



**UK IT SECURITY EVALUATION  
AND CERTIFICATION SCHEME**

**UK Scheme Publication No 3**

**SPONSOR'S GUIDE**

**Part I**

**GENERAL INTRODUCTION**

**Issue 2.2  
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 I – General Introduction

## FOREWORD

The UK IT Security Evaluation and Certification Scheme has been established to evaluate and certify the trustworthiness of security features in 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 I, provides an overview of the concept of evaluation, the associated roles of the bodies involved in developing secure products and systems, and the practical issues involved in preparing for evaluation.

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](mailto:iacs@cesg.gsi.gov.uk)

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

**UK IT Security Evaluation & Certification Scheme  
Sponsor's Guide Part I – General Introduction**

**AMENDMENT RECORD**

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

<b>Issue Number</b>	<b>Major Changes</b>	<b>Date</b>
1.0	First issue, which replaced UKSP 04 Part I of July 1996.	September 2002
1.1	Minor changes: incorporated SIN 86, and new postal and website addresses.	October 2003
2.0	Version for use with revised certification processes. (Issue 1.1 remains applicable for applications that still use the previous certification processes.)	July 2005
2.1	Refinements and clarifications.	October 2008
2.2	UKSP 03 is now in two parts. Part I is General Introduction and Part II is Assurance Continuity.	December 2009

**UK IT Security Evaluation & Certification Scheme  
Sponsor's Guide Part I – General Introduction**

**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>.

**UK IT Security Evaluation & Certification Scheme  
Sponsor's Guide Part I – General Introduction**

**CONTENTS**

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
	How to Use this Guide .....	1
	Scope .....	1
	Terminology .....	2
	Request for Feedback.....	2
<b>II.</b>	<b>MANAGEMENT ISSUES.....</b>	<b>3</b>
	Introduction .....	3
	Contractual Considerations.....	3
	Sensitivity of Information .....	6
	Copyright of Evaluation Outputs.....	7
	Marketing .....	8
	CESG Website .....	9
<b>III.</b>	<b>PREPARATION FOR SECURITY EVALUATION .....</b>	<b>10</b>
	Introduction .....	10
	Task Startup Review .....	10
	Task Startup Meeting.....	10
	Scope of TOE.....	11
	Cryptographic Mechanisms.....	13
	Evaluation Deliverables.....	13
	Security Target.....	14
<b>IV.</b>	<b>EVALUATION AND CERTIFICATION .....</b>	<b>16</b>
	Introduction .....	16
	Evaluation Process .....	16
	Observation Reports .....	16
	Evaluation Progress Meetings.....	17
	Evaluator Testing .....	17
	Certification Process .....	18
	Validity of Certificates.....	18
	Vulnerabilities.....	19
<b>V.</b>	<b>ASSURANCE MAINTENANCE.....</b>	<b>20</b>
<b>ANNEX A</b>	<b>SUMMARY GUIDANCE FOR TOE SCOPE INFORMATION .....</b>	<b>21</b>

**UK IT Security Evaluation & Certification Scheme  
Sponsor's Guide Part I – General Introduction**

(This page is intentionally left blank<sup>1</sup>)

---

<sup>1</sup> Regarding the “Blank Page” problems, and their solutions in Word, please refer to:  
<http://sbarnhill.mvps.org/WordFAQs/BlankPage.htm>

# UK IT Security Evaluation & Certification Scheme

## Sponsor's Guide Part I – General Introduction

### I. INTRODUCTION

#### How to Use this Guide

1. Scheme Publication UKSP 03 has been produced to assist Sponsors intending to submit a product<sup>2</sup> 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 (this document) 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 sets out the requirements for Assurance Continuity (AC) under the Scheme.

2. There are many matters surrounding an evaluation that are treated differently in different nations for reasons of, for example, jurisdiction or national security. The rules of the national scheme take precedence in each of the countries. This guide is concerned only with the (UK) Scheme.

3. The information in this guide is applicable to both Common Criteria (CC) and Information Technology Security Evaluation Criteria (ITSEC) evaluations. It emphasises the role and responsibilities of Sponsors and their interactions with Developers (where Developers are different from Sponsors) and other organisations within the Scheme.

4. This document builds on, but does not repeat, the guidance given in UKSP 01.

5. Under the Scheme, Sponsors are responsible for ensuring that they have an understanding of: the evaluation process; the roles of the Sponsor, Developer, Commercial Evaluation Facility (CLEF) and Certification Body (CB); and the Sponsor's responsibilities throughout the evaluation and certification.

