
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.3/010

1 March 2007

Status: Endorsed for use in UK Scheme

Subject: Use of Extended Components for Specifying Optional Requirements in a PP

REFERENCES CC, Version 2.3, August 2005

Issue

1. This interpretation addresses the question of how a PP author can direct the ST author to choose between two (or more) CC Part 2 components, where the PP author considers either alternative to be an acceptable means of meeting a given TOE security objective.

Scope of Interpretation

2. This interpretation is not intended to *directly* address the question of permitting the use of alternative CC Part 2 components to express the same requirement.
3. Whilst the issue described above is expressed in terms of CC Part 2 components, this interpretation does not *explicitly* rule out the possibility of its application to CC Part 3 components. However, as will be explained, it is not anticipated that there will be many cases where choice is required between different assurance requirements.

Premises

4. This interpretation is based upon the following premises:
 - a. CC does not permit a PP to specify optional requirements for a compliant ST to meet: in order to comply with a PP, all requirements in the PP must be satisfied. (The exception being where a PP requirement is not applicable to a particular environment.)
 - b. The selection operation, if uncompleted in a PP, provides a capability for an ST author to choose between different options within the same requirement element, and CC does not preclude the use of such operations within extended components.
 - c. It is valid to construct PP TOE security objectives that can be satisfied by different SFRs, i.e. that do not uniquely point to a specific CC Part 2 component.

Interpretation

5. If a PP author wishes to include optional requirements based on CC requirements components, the PP author may construct an extended component that incorporates an uncompleted selection operation, in which the options correspond to the text of the CC requirements components that the PP author wishes the ST author to choose between.

6. Such specification of options, permitting choice between two requirements A and B, is subject to the following limitations:
 - a. The optional requirements A and B must contribute to meeting the same TOE (or IT environment) security objective(s), in the same general manner.
 - b. There must be no hierarchical relationship between A and B.
 - c. The resultant set of security requirements must satisfy all relevant APE_REQ.1 and APE_SRE.1 requirements, particularly with respect to clarity, self-consistency, and consideration of dependencies.
7. In practice (given the first limitation), the use of this technique will be limited to components that are closely related – almost certainly within the same requirements class, and very often within the same family. It would not, for example, be permissible to present a choice of options between FAU_STG.1 (which is primarily concerned with the integrity of generated audit data) and FAU_STG.3 (which is primarily concerned with the availability of generated audit data). Whereas both could contribute to meeting the same security objective, their contributions are different (albeit complementary).
8. The second limitation simply reflects the fact that if, for example, requirement B is hierarchic to requirement A, then an ST that satisfies B will also satisfy A. Hence, for any requirement in a PP, the PP author implicitly permits an ST author to choose any alternative requirement that is hierarchic to it.
9. Where the approach described in this interpretation is adopted, the PP should include appropriate application notes describing how to complete the selection operation. The notes should point out that (providing all operations are properly completed) the resultant requirement (based on the chosen CC Part 2 component) will conform to the PP’s (extended) requirement. The notes should also point out that if the ST author chooses more than one option, the ST will still conform to the PP (assuming the options are not mutually exclusive).
10. An example is the following requirement, which permits a PP author to direct a conformant TOE to provide for pre-selection (FAU_SEL.1) or post-selection (FAU_SAR.3) of auditable events.

FAU_SAR_SEL.1.1 The TSF shall [selection:

“provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations]”,

“be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection: object identity, user identity, subject identity, host identity, event type]; b) [assignment: list of additional attributes that audit selectivity is based upon]”].

11. It may be seen that this extended component comprises a selection operation consisting of two options. The first option in this selection operation contains the text of FAU_SAR.3.1, whilst the second contains the text of FAU_SEL.1.1. (Following CC Part 1 paragraph 165, either or both options may be selected in this example; “None” is not a valid selection.) The PP author should include an application note advising the ST author, when completing the selection operation, to replace the “FAU_SAR_SEL.1.1” label with the appropriate CC Part 2 element label(s).
12. Each of the (embedded) selection and assignment operations that form part of the FAU_SAR.3.1 and FAU_SEL.1.1 requirements elements must (naturally) also be

completed by the ST author. (Note that, alternatively, the PP author could have elected to complete any of these operations.)

13. The above example is a simple one, since both options contain only one requirement element. If, say, the optional components A and B each had two requirements elements, the extended component would similarly contain two elements, constructed in the following manner:

A_B.1 [selection: A.1, B.1]

A_B.2 [selection: A.2, B.2]

14. In such cases, the PP author would need to give clear direction to the ST author (in the form of application notes), to ensure that a consistent set of selections is made (i.e. if A.1 is chosen, then A.2 must also be chosen). It is not difficult to see that the situation becomes even more complex if the component options have differing numbers of elements.
15. An alternative presentation of such extended components – which is likely to be preferred where the options involve more than one requirements element - is for the extended component to incorporate a single requirements element. In this approach, the element contains a single selection operation, where each option corresponds to the **complete** text of a component. For example:

FAU_SAR_SEL.1.1 [selection:

*“FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: searches, sorting, ordering] of audit data based on [assignment: criteria with logical relations]”,
“FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes: a) [selection: object identity, user identity, subject identity, host identity, event type]; b) [assignment: list of additional attributes that audit selectivity is based upon]”].*

16. In this case, the PP should include an application note explaining that the extended component is, in effect, the following requirement:

“[selection: FAU_SAR.3, FAU_SEL.1]”.

