



**UK IT SECURITY EVALUATION
AND CERTIFICATION SCHEME**

UK Scheme Publication No 3

SPONSOR'S GUIDE

Part II

ASSURANCE CONTINUITY

**Issue 1.0
December 2009**

© Crown Copyright 2009 – All Rights Reserved

Reproduction is authorised provided the
document is copied in its entirety.

UK IT Security Evaluation and Certification Scheme
IA Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

**UK IT Security Evaluation & Certification Scheme
Sponsor's Guide Part II – Assurance Continuity**

FOREWORD

The UK IT Security Evaluation and Certification Scheme ('the Scheme') has been established to evaluate and certify the trustworthiness of security features of Information Technology products and systems.

Scheme Publication UKSP 03 provides advice to the Sponsor regarding the UK Scheme evaluation and certification processes for secure products.

This document, UKSP 03 Part II, describes the requirements for Assurance Continuity (AC) under the Scheme, by extending and complementing the Common Criteria [CC] CCRA [CCRA] AC [AC] requirements, which will facilitate the mutual recognition process.

In the event of any questions concerning this publication, or for further information, please consult the Certification Body.

Address: UK IT Security Evaluation and Certification Scheme
IA Delivery Office
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Telephone: +44 (0)1242 221491, Ext 30074

Facsimile: +44 (0)1242 709194

Email: iacs@cesg.gsi.gov.uk

Website: <http://www.cesg.gov.uk>

AMENDMENT RECORD

Amendments to this document will be published as and when required.

Issue Number	Major Changes	Date
1.0	First Issue	December 2009

**UK IT Security Evaluation & Certification Scheme
Sponsor's Guide Part II – Assurance Continuity**

ABBREVIATIONS AND REFERENCES

Please refer to the *Abbreviations and References* document [UKSP00] on the Formal Documentation page of the CESG website at <http://www.cesg.gov.uk>.

CONTENTS

I. INTRODUCTION.....	1
General	1
Objectives	1
Scope	1
Assurance Continuity	2
Assurance Maintenance.....	2
Re-evaluation	2
II. TECHNICAL CONCEPTS.....	3
Certification Lifecycle Diagram	3
Assurance Maintenance.....	4
Re-evaluation	5
Certification Work Programme	5
III. CHARACTERISATION OF TOE CHANGES.....	6
IV. PERFORMING AN IMPACT ANALYSIS	7
V. IMPACT ANALYSIS REPORT (IAR).....	8
VI. TEMPLATES, PRINCIPLES AND PROCEDURES	9
Templates	9
Principles.....	9
Procedures.....	10
VII. GLOSSARY	11

**UK IT Security Evaluation & Certification Scheme
Sponsor's Guide Part II – Assurance Continuity**

(This page is intentionally left blank)

UK IT Security Evaluation & Certification Scheme

Sponsor's Guide Part II – Assurance Continuity

I. INTRODUCTION

General

1. Scheme Publication UKSP 03 has been produced to assist Sponsors intending to submit a product¹ for evaluation under the UK IT Security Evaluation and Certification Scheme ('the Scheme'). Some aspects also affect Developers. UKSP 03 is divided into two parts:

a) Part I sets out the Sponsor's Role in the evaluation framework and describes the organisational and procedural aspects to be followed during the conduct of an evaluation under the Scheme.

b) Part II (this document) sets out the requirements for Assurance Continuity (AC) under the Scheme.

2. This document should be read in conjunction with (since it builds upon) UKSP 01 *Description of the Scheme* [UKSP01], UKSP 02 *CLEF Requirements* (Parts I & II) [UKSP02-I, UKSP02-II] and UKSP 03 *Sponsor's Guide – Sponsor's Role* (Part I) [UKSP03]. For a list of abbreviations and references, see UKSP 00 *Abbreviations and References* [UKSP00] on the CESG website at <http://www.cesg.gov.uk>.

3. The approach in this document extends [AC], where appropriate, in the areas of Technical Concepts, Change Characterisation, Impact Analysis and production of the Impact Analysis Report.