6. Sponsors must therefore understand their obligations, and in particular should ensure that Developers agree to supply the required deliverables for the evaluation.

7. For the *Abbreviations and References* document please refer to the Formal Documentation section of the CESG website at <http://www.cesg.gov.uk>.

#### Scope

8. The main phases within the evaluation process are the Preparation phase and the Evaluation and Certification phase. Any subsequent Assurance Maintenance phase commences once the evaluation is complete, and is described in other

---

<sup>2</sup> 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 I – General Introduction

documents (e.g. see the *Assurance Continuity* document at <http://www.commoncriteriaportal.org> and UKSP16 in the *Abbreviations and References* document). Any requirements for Assurance Maintenance should be discussed during the preparation phase to determine any impact on the evaluation (e.g. additional procedures that may require assessment).

9. The process outlined here is for a typical evaluation, and covers CC and ITSEC evaluations. To provide the appropriate level of information for a new Sponsor, it includes an overview of the following:

- some of the management, contractual and planning issues involved;
- work involved in the preparation phase prior to starting an evaluation;
- the evaluation and certification processes.

### Terminology

10. The word *must* indicates mandatory requirements (i.e. that are mandated by the Scheme or by the UK Accreditation Service (UKAS)) that the Sponsor is required to perform. The word *should* indicates an optional requirement.

11. The word *criteria* is used to apply to the CC and the ITSEC. Similarly, the word *methodology* is used to apply to the Common Evaluation Methodology (CEM) and the IT Security Evaluation Manual (ITSEM). The CC, CEM, ITSEC and ITSEM documents should be consulted for details of criteria and methodology.

### Request for Feedback

12. Sponsors play a significant part in the performance and success of the Scheme. The CB wishes to assist Sponsors with their understanding of the Scheme, to enhance the likelihood of successful evaluations and to further increase the number of certificates awarded, hence increasing the choice of security products available to potential consumers in the global market.

13. Therefore the CB invites all Sponsors and Developers to contact the CB, with feedback on this guide and the Scheme, or to obtain further advice on the Scheme. Please contact the CB using the details shown in the Foreword.

## **II. MANAGEMENT ISSUES**

### **Introduction**

14. The Sponsor can considerably reduce the risks to the evaluation and to the development, by giving early consideration to factors that can affect costs, timescales and efficient management of an evaluation. These factors include:

- the relationships between the parties involved, including the Evaluators' access to Developers and subcontractors;
- the readiness and quality of the product to be submitted into formal evaluation;
- the supply of deliverables to the Evaluators, and access to development and operational sites;
- the Evaluation Assurance Level that is chosen for the product, together with any augmentations<sup>3</sup> or extensions<sup>4</sup>;
- whether the evaluation is performed concurrently or consecutively with the development;
- the availability of resources to support the evaluators in gaining detailed technical knowledge of the TOE and its development and test environment by answering questions about the TOE and its documentation;
- the availability of resources to make timely changes to the TOE and its documentation as may be necessitated by findings and observations during the evaluation;
- the time taken to respond to ongoing informal questions and any formal Observation Reports;
- intangible factors such as product launch date and publicity requirements.

### **Contractual Considerations**

15. The Sponsor will need to obtain separate quotations (and hence enter into separate contracts) for the evaluation and certification services from the CLEFs and the CB respectively. The CB will usually arrange one contract between itself and the Sponsor, to cover the Preparation phase and the Evaluation and Certification phase.

---

<sup>3</sup> An *augmentation* is a SAR from CC Part 3 that is added to the set of SARs defined for a chosen EAL $n$  in CC Part 3. For example, ALC\_FLR.3 is a popular augmentation to EAL4. A TOE may have multiple augmentations.

<sup>4</sup> An *extension* is a new SFR or SAR that is not already in CC Part 2 or 3 respectively. An extension may be based on an existing SFR or SAR, but can also be completely new.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

However, a separate consultancy contract may be required for the preparation phase of a particularly complex TOE.

16. The Sponsor is advised to:

- consider the requirements which evaluation may impose on other parties, particularly the Developer;
- consider whether there are sufficient financial, technical, staff and other resources to ensure completion of the evaluation;
- consider links with any related assessments, e.g. CESA Assisted Products Scheme (CAPS) or Federal Information Processing Standards (FIPS);
- consider whether there is a requirement in relation to the Mutual Recognition Arrangement (MRA) or the Common Criteria Recognition Arrangement (CCRA);
- consider the maintenance of assurance;
- obtain ownership of outputs from the evaluation process and the rights to their reuse.

