
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.3/012

1 March 2007

Status: Endorsed for use in UK Scheme

Subject: Multi-platform TOEs

REFERENCES CC/CEM, Version 2.3, August 2005

Issue

1. This interpretation addresses the case where a sponsor of an evaluation wishes for the resultant certificate to confirm that the TOE operates in accordance with its Security Target on a number of underlying platforms that are not part of the TOE. The issue of specific concern is what level of information must be supplied to the evaluators, and what activities must they undertake, in this scenario.

Scope of Interpretation

2. In the context of this interpretation, a *platform* is any hardware, firmware or software underlying the TOE that is required by the TOE for its operation, but which is outside the scope of the actual TOE. In other words, this interpretation applies where the underlying platform is part of the IT environment for the TOE.
3. Whilst the focus of this interpretation is on handling multi-platform claims where the platform is part of the IT environment, it rests on certain premises (stated below) as to how a TOE is evaluated on an underlying platform in the first instance.
4. This interpretation describes a generic approach for addressing platform dependencies. Where additional technology-specific issues need to be considered (for example, where the platform is a Smartcard/IC), these will be the subject of other CC Interpretations or CC Supporting Documentation.
5. Note that this interpretation complements, and is intended to be consistent with, UK CC Interpretation UK/2.3/008 *Treatment of commercial hardware that is part of a TOE*.

Premises

6. This interpretation is based upon the following premises:
 - a. The extent to which a TOE evaluation must consider an underlying platform (within its IT environment) is limited to those aspects of the platform on which the security of the TOE depends. This relates both to the support the platform provides for the TOE's SFRs, and to the introduction of potential vulnerabilities into the TOE. Where it is evident (e.g. from testing) that problems exist in the platform which compromise the security of the TOE, these issues must be addressed.
 - b. The principle of reuse of TOE evaluation results may be applied, provided it is supported by a sound rationale that justifies that the results are not impacted by

changes to the underlying platform. This permits a cost-effective approach to evaluating multi-platform claims.

7. It should be clear from the first premise is that there is no requirement to evaluate the platform itself, nor indeed to evaluate any security functionality which it offers. In other words, insofar as the TOE evaluation is concerned, the platform is to be treated as a 'black box'. Assurance that the underlying platform does not undermine the security of the TOE will thus derive primarily from:
 - a. The search for public domain vulnerabilities (which must include a determination of whether there are any obvious vulnerabilities in the platform that could undermine the TOE's SFRs), and
 - b. Testing of the TOE on the platform (which will – at least indirectly - cover all aspects of the platform upon which the security of the TOE depends).
8. It is otherwise assumed that the platform operates correctly to provide its specified functionality and contains no vulnerabilities. Where further assurance in the platform is required, the TOE boundary must be extended to include the platform (or specific platform functionality) within its scope.

Interpretation

9. Where the TOE is certified for more than one platform, then this is a declaration that equivalent assurance has been demonstrated for the evaluation of the TOE on each platform.
10. It is first necessary for a TOE to be fully evaluated on one platform.
11. The default position is then that all evaluation activities must be repeated in full for each underlying platform. In practice, however, the effect of a platform change is limited in scope: to the need for resultant change in the TOE itself for operation on the platform, and to the behaviour of the TOE when run on the platform.

Impact Analysis and Rationale

12. A rationale provides an acceptable basis for justifying that the security assurance requirements for the TOE are met across the range of platforms claimed in the ST, without recourse to repeated evaluation activity in respect of every one of those platforms.
13. At the heart of the rationale is an impact analysis that identifies the impact of platform changes on the assurance in the TOE, and correlates each impact to those evaluator actions which would, if repeated, demonstrate that the required assurance exists. The impact analysis may be developed further to justify that the nature of an identified platform change is such that it is not necessary to repeat a given evaluation activity (which may therefore be waived for that platform).
14. The sponsor is required to provide the following evidence in support of a multi-platform claim, in addition to the full set of CC deliverables (as directed by the security assurance requirements) in respect of the baseline platform referred to at paragraph 10 above:
 - a. All CC deliverables for the TOE where these are impacted by a platform variation.
 - b. Details of differences in the underlying platforms claimed.
15. Impact analysis and rationale is considered to be an evaluation activity that is based on the above evidence supplied by the sponsor. The sponsor may, nonetheless, choose to

additionally provide the impact analysis and rationale; in this event the impact analysis and rationale will be independently evaluated by the CLEF.

