes to *ACE_CCL*

3.2.1 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.**

3.2.2 Additions to ACE_CCL Content Elements

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

ACE_CCL.1.5C **The conformance statement shall identify other PP-modules that, in combination with the module under evaluation, can be used in a PP-configuration.**

DRAFT - For Trial Use

3.3 Changes to *ACE_CCO*

3.3.1 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 Base-PP(s) and PP-Module claim conformance.**

DRAFT - For Trial Use

4 Addendum to the CEM

119 The additions required to support the concepts of exact conformance, selection-based SFRs, and optional SFRs 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. Adds work units APE_CCL.1-6a, APE_CCL.1-6b, and APE_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].)

APE_CCL.1-6a The evaluator ***shall check*** that, for each PP to which the PP 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.

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

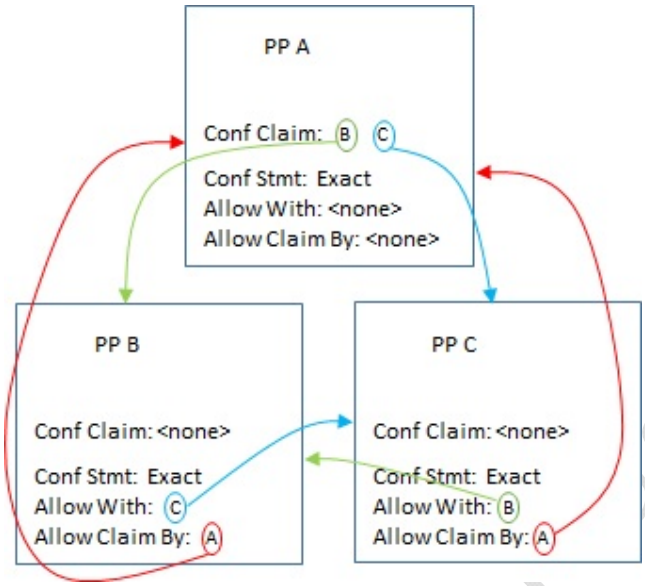
121 If the PP does not require exact conformance in its conformance statement, this work unit is not applicable and therefore considered to be satisfied.

122 If a PP to which conformance is being claimed requires either strict or demonstrable conformance (and the PP being evaluated is claiming exact conformance to a set of PPs), then this work unit fails since if a PP claims exact conformance to other PPs, those other PPs must require exact conformance as well.

123 The evaluator determines that the conformance statement of the PP to which conformance is being claimed lists each of the PPs identified in the conformance claim section of the PP being evaluated as being "allowed to be claimed with" that PP. Note that this is only applicable in cases where that PP requires exact conformance and the PP being evaluated requires exact conformance.

124 For example, consider the case where PP A is being evaluated and claims conformance to PPs B and C; this is depicted in the figure below. All PPs require exact conformance in their conformance statements. Under this work unit, the evaluator determines that PP B lists (in its conformance statement) "PP C" as being a PP that can be claimed (by another PP; in this case PP A) with PP B. Likewise, the evaluator determines that PP C lists (in its conformance statement) "PP B" as being a PP that can be claimed (by another PP; in this case PP A) with PP C.

DRAFT - For Trial Use



APE_CCL.1-6b The evaluator ***shall check*** that, for each PP to which the PP claims conformance, the conformance statement of that PP lists the PP being evaluated as a PP that is allowed to claim conformance with that PP.

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

126 If the PP does not require exact conformance in its conformance statement, this work unit is not applicable and therefore considered to be satisfied.

127 If a PP to which conformance is being claimed requires either strict or demonstrable conformance (and the PP being evaluated is claiming exact conformance to a set of PPs), then this work unit fails since if a PP claims exact conformance to other PPs, those other PPs must require exact conformance as well.

128 The evaluator examines each PP to which the PP being evaluated claims conformance. The evaluator determines that all PPs require exact conformance. The evaluator determines that that PP's conformance statement lists the PP being evaluated as one that is allowed to claim conformance to that PP. In the example above, This means that PP A (the PP being evaluated) must be listed by both PP B and PP C (since PP A is claiming conformance to both of those PPs) as being allowed to claim conformance to those PPs in their respective conformance statements.

APE_CCL.1-7a The evaluator ***shall check*** that the conformance statement of each PP to which the PP claims conformance lists each package identified in the conformance claim of the PP being evaluated.