17. The Sponsor has the option of engaging a security consultant, who may be from a CLEF, to assist with the preparation for evaluation. For example, the Sponsor might contract a consultant to prepare the Security Target. The scope of any such advice or consultancy during the preparation for evaluation is a matter for negotiation between the Sponsor and the consultant.

18. Evaluators must remain impartial before and during the evaluation. They must be free from any commercial, financial and other pressures which might influence their technical judgement. Consequently under the rules of the Scheme:

- the CLEF cannot evaluate the development work of a group or division within its parent company, unless it successfully demonstrates to the CB that the independence of the evaluation will be maintained;
- the Evaluators cannot be involved in the development of the Target of Evaluation (TOE);
- the Evaluators cannot provide consultancy advice to the Sponsor which would compromise the independence of the evaluation;
- the Evaluators cannot advise Sponsors or Developers how to resolve problems, but they can comment on the adequacy of a proposed response;
- the Evaluators cannot guarantee the completion date of an evaluation or the issue date for certification.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

### **19. The Sponsor must make suitable arrangements with a CLEF to evaluate the TOE.**

20. Evaluations undertaken within the Scheme must be performed by a UK CLEF.
21. The Sponsor must ensure that there is adequate contractual cover for the resolution of issues and observations.
22. Subject to contractual arrangements regarding the reuse of evaluation results, Sponsors are free to choose different CLEFs for different evaluations, for re-evaluations and for assurance maintenance. The requirements stipulated by the Scheme ensure that each CLEF:
- records its work in sufficient detail to enable the evaluation results to be re-used where required;
  - retains sufficient evaluation documentation to enable re-evaluations to be performed.
23. Sponsors should note that for CC products, any assurance continuity must be performed by the same national scheme as the original evaluation.

### **24. The Sponsor must arrange for the provision of certification services.**

25. This is normally achieved by a contract with the CB. The Sponsor should complete the CB's business questionnaire, which is available on the CESG website. This questionnaire requires the Sponsor to answer a number of questions that will assist the CB to scope the certification work and to provide the Sponsor with a quote for the Preparation phase of their certification services and, normally, to provide the Sponsor with an estimate for the Evaluation and Certification phase.

### **26. The Sponsor should establish separate contracts with Developers, sub-contractors and external consultants to ensure that they accept and understand their responsibilities to support the evaluation.**

27. This will ensure the following:
- all evaluation deliverables, including all security-relevant products of the development, are supplied to the CLEF;
  - the Developer's procedures and practices meet the evaluation criteria for a development environment;
  - appropriate technical support is provided to the CLEF;
  - the Developer has agreed to participate in the Task Startup Review (and attend the Task Startup Meeting, where appropriate), and to contribute as required to Evaluation Progress Reviews.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

28. Where necessary, arrangements should also be made for access by the Evaluators to any of the above parties' relevant data and should include:

- confirmation from the parties involved of the extent and nature of any commercially sensitive or proprietary data;
- consent of the parties to allow access to that data by the Evaluators and the CB, where required;
- agreement from the parties to relinquish rights to the results of the evaluation that may compromise proprietary information.

**29. The Sponsor should ensure that, where the TOE contains certified components or is subject to a re-evaluation, permission for the release of previous evaluation results is obtained from the relevant copyright holders.**

30. If a TOE has previously been evaluated, then time, effort and cost may be saved by re-using the results of the *unchanged* aspects or components of that previous evaluation. Sometimes this can be done from the Certification Report and Security Target alone. If required, access should be gained to the Evaluation Technical Report, Observation Reports and other deliverables. The Sponsor is responsible for the delivery to the Evaluators of all deliverables, including evaluation results for certified components of the TOE.

**31. The Sponsor should consider taking out insurance to cover the TOE and all deliverables.**

32. Unless specifically agreed otherwise, the Sponsor will be responsible for all deliverables, even when transferred to CLEF premises. Some deliverables, such as new or special-purpose types of hardware, may not have an easily identified replacement cost and may represent an insurance risk that cannot be transferred to other parties.

33. Otherwise it is the Sponsor's responsibility to ensure that the TOE can be recovered. The CLEF may require the owner of the system used for penetration tests to sign a disclaimer to the effect that the Evaluators will not be held liable if any damage occurs during the tests. Such damage might, for example, involve data, programs, source files and configuration parameters.