4. The Assurance Continuity process described in this document can only be performed for products previously certified under the Scheme.

Objectives

5. The objective of this document is to define the requirements for Assurance Continuity under the Scheme.

6. In order to satisfy the accreditation criteria of the United Kingdom Accreditation Service (UKAS), it is necessary that established procedures are used for the conduct of all Assurance Continuity activities performed under the Scheme. The responsibilities identified in this document reflect UKAS requirements; however the appropriate UKAS documentation must be consulted concerning the full accreditation requirements.

Scope

7. The Assurance Continuity requirements defined here are applicable to the Information Technology (IT) security evaluations of products against the criteria laid down in the Common Criteria [CC], [CCRA] and [AC], subject to the relevant International Interpretations, UK Interpretations and Scheme Information Notices (SINs).

¹ The processes described by this document relate to internationally recognised evaluation and certification of secure products. Some aspects may be more widely applicable to similar CESG assurance services.

UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part II – Assurance Continuity

Assurance Continuity

8. Assurance Continuity [AC] is an enhancement to Common Criteria [CC] Certification. The term Assurance Continuity covers Assurance Maintenance and Re-evaluation. The Re-evaluation process is already covered by the standard Evaluation process, as described in [UKSP01] and [UKSP02-II], therefore it is sufficient for this document to primarily elaborate on the Assurance Maintenance process.

9. The concept of Assurance Maintenance was introduced in [UKSP01] and is based on the production of an Impact Analysis Report (IAR) by the Sponsor/Developer. If all of the changes to a Certified TOE are demonstrated to be *Minor* in terms of their security impact, then the Assurance Maintenance process is applicable. If any change to a Certified TOE is demonstrated to be *Major* in terms of its security impact then a Re-evaluation is necessary.

10. Assurance Continuity enables the Sponsor/Developer of a Certified TOE to provide ongoing assurance when the TOE is subject to any type of update, modification or change. Assurance Continuity is intended to be a relatively quick, cheap and efficient process to achieve a Certified or Maintained TOE, since evaluation work that was previously performed does not need to be unnecessarily repeated. This is clearly beneficial to the Sponsors/Developers and the TOE Consumers.

Assurance Maintenance

11. Assurance Maintenance is based on the production of an IAR, by the Sponsor/Developer, which is submitted to the CESG Certification Body (CB) for Review. CLEF Evaluators are not involved during Assurance Maintenance, but the CB or Sponsor/Developer may utilise consultants or experts (e.g. CLEF Consultants) if they are required. Although there is no formal CC requirement to supply any further Developer Evidence in the assessment process, beyond those items listed in Chapter 2, the CESG CB reserves the right to inspect original and/or updated deliverables. In particular, the inspection of deliverables may be required in order to confirm whether specific changes are *Major* or *Minor*. Appropriate arrangements for the supply of such deliverables should be made when placing contracts with the CESG CB.

12. A satisfactory outcome from the CESG CB Review will lead to the publication, on the CESG website, of an updated Security Target (ST) and a Maintenance Report (MR) summarising the changes from the Certified TOE. A Maintenance Addendum (MA) will be appended to the original webpage containing information about the Certified TOE. An MA Certificate will be issued to the Sponsor/Developer to supplement the original Certificate.

Re-evaluation

13. Any security relevant change that is deemed to be *Major* will necessitate a Re-evaluation if assurance in the product is to be maintained. The Re-evaluation process is identical to the Evaluation process described in [UKSP01] and [UKSP02-II] except that the Evaluation may be optionally guided by an IAR, and supported by appropriate reuse of any previous Evaluation or Maintenance evidence. The extent of reuse must be agreed and documented at the TSM. See also paragraph 25.

II. TECHNICAL CONCEPTS

Certification Lifecycle Diagram

14. The following diagram is a representation of the technical concepts presented in Section 2 of [AC], pertaining to the Certification and Assurance Continuity process (including Re-evaluation and Maintenance). Please refer to Chapter VII *Glossary*, for a summary of the terminology.