17. Note that the FAU_SAR_SEL.1.1 label becomes redundant when the operation is completed, and should therefore be omitted from the ST. (The only reason for its inclusion in the PP is to ensure that the extended component satisfies the APE_SRE.1.4C requirement that it “shall use the CC requirements components, families and classes as a model for presentation”.)
18. Due consideration must be given to dependencies, to ensure that the PP/ST criteria are met. In the example given above, FAU_SAR.3 is dependent on FAU_SAR.1 (and, indirectly, FAU_GEN.1), whereas FAU_SEL.1 is dependent on FAU_GEN.1 and FMT_MTD.1. The PP author would therefore need to give careful consideration to how these dependencies should be reflected in the PP.
19. It may be noted that use of the technique described in this interpretation may result in the apparent paradox of a “CC Part 2 Conformant” ST being conformant with a PP that is “CC Part 2 extended”. In view of this, the UK Scheme recommends that the CCMB give due consideration to how this paradox might be avoided, e.g. by revisiting the definition of CC Conformance claims.

Rationale

20. Given premise a. above, there are only two methods of specifying options within a PP document:
 - a. Through the specification of optional functional packages in the PP document; however, such requirements are not part of the ‘core’ PP requirements that all STs must comply with.
 - b. Through the use of the selection operation within an SFR.
21. The functional package approach does not offer a solution to the specific issue raised by this interpretation, since the question to be addressed is how a PP author can specify options *within* the core set of PP requirements. Therefore, the only available solution would appear to be via use of a selection operation within an SFR – which of necessity must be an *extended* component.
22. The use of an extended component containing an open selection operation is valid (with respect to the APE_SRE.1 criteria for extended requirements). It is therefore possible, in principle at least, to use such a component as a vehicle for directing the ST author to choose between two or more options, where this is equivalent to presenting a choice between two (or more) CC Part 2 components.
23. The onus is then on the PP author to ensure that the extended requirement is properly worded, such that it is possible to use any of the ‘optional’ CC Part 2 components in such a way as to comply with the extended requirement.
24. The following are further examples of where the approach described in this interpretation is considered most likely to be applied. It should be stressed that the intent here is to provide illustrative examples; the list is not exhaustive, and does not in any way preclude the possibility of other combinations of options being specified in a PP.
 - a. The PP author may specify an extended component in order to select between FAU_SAA.2 and FAU_SAA.3 (or FAU_SAA.4, which is hierarchic to FAU_SAA.3). This would be appropriate if (for example), a PP author wished to mandate a more sophisticated form of intrusion detection than would be provided by FAU_SAA.1, but considered either option as acceptable for satisfying the ‘intrusion detection’ security objective.
Note that, in this example, the available options each comprise three requirements elements. The second form of presentation (“[selection: FAU_SAA.2, FAU_SAA.3]”) is thus likely to be preferred by the PP author. (The alternative would be an extended component of three elements, each of which would require selection operations providing the ability to choose between a FAU_SAA.2 element or the corresponding FAU_SAA.3 element. In this case, the PP would need to direct the ST author to make a consistent set of choices, e.g. it would not make sense for an ST author to complete the selections such that the ST mandated FAU_SAA.2.1 and FAU_SAA.3.2 as part of the same requirement.)
 - b. The PP author may specify an extended component in order to select between FIA_SOS.1 (user generated passwords) and FIA_SOS.2 (machine generated passwords). This might be appropriate where the PP author considers that the critical requirement is that the selected passwords satisfy the appropriate quality/strength metrics. (It may be noted that a PP that mandates FIA_SOS.1 is not satisfied by an ST that includes FIA_SOS.2 instead.)
One noteworthy aspect of this example is that FIA_SOS.1 contains one element,

whereas FIA_SOS.2 contains two. Again, the second form of presentation (“[selection: FIA_SOS.1, FIA_SOS.2]”) is likely to be preferred by the PP author. (The alternative would be an extended component of two requirements elements, the second of which would effectively present the ST author with the choice of either FIA_SOS.2.2, or a null requirement in the event that FIA_SOS.1 is the selected option. In this case, the PP would need to include an application note directing the ST author who chooses the FIA_SOS.1 option to, for the sake of clarity, omit the second (null) requirement element.)

- c. The PP author may specify an extended component in order to select between FPT_PHP.1 and FPT_PHP.3. This would be appropriate if (for the specified physical attacks) the PP author considers that either tamper detection or resistance is an appropriate means of satisfying the relevant TOE security objective. (Note that a PP which mandated FPT_PHP.1 would not be met by an ST that instead includes FPT_PHP.3.)
25. Other possible combinations of options include those cases where CC Part 2 identifies ‘optional’ dependencies, i.e. dependencies that can be met by more than one SFR. For example, FDP_UCT.1 is dependent on either FTP_ITC.1 or FTP_TRP.1.
 26. Whilst this interpretation is not explicitly intended to address cases where different CC Part 2 components can be used to express the same SFR, it is conceivable that the approach described here could be used. For example, this might be thought appropriate where potential conformant STs exist, but there is no established consensus as to the appropriate CC Part 2 component which should be used to articulate a particular SFR common to all (the PP author might not wish to be seen to favour one ST over another, or to needlessly force ST authors to rewrite their STs in order to claim PP compliance).
 27. As a final point, it may be noted that the principal reason why this interpretation has limited application to CC Part 3 components is that assurance requirements which have the same general objective will normally be found within the same CC Part 3 family – and all such families are organised such that there is a hierarchical relationship between all components in that family.