### Sensitivity of Information

**34. The Sponsor must ensure that any limitation on the distribution of commercially sensitive information does not adversely affect the evaluation.**

35. During the evaluation, the CLEF, and to a lesser extent the CB, will inevitably be given access to commercially sensitive information. The Sponsor must ensure that any confidentiality requirements are consistent with the Scheme requirement for the free flow of evaluation deliverables to the Evaluators. The Sponsor and Developer

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

may wish to enter into a confidentiality agreement with the CLEF, and possibly with the CB. The CB is a non-commercial, government body and normally does not enter into confidentiality agreements, as it routinely handles sensitive information in an appropriate manner.

**36. The Sponsor must accept that the CB reserves the right to record vulnerabilities and use this information to guard against similar vulnerabilities that may occur in similar TOEs.**

37. Where there is a possibility of a vulnerability compromising the security of other TOEs of a similar type, the CB must be able to use the associated vulnerability and countermeasure information in other evaluations to safeguard against a widespread threat. In using this information for other evaluations, the CB will sanitise the information (so as to exclude explicit reference to the TOE in which the vulnerability was found) and will not disclose details of the method used to detect the vulnerability.

**38. The Sponsor must agree to a possible UKAS assessment of the evaluation.**

39. Where necessary, UKAS can enter into a confidentiality agreement.

### Copyright of Evaluation Outputs

**40. The Sponsor and CLEF should agree the ownership and copyright of evaluation outputs.**

41. Ownership of the copyright of evaluation outputs should be determined prior to commencing the evaluation. Evaluation outputs include:

- Evaluation Work Programme (EWP);
- Deliverables List, where produced;
- Observation Reports (ORs);
- Observation Report Status Register (ORSR);
- Evaluation Technical Report (ETR);
- Test Strategy and Test Scripts.

42. The Sponsor is expected to keep ownership and copyright of evaluation outputs which may be needed in later evaluation or assurance maintenance work, e.g. the Evaluation Technical Report.

43. Where a CLEF claims intellectual property rights over methods and techniques developed at its own expense, the CLEF may include the evaluation outputs specific

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

to these methods and tools in a separate document, as property and copyright of the CLEF.

44. Where a Developer claims intellectual property rights over proprietary data, then the evaluation results for this data may be issued separately from the rest of the evaluation results.

45. It should be noted that evaluation results will be used in producing the Certification Report, which will be Crown Copyright and may be made publicly available on the CESG website. The CB will always give the Sponsor the opportunity to review the Certification Report before publishing it.

**46. The Sponsor should give permission in principle for the future release<sup>5</sup> of evaluation results and in particular the Evaluation Technical Report.**

47. This is required in order to prevent future problems related to re-use of evaluation results.

### Marketing

**48. The Sponsor must submit all press releases and other promotional material, relating to evaluation and certification of the TOE, to the CB for approval.**

49. A Sponsor must not make any statements in press releases or other promotional material which might be misleading, might misrepresent the conclusion of the evaluation and certification, or might otherwise bring the Scheme into disrepute. Sponsors are responsible for ensuring that Developers understand that they have a similar responsibility. The CB therefore reviews all marketing information, relating to evaluation and certification of the TOE, that the Sponsor wishes to issue, but will not unreasonably withhold permission for its release.

50. When the TOE has been formally accepted into evaluation by the CB, the Sponsor is allowed to state that a product has entered evaluation together with the expected date for the completion of the evaluation.

51. Once the TOE is certified, the Sponsor must only market the product as a certified product on the basis of a valid certificate, i.e. for a certified product and platform configuration. A Sponsor must not claim that a product is certified when it is not, for example:

- where a product comprises a certified TOE together with integrated, but uncertified, components;
- when a certified product changes, e.g. following a software upgrade;

---

<sup>5</sup> Evaluation results are not public, but may be required by other CLEFs and CBs.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

- where a certified product in its operational environment does not conform to the evaluated configuration.

52. The Sponsor must not exaggerate the benefits of the certification by claiming features or levels of assurance that have not been certified.

### CESG Website

**53. The “In Evaluation” entry, if required, for the CESG website should be agreed between the Sponsor and the Certification Body when the product has been formally accepted into the Scheme. The “Certified”<sup>6</sup> entry, if required, for the Directory of Infosec Assured Products and the CESG website should be agreed between the Sponsor and the Certification Body when the product has successfully completed evaluation and certification.**

54. The CESG website provides information on products that are either in evaluation or have been evaluated and certified under the Scheme. The Directory of Infosec Assured Products provides information on products that have been evaluated and certified under the Scheme. The current version of the Directory of Infosec Assured Products may be viewed on the CESG website or requested from the Certification Body. Product entries are written by the Sponsor and agreed by the CB.