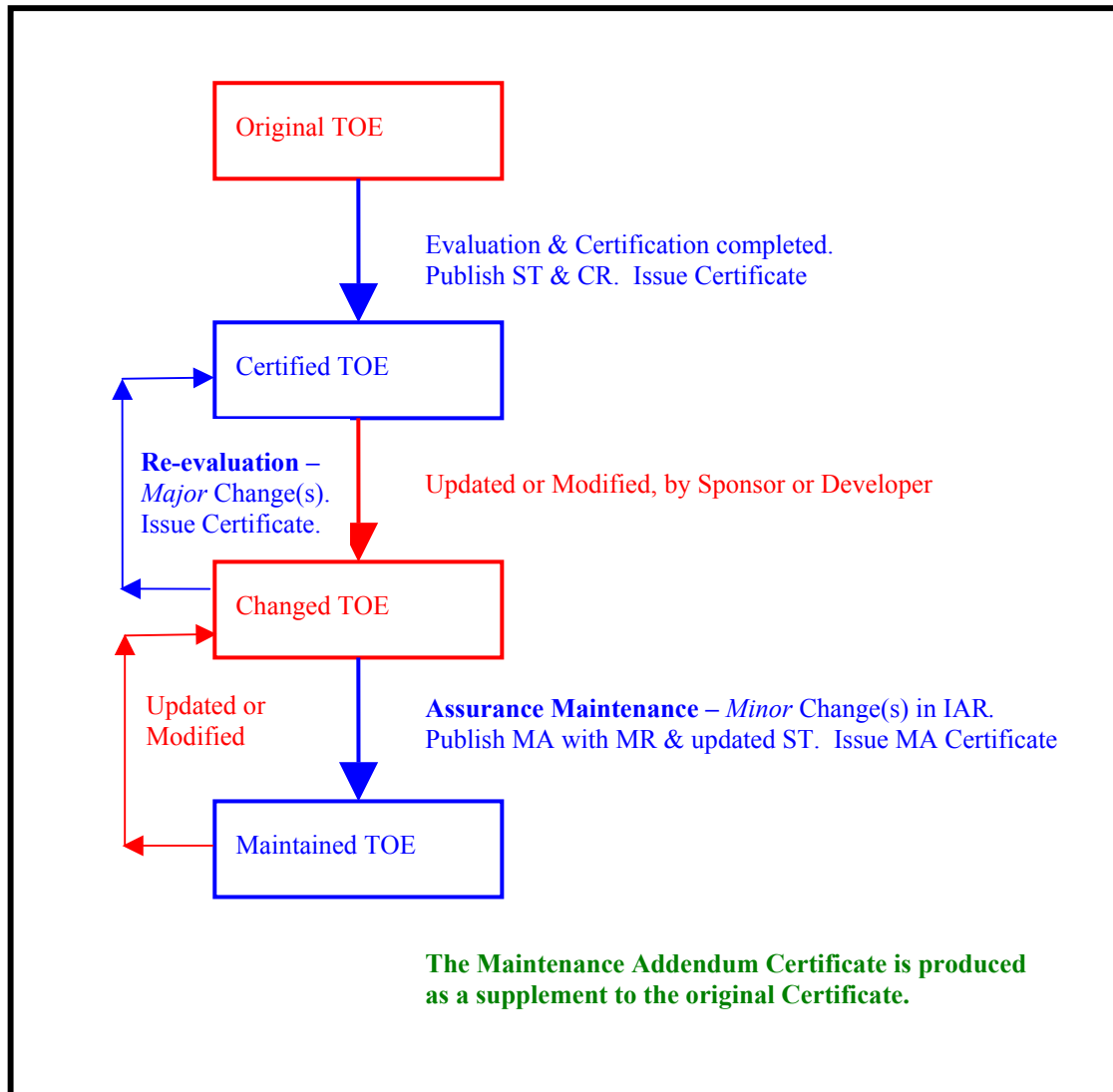


Figure 1 – The Assurance Continuity Process (Re-evaluation and Assurance Maintenance)

15. The Assurance Continuity process for Re-evaluation is basically the same as the standard CC Evaluation process (including issue of a Certificate). However, the results of the previous Evaluation (or Assurance Maintenance) are available for reuse where appropriate; for example, covering areas of the TOE where there have not been any changes. For Assurance Maintenance it is sufficient that all the changes described in the IAR are assessed and verified to have a *Minor* security impact on the TOE. If this fails and

UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part II – Assurance Continuity

there is a change with a *Major* security impact then the IAR may still be useful for the Re-evaluation process.