Content of a Rationale

16. A rationale must relate all security assurance requirements (SARs) to platform variations. The nature of the platform variations must be detailed. However, where there are a number of platforms, there may be benefit in employing a generic platform variation entity (e.g. clock speed) to characterise variations of that type.
17. Conceptually (if not actually in its presentation), this leads, in the first instance, to an impact analysis based on a 2 dimensional matrix, which comprises (say) rows for each of the SARs, and columns for the platform variation entities. For each cell in the matrix a justification must then be given to demonstrate that platform variation can have no effect on TOE assurance. There may, however, be scope for applying a given justification to a number of cells.
18. A third dimension to be considered is that of *assurance-related TOE entities*. These are TOE entities that relate to one or more SARs, and which may be affected in different ways by a given platform variation. Consideration of the impact of a platform variation on a SAR therefore requires that the impact on the different TOE entities be considered, where these relate to the SAR.
19. The table below identifies the assurance-related TOE entities that must, as a minimum, be considered by the rationale (where relevant to the SARs specified in the ST). The most commonly encountered potential impacts of a platform variation are also identified (to serve as illustrative examples). Further discussion and examples are provided at paragraphs 24-32 below.

Assurance-related entity	Possible impacts of a platform variation include:
SFRs	<ul style="list-style-type: none"> • The correct operation of a SFR may be affected. • There may be SFR-relevant changes to the TSF representations.
SOF-relevant mechanisms	The strength of function determination may be impacted.
Potential vulnerabilities	<ul style="list-style-type: none"> • Additional vulnerabilities may be introduced by a platform variation. • The rationale for non-exploitability of vulnerabilities, as declared for the TOE on the baseline platform, may be impacted.

20. The above list is not exhaustive. Firstly, it is limited in scope to the set of assurance requirements that are covered by CEM. Secondly, it explicitly addresses those assurance-related entities that are most commonly affected by platform variations; it is possible that other assurance-related TOE entities could be identified in specific cases.
21. It should be noted that, whilst the rationale must cover each assurance-related TOE entity, there is likely to be scope for applying a given justification to defined groups of TOE entities. For example, a rationale may address defined groups of SFRs (such as Security Audit) where the rationale applies to the group as a whole.

22. A verdict justification for an evaluation activity will be considered adequate if it is seen to follow logically, from a consideration of the impact of platform variation, that waiving repeated evaluation activity will not cause a reduction in assurance. Where appropriate the justification may reference other evaluation material. So, for example:
- a. A cell relating a set of FDP_IFF.2 (MAC) SFRs to clock speed may assert that this platform variation is of no concern, noting as justification that the vulnerability assessment activities uncovered no potential vulnerabilities that could take effect in this context.
 - b. A cell relating an FDP_RIP (Residual Information Protection) SFR to memory size would need to refer to the way in which mechanisms for clearing memory were implemented to justify that equivalent assurance exists for such a platform variation.
 - c. A cell relating an FPT_SEP (Domain Separation) SFR to platform memory management functions could offer no justification (and thus require repeated evaluation activity) wherever the memory management interface specification varies.
 - d. A cell relating a covert timing channel to clock speed would need to refer to an analysis of exploitable bandwidths within a covert channel analysis.
23. The following sections consider further the impact on deliverables and evaluator activities for those assurance aspects most commonly affected by platform variations (i.e. ASE, ADV, ATE and AVA, as noted at paragraph 20 above). This should not be construed as ruling out the possibility of there being an impact on other assurance aspects (i.e., ACM, ADO, AGD and ALC).

Security Target & Certification Report

24. The Security Target must specify the platforms on which the TOE is to be evaluated, in order to provide a clear definition of the evaluated configuration (following CEM Annex A.6).
25. The Certification Report will specify the platforms on which the TOE was evaluated. It will identify the platform(s) on which the TOE has been fully tested. It will also outline both the nature of variation between platforms and the means by which assurance has been achieved on the other platforms.

ADV

26. The TOE itself may require modification for its operation on different platforms. These modifications may exist at any level of TSF representation according to the impact of the platform variation (i.e. they may exist in object code, source code, low-level design, high-level design or the functional specification) but will typically be made at the lower levels of representation. For example:
- a. Porting a database from one operating system to another may involve the addition of new modules in the low-level design, in order to emulate functionality present in the first but not the second operating system.
 - b. Moving from a uniprocessor to a symmetric multiprocessor hardware architecture may involve modification of TOE source code.
 - c. The binary image of a TOE may contain a number of code paths, one of which is selected at run-time in order to correctly drive the hardware platform employed.
27. Platform variations assume significance when they involve a variation in the platform interface specification (e.g. involving a different chip instruction set). More generally, even where the platform interface specification does not vary, a platform variation may be significant where the platform functionality varies (e.g. involving a change in clock

speed). It is necessary not only to consider specific interface calls, but more generally to understand the role of the platform in contributing to or compromising the overall security of the TOE.

28. The evaluators must consider platform interface specifications at all assurance levels, in accordance with the requirements of the impact analysis and the deliverables supplied to support evaluation of the TOE. Increasing assurance levels will thus lead to greater rigour in the consideration of the TOE's usage of platform facilities.