55. The CB will review the status of the evaluation and certification and reserves the right to withdraw the product from the list if insufficient evaluation progress has been made.

56. Inclusion of any product, regardless of status, in the Directory of Infosec Assured Products and on the CESG website is ultimately at the discretion of the Head of the CB.

57. It is a requirement for the mutual recognition of CC certificates that the Certification Report and Security Target are made publicly available. Consequently the CB publishes the Certification Report and Security Target, with agreement from the Sponsor, on the CESG website. If a Security Target includes commercially sensitive information, this can be excluded from the version entered on the CESG website.

58. A certified product may be withdrawn from the Directory of Infosec Assured Products and the CESG website when the product becomes obsolete or when an exploitable vulnerability is discovered that undermines the certification (see paragraph 121).

---

<sup>6</sup> The “Certified” entry may not require any change in relation to the “In Evaluation” entry.

### III. PREPARATION FOR SECURITY EVALUATION

#### Introduction

59. This chapter discusses the Preparation phase of the evaluation. The Sponsor supplies the TOE Scope Information<sup>7</sup> to the CB and the Evaluators. The CB performs a Task Startup Review, which may include a Task Startup Meeting, and determines whether the evaluation will be certifiable, in principle, under the Scheme. Finally the Sponsor completes the Security Target, which the CLEF evaluates and reviews, and the CB formally approves it as a valid definition for the evaluation.

#### Task Startup Review

60. The Sponsor must provide the TOE Scope Information to the CB, normally at least 10 working days in advance of the date agreed for the Task Startup Meeting or Task Startup Review. In some cases, a separate document will not be necessary for the TOE Scope Information requirement because a draft Security Target (consisting of at least Chapters 1 to 5, possibly Chapter 6, but no need for Chapter 7 Rationale) may be submitted provided that it satisfied the requirements<sup>7</sup>. The draft Security Target may be inherited from a previous evaluation or it may already be in preparation.

#### Task Startup Meeting

**61. The Sponsor must attend the Task Startup Meeting, where one is required, or must provide the required inputs to the Task Startup Review. The Sponsor must provide an overview of the TOE, in the form of the TOE Scope Information, at least 10 working days in advance of the meeting and should be prepared to discuss this at the Task Startup Meeting.**

62. A formal Task Startup Meeting involves the CB, the CLEF, the Sponsor and the Developer (where different), and may also involve an Independent Technical Consultant assisting the Developer with the evaluation. It is used by the CB to ensure that the TOE is certifiable in principle, and is used by the CLEF and the CB to clarify any issues regarding the TOE.

63. A Task Startup Meeting is usually required by the Scheme but, for straightforward re-evaluations or other cases agreed by the CB, the CB will perform a Task Startup Review without the need for a meeting.

64. The main topics addressed at the Task Startup Meeting are:

- a. suitability of the TOE, as defined in the TOE Scope Information;
- b. clarification and approval of the Evaluation Work Programme;

---

<sup>7</sup> See Annex A *Summary of Guidance for TOE Scope Information*.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

- c. proposals for monitoring evaluation progress, defined by the CB in its Certification Work Programme<sup>8</sup>;
- d. discussion of the sampling and testing strategy.

### Scope of TOE

65. The precise scope of the TOE and its environment will need to be defined in the TOE Scope Information presented during the Task Startup Review, which may include a Task Startup Meeting.

66. The TOE may be a complete product or parts of a product (or a set of products). Where the TOE is not the complete product (or set of products), the Sponsor must clearly define the TOE scope and boundary, i.e. which parts are to be included in the evaluation and which are not.

67. The TOE Scope Information should provide a high-level description of the architecture of the full product, without reference to which parts of the product will be evaluated, as follows:

- the product's decomposition into major components or subsystems;
- the security functionality provided by the product and how this relates to the components and subsystems;
- the threat environment of the product;
- other IT products (e.g. COTS products) required to support the operation and management of the product;
- the method of secure use of the product;
- how the product interfaces to its environment, including relevant standards and protocols;
- the product's modes of operation;
- the claimed platforms.