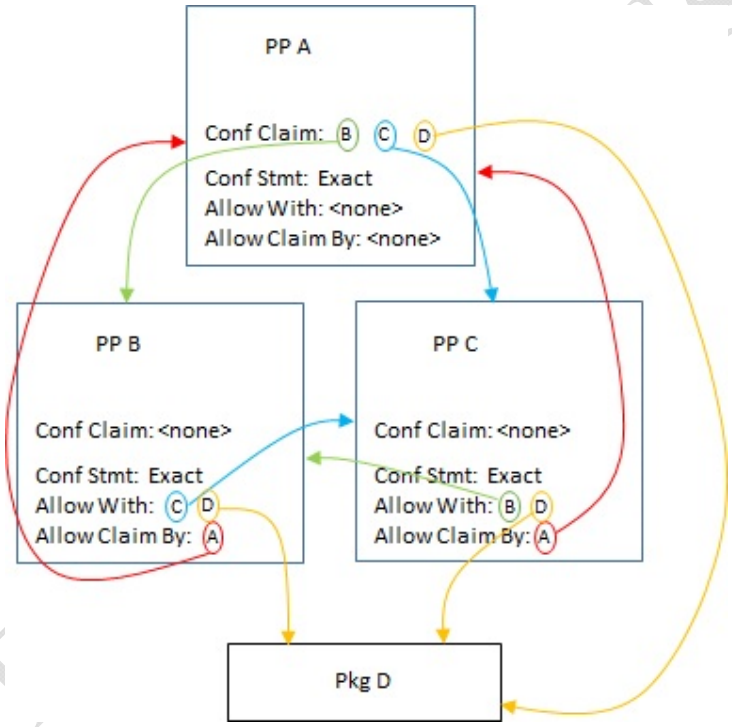
129 If the PP does not claim conformance to a package, this work unit is not applicable and therefore considered to be satisfied.

DRAFT - For Trial Use

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

131 If the PP does not require exact conformance in its conformance statement, this work unit is not applicable and therefore considered to be satisfied.

132 This work unit is only applicable when the PP being evaluated 1) requires exact conformance; 2) claims exact conformance to other PPs; 3) claims conformance to a package. In these cases, the evaluator ensures that each PP to which conformance is being claimed lists the package (or packages) as ones that are allowed to be used with those PPs. This is illustrated in the following example:



133 In the example, PP A is claiming (exact) conformance with PPs B and C, and also claiming conformance to Package D (since the conformance statement for PP A requires exact conformance, then the conformance claim for Package D must be Package D-conformant; Package D-augmented is not allowed). For this work unit, then, the evaluator examines the conformance statements for both PP B and PP C. These must list Package D as being allowed to be used in a conformance claim with that PP.

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

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

135 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.

136 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.

c) The conformance statement for the PP is either "strict" or "demonstrable".

4.1.3 Changes to work units associated with *APE_CCL.1.8C*

(changes [CEM] work unit APE_CCL.1-10. Due to the length of the work unit and the minor change necessary, 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 177 and 178.))

137 If exact conformance is required by the PP being evaluated, then this work unit is not applicable (the work has been done when listing the PP being evaluated in the conformance statements of the PPs to which this PP is claiming conformance) and therefore considered to be satisfied.

4.1.4 Changes to work units associated with *APE_CCL.1.9C*

(changes [CEM] work unit APE_CCL.1-11. Due to the length of the work unit and the minor change necessary, 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 181 and 182.))

138 If exact conformance is required by the PP being evaluated, then this work unit is not applicable (the work has been done when listing the PP being evaluated in the conformance statements of the PPs to which this PP is claiming conformance) and therefore considered to be satisfied.

DRAFT - For Trial Use

4.1.5 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.)

APE_CCL.1-12 The evaluator ***shall examine*** the PP 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.

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

140 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 PPs to which conformance is being claimed is 1) completely contained in and 2) identical at the SFR component level (for example, no hierarchically higher or lower components are allowed) to the statement of security requirements in the PP being evaluated, with the following allowances:

- an SFR from the PP may be iterated or refined in the PP being evaluated,
- SFRs identified as optional in the PP to which conformance is being claimed may or may not be included in the PP being evaluated.
- all SFRs that are defined in the PP to which conformance is being claimed as selection-based for a particular selection shall be included if and only if that selection on which inclusion is based is present in the PP being evaluated.

141 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 PP under evaluation is a superset of or identical to the statement of security requirements in the PP to which conformance is being claimed (for strict conformance).

142 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 PP under evaluation is equivalent or more restrictive than the statement of security requirements in the PP to which conformance is being claimed.

143 For:

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

DRAFT - For Trial Use

claiming conformance would also meet the requirements defined by the set of all SFRs in the PP to which conformance is claimed;

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

4.1.6 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.

4.1.7 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 packages and other PPs 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 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.

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

145 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.

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

APE_CCL.1-15 The evaluator ***shall check*** the conformance statement to determine it lists the set of Packages which are allowed in combination with the PP being evaluated when an exact conformance claim (in an ST or PP) is being made against the PP being evaluated.