ATE

29. Repeated developer and evaluator testing in respect of platform variations will be required at all evaluation levels, unless a rationale can be given to demonstrate equivalent assurance. Whilst the fewer deliverables required at lower assurance levels may offer less evidence on which to base a rationale, testing requirements are less onerous at these levels. Note that:
 - a. Developer testing covers testing of security functions and external interfaces. ATE_DPT.1 introduces the additional requirement for testing against the high-level design, covering TSF subsystems and their interfaces.
 - b. Different (additional) tests may be required on different platforms to reflect possible variations in effect, as part of the evaluator's independent testing (ATE_IND).
 - c. Independent testing of platform variations should form part of the evaluators' overall strategy for testing a subset of the TSF. Note that, within the context of this requirement, it is acceptable for the evaluators to adopt a risk-based approach in which testing focuses on those variations that are judged to carry the greatest risk of a vulnerability arising from an implementation error.

AVA

30. Changes to TSF representations may, of course, introduce vulnerabilities. However, even where modification of the TOE is not required, a platform variation may still affect its security. For example:
 - a. Moving a TOE, without modification, to a processor offering additional instructions, including privileged instructions accessible from user mode code, may introduce a vulnerability.
 - b. Moving from one hardware platform to another may be unacceptable on account of a BIOS vulnerability.
 - c. Whilst not requiring modification of the TOE, a change in hardware clock speed may be significant where covert timing channels are considered to constitute a threat.
 - d. The validity of a SOF analysis may be critically dependent on the underlying platform, as this may be the only limiting factor to the rate achievable for automated attack on a password mechanism.
31. The potential introduction of vulnerabilities into the TOE, as a result of platform variations, must be considered at all evaluation levels. Any potential vulnerabilities apparent to the sponsor must be addressed in updated vulnerability analysis deliverables. The evaluators will check for the introduction of vulnerabilities by reference to these and, as appropriate, any other deliverable.
32. Repeated penetration testing in respect of platform variations will be required at all evaluation levels unless a rationale can be given to demonstrate equivalent assurance, i.e. that such variations do not introduce new vulnerabilities, or undermine any arguments

presented by the developer that known vulnerabilities are not exploitable. Penetration testing must address any potential vulnerabilities arising from the TOE's usage of platform facilities. As with independent testing (ATE_IND), it is acceptable for the evaluators to focus their penetration testing on those variations that are judged to carry the greatest risk of vulnerability.

Application under Assurance Maintenance

33. A sponsor may provide an impact analysis and rationale in support of an Impact Analysis Report submitted under an Assurance Maintenance process. This approach may therefore - subject to the approval of the CB, and established case law - be used to extend the certificate to new platforms under maintenance. It is likely that one prerequisite for this is that the impact analysis and rationale demonstrates that the impact of platform changes on assurance is *Minor*, such that assurance is maintained if the developers repeat their tests (or a subset thereof) on the new platforms (or a representative sample of those platforms).

A Note on Compatibility Testing

34. Where the developer operates a Platform Compatibility Testing (PCT) facility, with platforms which pass the PCT placed on a Platform Compatibility List (PCL), he may wish for this testing to contribute to assurance.
35. In principle this is acceptable. As a first prerequisite however, PCT must incorporate those tests required for the evaluation level by impact analysis and rationale, in accordance with paragraph 29 above (if the developer wishes to incorporate lower level tests then it must be justified by rationale that this gives equivalent assurance). Essentially there are then two options in this area:
 - a. PCT test results (together with associated test plans, purposes and procedures) are supplied to the evaluators as a deliverable,
 - b. Subject to the agreement of the CB, the developer may cite the operation of PCT to justify platform changes as having a *Minor* impact on assurance, as part of an Assurance Maintenance process.
36. The following points should be noted where it is desired that PCT form part of an Assurance Continuity process:
 - a. PCT must be controlled by well-defined procedures. The CB or CLEF must have independently checked these procedures and their application.
 - b. The PCT procedures must place constraints on the type of platform variations that can be accommodated by PCT alone.
 - c. Where PCT has been operated before the evaluation of the TOE the evaluators will need to confirm that the necessary assurance holds for all PCL entries back to the first PCL entry.
 - d. Where PCT is operated after evaluation of the TOE as part of an Assurance Continuity process, there will a need for a check of the application of its procedures to confirm that the necessary assurance holds for all latter PCL entries. This may be carried out by the CB (under Assurance Maintenance) or by a CLEF (as part of a subsequent re-evaluation).
 - e. Further details of this process must be agreed with the CB.
37. Where PCT is further extended to encompass the developer's partners, then assurance will also need to be demonstrated in respect of their contribution.

Rationale

38. There is obvious benefit to the sponsor from certification of a TOE on a number of platforms. This interpretation seeks to outline the issues involved in multi-platform evaluations, and to indicate a general approach acceptable to the CB.