16. In contrast to Section 2.2 of [AC], which states that there is “no implied issuance of an updated certificate”, a MA Certificate will be produced as an Addendum to either the original Certificate or the most recent Re-evaluation Certificate.

17. It is stated in Section 2.4 of [AC] that new vulnerabilities and attack methods are *not* assessed during the Assurance Maintenance process. However, even a few weeks is a long time period in terms of security vulnerability development/deployment and analysis. Therefore, the CESG CB may wish to increase confidence in the Assurance Maintenance process by ensuring that *either* no new vulnerabilities or attack methods have been found *or* if found they are not in scope of the defined TOE boundary or at least they are not relevant to the evaluated configuration of the TOE. It is the responsibility of the CESG CB to determine the extent of additional vulnerability analysis that is required beyond any that may have been produced by the Developer. The CB will also determine who should perform any such analysis.

Assurance Maintenance

18. In accordance with the information in [RERE] and Sections 2.4.1.1 & 4.1 b) of [AC], the following deliverables are required for Assurance Maintenance by the Scheme:

- For the Certified TOE:
 - a) Common Criteria Certificate (including any Maintenance Addendum);
 - b) Certification Report (CR – including any Maintenance Report);
 - c) Evaluation Technical Report (including any Evaluation Work Packages);
 - d) Security Target (including the Security Target for any Maintained TOE);
- For the Changed TOE:
 - a) Impact Analysis Report and updated Security Target;
 - b) Product and supporting documentation (including the updated Developer Evidence).

19. The above list provides a suitable initial set of deliverables that are required as input into the CESG Assurance Maintenance process (and potentially the Re-evaluation process).

20. The UK Scheme may require the following additional inputs to resolve any decisions regarding the characterisation or categorisation of changes:

- Security Architecture and Design
- Vulnerability Analysis
- Test Scripts and Results
- Configuration List
- Operational Guidance

21. Although there is no defined time limit between the TOE Certification date and the start of the Assurance Maintenance process, the Certifier should ensure that the time gap

UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part II – Assurance Continuity

is consistent and reasonable in relation to other aspects of the proposed Assurance Maintenance process.

22. The CESG Certification Body will perform a formal Review of the Impact Analysis Report, using a standard CESG CB Review form, to ensure that all changes have a *Minor* impact on the assurance of the TOE. If this is indeed the case then a Maintenance Report and Maintenance Addendum will be published on the CESG website, as an update to the information about the Certified TOE. *Note that the IAR is normally shared only between the Sponsor/Developer and the CESG Certification Body.*

23. The Maintenance Addendum is just a few additional paragraphs, referencing the Maintenance Report and the updated Security Target, which are appended to the information about the Certified TOE on the CESG website. This clearly satisfies the Maintenance Addendum requirements stated in Section 2.4.1.2 of [AC].

24. To assist the Certifier, a Maintenance Report Template has been created which satisfies the requirements stated in Section 2.4.1.3 of [AC].

Re-evaluation

25. Apart from the potential use of an IAR in a Re-evaluation, everything else in Section 2.4.2 of [AC] regarding the Re-evaluation process is already covered by [UKSP02-II].

Certification Work Programme

26. The Certification activities performed by the CB for the Assurance Maintenance process and Re-evaluation process are outlined in the Standard Certification Work Programme ([CWP-AM] and [CWP] respectively) on the CESG website.

27. For some TOEs, depending on the scope and quantity of changes, the CB may seek the support of a consultant (typically from the CLEF that performed the original evaluation) to perform the initial analysis of the changes detailed in the IAR and to draft the Maintenance Report.