DRAFT - For Trial Use

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

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

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

4.1.8 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 that are allowed to specify the PP under evaluation as a base PP.***

APE_CCL.1-16 The evaluator ***shall check*** the conformance statement to determine it lists the set of PP-modules that are allowed to use the PP as a base PP in a PP-configuration.

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

151 If the PP does not allow any PP-module to use it as a base PP in a PP-configuration, then the evaluator confirms that no PP-modules are listed.

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

APE_CCL.1-17 The evaluator ***shall check*** the conformance statement to determine that, for each PP-module that lists the PP as a base PP, all other PPs listed by that PP-module in the same base set are listed as allowed to be used with the PP being evaluated.

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

154 If the PP does not allow any PP-module to use it as a base PP in a PP-configuration, then this work unit does not apply and is therefore considered satisfied.

155 The evaluator examines the list of base PPs specified for each PP-module identified in the subject PP's conformance statement. A PP-module can have several sets of base PPs, but the only set that the evaluator has to examine is the one that includes the PP being evaluated. The evaluator determines, for every other PP listed in that set, the conformance statement of the PP being evaluated has those other PPs listed as allowed to be used with the subject PP.

DRAFT - For Trial Use

156 For example, suppose PP A is being evaluated. PP A specifies exact conformance in its conformance statement. It also specified that it can be used with PP-module X and PP-module Y in a PP-configuration. PP-module X specifies just one set of base PPs: PP A, PP B, and PP C. PP-module Y, on the other hand, specifies 3 sets of base PPs: set 1 is PP A and PP B; set 2 is PP C and PP Q; and set 3 is PP A and PP D.

157 Then for this work unit, the evaluator would determine that:

158 1) PP-module X and PP-module Y were listed in PP A's conformance statement as being "allowed" PP-modules.

159 2) For PP-module X, PP A needs to have PPs B and C listed in the conformance statement as being allowed to be used with PP A.

160 3) For PP-module Y, PP A needs to have PP B listed in the conformance statement as being allowed to be used with PP A for base set 1.

161 4) For PP-module Y, the evaluator ignores base set 2 since it does not include PP A.

162 5) For PP-module Y, PP A needs to have PP D listed in the conformance statement as being allowed to be used with PP A for base set 3.

4.1.9 Addition of *APE_CCL.1.14C* and associated work units

(adds [CEM] statement of APE_CCL.1.14C to correspond to [CC-3], and adds associated (new) work units.)

APE_CCL.1.14C ***The conformance statement shall identify the set of other PPs that can claim exact compliance to the PP under evaluation.***

APE_CCL.1-18 The evaluator ***shall check*** the conformance statement to determine it lists the set of PPs that are allowed to make an exact conformance claim with the PP under evaluation.

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

164 If the PP does not allow other PPs to claim of exact conformance to it, then the list is empty and this work unit is considered satisfied.

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

166

DRAFT - For Trial Use

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.

167 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; that is, SFRs that may or may not be included in a PP or ST claiming conformance to this PP, at the PP/ST author's discretion.

– 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.

168 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.

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

170 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.

DRAFT - For Trial Use

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.

171 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.

172 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.

173 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; that is, SFRs that may or may not be included in a PP or ST claiming conformance to this PP, at the PP/ST author’s discretion.
- 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.

DRAFT - For Trial Use

174 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.

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

176 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.

177 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.

178 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 to work units associated with *ACE_CCL*

4.3.1 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 statement shall identify other PP-modules, in combination with the module under evaluation, that can be used in a PP-configuration.***

ACE_CCL.1-5 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.

DRAFT - For Trial Use

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

180 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 conformance statement, and the evaluator ensures the PP-configuration contains no other PP-modules in the PP-configuration's components statement.

181 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 conformance statement.

4.4 Changes to work units associated with *ACE_CCO*

4.4.1 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 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.

182 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 Base-PP(s) and PP-Module claim conformance.

183 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 Base-PP(s) and PP-Module.

184 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. 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.

DRAFT: For Trial Use

185 CC versions used in a PP-Configuration and its underlying 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 base PP, all PP-modules specified in the components statement is listed as allowed to be used with that base PP.

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

187 The evaluator examines each base 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 conformance statement.

4.5 Changes to work units associated with *ASE_CCL*

4.5.1 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].)

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.

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

189 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.

190 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).

191 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.

