



Joint Interpretation Library

Collection of Developer Evidence

Version 1.0

August 2000

This document is paginated from i to iv and from 1 to 4

Table of contents

1	Background	1
2	Interpretation	1
2.1	Collection of evidence	1
2.2	Creation of evidence	2
2.3	Small deficiencies	2
2.4	Types of Assistance to Developer	2
2.5	Specific Cases	3

Collection of Developer Evidence

1 Background

- 1 The objective is to facilitate effective and flexible application of the Criteria. There is considerable flexibility in the form in which developers may supply deliverables as inputs to evaluation. This interpretation examines some of the alternatives that the developer may choose, and the ways in which the evaluator may respond while complying with the requirements of the criteria, EN45001 or guide ISO 25 (or the new standard ISO/IEC 17025), and mutual recognition. It also identifies and considers cases where there may be a danger that evaluators undertake work that is strictly outside their scope.
- 2 The way the Criteria are phrased, and traditional practice under ITSEC, imply that the developer should supply specific documents containing each particular type of evidence. Normally it will be most efficient if that is the case; the effort required by the evaluator to review the evidence will thereby be minimised. However, there is no explicit requirement on the format of the evidence; only the information content is prescribed. In particular cases it may be more efficient for the developer to present the evidence in more diffuse form, which requires more substantial evaluator effort to marshal and review. Provided that this can be done objectively and impartially, this *collection* of evidence is completely proper and acceptable.
- 3 The emphasis is on the objective justification of evaluation verdicts from developer-supplied deliverables. Where objective justification is not possible, the work becomes *creation* rather than collection of evidence. Since the intention of the criteria is that developers should demonstrate familiarity with the IT features of the TOE, and that they have taken care with the security aspects, it can only be in exceptional cases, with prior CB approval, that the evaluator can be allowed to create evidence.

2 Interpretation

- 4 This is an interpretation independent of the criteria.
- 5 The developer is responsible for providing the information required by the criteria. The evaluator may exceptionally provide some of this information provided that:
 - a) evaluator contributions are fully endorsed by the developer;
 - b) approval is given in advance by the CB, and;
 - c) the evaluator contributions are independently reviewed by other members of the evaluation team, and their review is documented in the ETR.

2.1 Collection of evidence

- 6 According to internationally agreed criteria and methodology, the developer must provide specified evidence but the format is not mandated. The evidence may be presented in a single document that addresses all the requirements of an assurance component, or the evidence may need to be collected from a number of documents.

Collecting evidence from a number of separate sources and formats is legitimate evaluator work. It may be convenient for the evaluator to construct a working document that approximates the ideal developer deliverable, but it is not mandatory. The evaluator work must be limited to the objective *collection* of developer-supplied material, rather than subjective *creation*, so that it remains repeatable, reproducible and impartial. A suitable test is whether any competent evaluator would obtain essentially the same result.

2.2 Creation of evidence

7 The difference between objective collection and subjective creation of evidence is illustrated by considering the difference between an open-ended and a leading question to the developer. If the evaluator makes a definite hypothesis and asks the developer for a yes or no confirmation, this falls on the side of creation of evidence, but an open-ended question that does not suggest the required answer falls on the side of collection.

2.3 Small deficiencies

8 The evaluator may address small deficiencies in a developer-supplied deliverable by interviewing the developer and documenting his response, or by making hypotheses and requesting developer confirmation; however the evaluator should check the consistency of such input with other developer-supplied material. When doing so, the evaluator must supply a rationale, to be agreed by the Certifier, that the compensatory work is not excessive.

2.4 Types of Assistance to Developer

9 Objective collection of evidence is proper to the evaluators, should not be considered consultancy, and therefore does not need to be performed by an independent team.

10 The developer may subcontract production of deliverables to a consultant, provided that this does not compromise the independence of the evaluation. The CB has determined specific conditions to ensure such independence.

11 In exceptional cases, the CB may agree that work that is strictly the developer's responsibility may nonetheless be carried out by members of the evaluation team on the grounds that it is an objective collection-like activity. Cases where this is anticipated are described further below. Such cases will be subjected to additional Certifier oversight (e.g. spot checks in the documentation or attendance at technical meetings), and should constitute only a small proportion of the documentation associated with the evaluation. It is important that an evaluator is not in the position of reviewing his own work. Thus any document produced under this dispensation must be reviewed by another member of the evaluation team. Such documents must also be fully endorsed by the developer, including their adoption in the developer's configuration management and quality control systems where appropriate. The ETR should state which evaluator has provided such assistance, and identify the documents he produced and the evaluator who reviewed them.

2.5 Specific Cases

- 12 Arguably, the rationale of a CC PP/ST is based on other PP/ST material and could thus be objectively derived by the evaluator. In practice the PP/ST is a published document, its rationale supplements the understanding of the reader (if only by simply relating threats to objectives etc.), and it is thus important that this material is clear. The CB therefore requires the complete PP/ST to be independently evaluated.
- 13 Guidance documentation constitutes part of the TOE delivered to the purchaser. Deficiencies therefore constitute errors. It is not permissible for the Evaluator to make up for deficiencies.
- 14 The requirement for the developer to provide correspondence analysis does not necessarily demand the production of a tabular summary. If traceability is evident the evaluator may produce such a summary (if required) as part of the collection of evidence. If correspondences have to be inferred based on general similarities of the functions involved, then the work goes outside the scope of collection and the specific approval of the CB should be sought. Any such work would need to be endorsed by the developer, and subject to particular oversight and review as described above.
- 15 The low-level design supplied by the developer may be found to be incomplete in certain respects, for example it may not provide complete details of all modules. There is scope for evaluator collection of supplementary evidence from alternative sources, such as:
- a) Other relevant design information.

This may include design documents for closely related TOEs, standard texts (e.g. on Unix or NT internals), as well as documentation relevant to the targeted version of the TOE which may provide a useful context (e.g. the functional specification).
 - b) Evidence in ETRs from previous evaluations of the TOE (i.e involving an earlier version or a different variant).

Where the evaluators in a previous evaluation of the TOE have documented in detail their understanding of the internal workings of the TOE security, such evidence may assist the evaluators in gaining the required overall understanding of the internal workings of the TOE.
 - c) Developer presentations of particular aspects of the TOE security.

Developer presentations may help the evaluators to gain an overall understanding of particular parts of the TOE, for example how certain TOE security functions are provided, or an overview of the internal workings of individual TOE subsystems. Such evidence may be used to complete the low-level design. Any evidence presented verbally should be documented

by the evaluators and, any such input should be checked for consistency with other developer-supplied evidence.

- d) Clarifications of specific technical queries from the evaluators, whether verbal or written (e.g. email).

Such evidence should be used to confirm the evaluator's understanding of specific points of technical detail.

- e) Evidence generated by the developer's configuration management system.

Such evidence may be useful in helping to establish an accurate picture of the interrelationships between modules, e.g. call trees (identifying which modules depend on which other modules), use of global data structures by modules, and so on.

- f) Module headers associated with the source code modules.

This will typically take the form of low-level design evidence contained within comments in the source code modules or header files.

- g) The source code itself, including any associated comments.

It is not anticipated that it would be practical to derive any substantial proportion of the detailed design from the source code itself, but it may be used to address particular questions of detail, as may comments within the source code.