III. CHARACTERISATION OF TOE CHANGES

28. No additional information is required in addition to Chapter 3 of [AC], since it just contains some examples of changes that have *Minor* or *Major* impact.

29. It is worth noting that the general problem of determining whether the impact on assurance of any specific change to a TOE should be classified as *Minor* or *Major* is a very difficult problem. Also, there is no guarantee that the security of an updated product can be determined by checking the updates *only* and ignoring the unchanged aspects, in the context of the whole product. In practice, the categorisation is agreed between the Sponsor, Developer and the CB, together with any assigned CB consultant, but the decision of the CB will be final.

IV. PERFORMING AN IMPACT ANALYSIS

30. No additional information is required in addition to Chapter 4 of [AC], which basically states that any changes that impact on any aspect of the original Evaluation and Certification (eg Objectives, Threats, SFRs, SARs, Documentation, etc) should be addressed by the Sponsor/Developer, who will produce updated Documentation and the IAR.

31. The information contained in Step 1 to Step 5 in Section 4.3 of [AC] may be used as a checklist by the Sponsor/Developer or the CESG Certification Body to ensure that the IAR covers all the stated requirements.

32. Clearly, a stricter requirement for evaluation deliverables or a stronger level of assurance than the Original TOE Evaluation and Certification is unnecessary and is not required.

V. IMPACT ANALYSIS REPORT (IAR)

33. The required minimum contents of the IAR are as follows and could be used by the Sponsor/Developer as a basis for an IAR template:

- Introduction:
 - the IAR configuration control identifiers (e.g. name, date and version);
 - current TOE configuration control identifiers (the current version of the TOE);
 - configuration control identifiers for the ETR, CR, and Certified TOE (Assurance Baseline);
 - configuration control identifiers for the version of the ST related to the Certified TOE;
 - identity of the Developer;
 - information in relation to legal or statutory aspects;
 - *information related to any previous Assurance Maintenance activity (e.g. MR).*
- Description of changes:
 - changes to the product;
 - changes to the development environment.
- Affected Developer Evidence:
 - for each change, the Developer shall list the affected items of the original Developer Evidence (i.e. the affected Evaluation Deliverables).
- Modifications to Developer Evidence:
 - the developer shall describe the required modifications to the affected items of the original Developer Evidence.
- Conclusions:
 - for each change the Developer shall report if the impact on assurance is considered *Minor* or *Major*;
 - for each change the Developer should provide a supporting rationale for the reported impact;
 - the Developer shall report if the overall impact is considered *Minor* or *Major*;
 - the Developer should include a supporting rationale, taking all the changes into consideration.
- Annex: Updated Developer Evidence:
 - the Developer shall report the title and the unique reference (e.g. issue date and version number) of each updated item of Developer Evidence.

34. The item shown in italics above is the only additional information that is required in addition to Chapter 5 of [AC], which describes the minimum contents of the IAR.

VI. TEMPLATES, PRINCIPLES AND PROCEDURES

Templates

35. The templates that are relevant to the CESC AC process are as follows.
- Template for an Assurance Maintenance Plan (AMP):
 - This is provided, *if required*, on the CESC website in the CTAS Methodology.
 - Template for an IAR, for the Sponsor/Developer:
 - This is provided in Chapter V of this document.
 - Template for an IAR Review, for the CESC Certification Body:
 - This is provided by a standard CESC CB Review Form.
 - Template for a Maintenance Report, for the CESC Certification Body:
 - This is available as required from the CESC CB.
 - Template for a Maintenance Addendum, for the CESC Certification Body:
 - This is not specifically provided, but the MA should satisfy at least the requirements of Section 2.4.1.2 of [AC].