DRAFT - For Trial Use

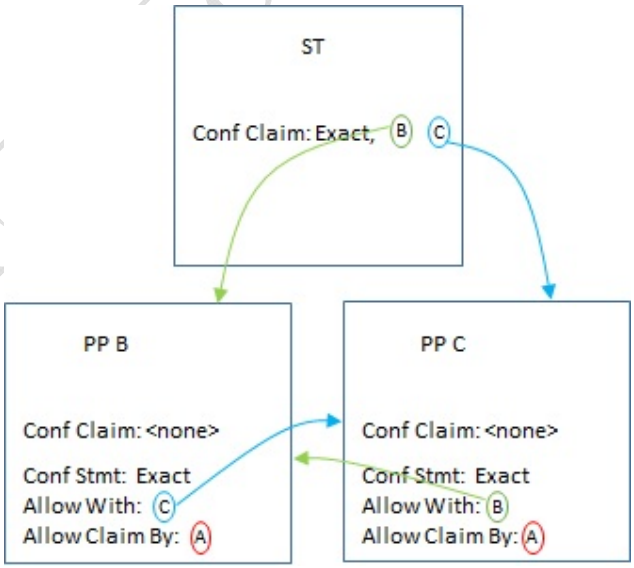
ASE_CCL.1-6a The evaluator ***shall check*** that, for each PP to which the ST claims conformance, the conformance statement of that PP allows all other PPs in the conformance claim to be allowed to be claimed with that PP.

192 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.

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

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

195 For example, consider the case where an ST is being evaluated and claims conformance to PPs B and C; this is depicted in the figure below. The ST is claiming exact conformance, so all PPs require exact conformance in their conformance statements. Under this work unit, the evaluator determines that PP B lists (in its conformance statement) "PP C" as being a PP that can be claimed (by an ST) with PP B. Likewise, the evaluator determines that PP C lists (in its conformance statement) "PP B" as being a PP that can be claimed (by an ST) with PP C.



APE_CCL.1-7a The evaluator ***shall check*** that the conformance statement of each PP to which the ST claims conformance lists each package identified in the conformance claim of the ST.

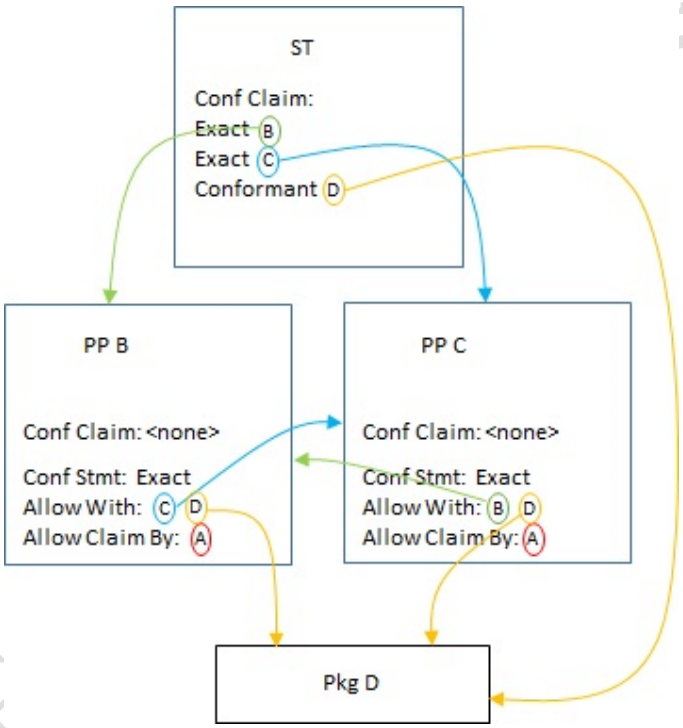
196 If the ST does not claim conformance to a package, this work unit is not applicable and therefore considered to be satisfied.

DRAFT for Trial Use

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

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

199 This work unit is only applicable when the ST being evaluated 1) claims exact conformance to one or more PPs; 2) claims conformance to a package. In these cases, the evaluator ensures that each PP to which conformance is being claimed lists the package (or packages) as ones that are allowed to be used with those PPs. This is illustrated in the following example:



200 In the example, the ST is claiming (exact) conformance with PPs B and C, and also claiming conformance to Package D (since the conformance claim to PPs B and C is exact conformance, then the conformance claim for Package D must be Package D-conformant; Package D-augmented is not allowed). For this work unit, then, the evaluator examines the conformance statements for both PP B and PP C. These must list Package D as being allowed to be used in a conformance claim with that PP.

4.5.2 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.))

DRAFT

201 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.

c) 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

DRAFT - For Trial Use

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.

4.5.3 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.))

202 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.

DRAFT - For Trial Use

4.5.4 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.

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

204 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.

205 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).

206 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.

DRAFT - For Trial Use

207 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).

208 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.

209 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.

DRAFT - For Trial Use