

---

## UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.2/002

25 February 2005

Status : Endorsed for use in UK Scheme

Effective from: 25 February 2005

Subject: Unsatisfied AVA\_VLA.2 dependencies in augmentation of EAL1

---

**REFERENCES** CC component - AVA\_VLA.2

### Issue

1. The PP "Intersector Electronic Purse and Purchase Device (Version for Pilot Schemes)" v1.2 - which has been evaluated and certified by the French CB (French certificate PP/9908) - requires an assurance level of EAL1 augmented with AVA\_VLA.2 (and no other components). AVA\_VLA.2 has dependencies on ADV\_HLD.2, ADV\_LLD.1 and ADV\_IMP.1, but none of these components is included in the resultant EAL1+ level. Section 7.3.4 of the PP argues that these dependencies are "not applicable in this context".
2. This raises two specific questions:
  - a) Is the statement that the assurance dependencies are "not applicable in this context" an acceptable justification as to why non-satisfaction of dependencies is appropriate (as is required by APE\_REQ.1.9C)?
  - b) In the case of AVA\_VLA.2, is it acceptable under any circumstances to argue that the dependencies on ADV\_HLD.2, ADV\_LLD.1 and ADV\_IMP.1 do not need to be satisfied?

### Interpretation

3. The statement referred to above is an assertion and not a justification. Therefore it is insufficient to satisfy requirement APE\_REQ.1.9C.
4. What is needed is an argument as a minimum which takes into account the threats and security objectives. In the case of assurance components, the PP/ST author needs also to consider the

Version 2.0

UK/2.2/002

reasons for the dependency and their indirect contribution to assurance provided by the component in question. For example whether non-satisfaction of a dependency means that - in assurance terms - there is little difference in practice between the component selected and another (lower) component in the same family.

5. The dependencies of AVA\_VLA.2 on ADV\_HLD.2, ADV\_LLD.1 and ADV\_IMP.1 cannot be dismissed as is done in the referenced PP. This is because the principal difference between AVA\_VLA.2 and AVA\_VLA.1 is the requirement for an independent vulnerability analysis (followed by penetration testing based on the analysis). The dependencies identified in CC Part 3 are there to ensure that there is sufficient evidence on which to base such an analysis. Given the information available at EAL1, it is unclear how the evaluation could be expected to identify anything other than obvious vulnerabilities. Therefore EAL1 augmented with AVA\_VLA.2 alone is misleading, because this provides no more assurance in practice than EAL1 augmented with just AVA\_VLA.1.