Principles

36. The main principles to be followed for Assurance Continuity are as follows:
- Maintain impartiality and objectivity, as with all Common Criteria evaluation and certification tasks. There should not be any time, money or resource pressures that would affect the impartiality or objectivity of the Assurance Continuity process.
 - Reuse evaluation results wherever possible. For parts of the Changed TOE where there has been no change, there is no point in repeating work that has already been performed during the evaluation of the Certified TOE.
 - No more detail is required than would have been provided during the evaluation of the Certified TOE. Only the changes that actually affect the deliverables of the Certified TOE are required to be reported. For example, if a certain document was not provided as a deliverable for the Certified TOE then any updates to that document do not need to be provided for the Maintained TOE.
 - Details of changes should be sufficient to support repeatability and reproducibility of results across CBs.
 - A non-security related change is usually completely irrelevant to the TOE. Therefore it can be eliminated quickly and does not need to be discussed in detail within the IAR. The impact of non-security related changes can be

UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part II – Assurance Continuity

categorised as *None* (rather than *Minor*). Note that changes with impact *None* would not have been discussed in the Original TOE evaluation anyway.

- Note that correcting an implementation fault (even to security functionality) is just strengthening the claimed behaviour of the TOE and hence cannot be considered a *Major* change for the Impact Analysis Report. Generic wording that may be used for this situation is as follows: “The < fault correction | bug fix > relating to the < subsystem | component > is a *correction* to the TOE functionality and hence does not affect the expression of the SFRs in the assurance evidence”.

Procedures

37. The CESG CB procedures for the initial stage of Assurance Maintenance are:

- Prepare for the IAR Review (i.e. familiarise with the previous ST, ETR, CR, IAR, MR as appropriate);
- Confirm whether the ST is essentially unchanged (except for trivial changes such as software version numbers);
- Review the draft IAR & check its change categorisations;
- Audit any updated deliverables regarding specific changes (such as the bug list and test results);
- Perform a search for any obvious vulnerabilities.

38. The CESG CB procedures for the final stage of Assurance Maintenance are:

- Review and approve the final IAR;
- Address any issues raised by CESG CB or the Sponsor/Developer;
- Produce and agree the Maintenance Report;
- Record the decision rationale;
- Produce and agree the MA and MA Certificate;
- Update the entries on the CESG and CC portal websites using ST, MR, and MA.
- Submit the MA Certificate to the Sponsor/Developer.

**UK IT Security Evaluation & Certification Scheme
Sponsor's Guide Part II – Assurance Continuity**

VII. GLOSSARY

Assurance Baseline	The culmination of activities performed by the Evaluator and Developer resulting in a Certified TOE, recorded or submitted as evidence and measurable by any change to that evidence.
Certified TOE	The TOE that has been successfully evaluated and certified (or re-evaluated and certified).
CESG CB	CESG Certification Body which is the UK Evaluation Authority.
Changed TOE	The patched, updated or otherwise modified TOE that is to be subjected to Assurance Continuity.
Developer Evidence	The TOE and documentation deliverables provided to the CLEF Evaluators in support of a TOE evaluation.
Evaluation Authority	A body that implements the CC for a specific community by means of an Evaluation Scheme.
Impact Analysis Report (IAR)	The report generated by the Sponsor/Developer that records the analysis of changes to the Certified TOE. The impact of each change should be <i>Minor</i> for Assurance Maintenance otherwise a Re-evaluation will be required.
Maintained TOE	The Changed TOE that has successfully undergone the Assurance Maintenance process and has been awarded a Maintenance Addendum Certificate.
Maintenance Addendum	The additional text that is appended to the description of the Certified TOE on the CESG website in order to describe the Maintained version(s) of the TOE. <i>(Note that the Certificate of the Certified TOE is not updated but it is supplemented with a Maintenance Addendum Certificate.)</i>
Maintenance Addendum Certificate	The Certificate of the Maintained TOE, which references the Certificate of the Certified TOE.
Maintenance Report	The publicly available report that describes all the changes that were made to the Certified TOE and that have been accepted under the Assurance Maintenance process.
Maintenance	The process applied when the changes to a Certified TOE have not adversely affected assurance in that TOE.
Original TOE	The TOE prior to being subjected to any evaluation and certification.
Re-evaluation	The process applied when changes to a Certified TOE require Evaluation (reusing results from any previous Evaluation and Maintenance activities as appropriate) in order to establish a new Assurance Baseline.