68. The TOE Scope Information should then include specific descriptions of the following:

- the components or subsystems, and security functionality and interfaces, that are in scope of the evaluation, and those which are out of scope of the evaluation;

---

<sup>8</sup> The *UK CB Standard Certification Work Programme* may be used either as provided or as a template to incorporate contract specific details. It is available at:  
[http://www.cesg.gov.uk/products\\_services/iacs/cc\\_and\\_itsec/formal\\_docs.shtml](http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/formal_docs.shtml)

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

- a diagram of the TOE boundary, interfaces and any hardware interconnections, including platform dependencies;
- any constraints on the threat environment, the software environment and the methods of use;
- the assurance requirements, including Strength of Function (where applicable);
- any use of certified components or plans to re-use previous evaluation results;
- *(for a CC Version 3.1 evaluation at EAL2 or higher)* the product's security architecture, including: the security functionality covering initialisation, operation and shutdown; and the security functionality providing protection against bypass, tampering and other forms of attack.

69. In defining the scope of the TOE, the Sponsor should also take care to define:

- The technical environment of the TOE. (Any IT product or part of an IT product, that supports the TOE but is not considered as part of the TOE, must be considered as part of the technical environment.)
- The physical environment of the TOE, including the procedures which operate in the environment.

**70. The Sponsor must define the scope of the TOE in a way which provides a coherent set of security functions which are of genuine use to potential customers.**

71. If the scope of the TOE is considered to be unreasonable, the CB will not accept it into the Scheme. For example:

- a. for the evaluation of a firewall, the scope of the evaluation should normally include core information flow control functionality;
- b. management software that is provided as part of a product should normally be included in the scope of the TOE.

72. The TOE and its configuration(s) must reflect a common method of deployment, or at least one which may reasonably be expected to become common. It should also make a reasonable contribution to security, where in most cases the technical environment and the physical environment will also make contributions. The issue of acceptable TOE scoping is described in Annex A *Summary Guidance for TOE Scope Information*. Note that this information may be satisfied by a draft Security Target.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

73. Should the CB have concerns over the proposed scope of the TOE, then the Task Startup Review and Task Startup Meeting will provide an opportunity for the discussion of its concerns, and the options for an acceptable scope.

### Cryptographic Mechanisms

**74. The Sponsor must discuss with the CB, the evaluation of any cryptographic mechanisms used within the TOE.**

75. Special considerations apply to the extent of evaluation of cryptographic mechanisms and the responsibility for this; in some cases CESG may evaluate such mechanisms. Requirements for evaluation of cryptographic mechanisms will be agreed with the CB at the time of the Task Startup Review.

### Evaluation Deliverables

**76. The Sponsor must provide all the information required by the Scheme, including the TOE Scope Information and the required evaluation deliverables.**

77. TOE Scope Information is required for the Task Startup Review and Task Startup Meeting, as described above.

78. The CLEF and the Sponsor will agree a schedule for the supply of the deliverables. If the Sponsor is not the Developer, it is the Sponsor's responsibility to ensure that the Developer provides the required deliverables.

79. It is the content, rather than the precise format, of the deliverables which is significant. So, for example, evidence may be presented in a single deliverable to address all the requirements of one or more particular aspects of the criteria, or may be collected by the Evaluators from a number of sources.

80. Ideally, the various deliverables (with the possible exception of the Security Target) should be produced as part of the development process. This will enable the Developer to produce, most effectively, deliverables that take account of the assurance requirements. It is particularly recommended that production of any vulnerability analyses and test strategies should be started as early in the development life cycle as possible. The early delivery of these analyses to the Evaluators will not only expedite the evaluation, but will also enable the Sponsor to take prompt action on any problems regarding the TOE's security discovered by the Evaluators.

81. The level and content of the deliverables for CC and ITSEC evaluations are described in the relevant criteria and methodology documentation. Some additional notes are provided below.

82. **Vulnerability information.** For most assurance requirements, the Sponsor will need to produce a set of vulnerability analyses. It is expected that these will include appropriate comment on publicly reported vulnerabilities. The Sponsor is expected to track and fix vulnerabilities in a timely manner, as part of the process of

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

marketing a secure product, and this will necessarily require an awareness of public domain vulnerability information relevant to the TOE. If a Sponsor requires the evaluation of the process that is used to track and fix vulnerabilities to support Assurance Maintenance then the Evaluation Assurance Level (EAL) should be augmented with ALC\_FLR.*n* (for an appropriate choice of *n* = 1, 2 or 3.)

83. **Cryptographic mechanisms.** Sponsors should confirm, with either the CB or the CLEF as appropriate, the requirements for deliverables in respect of any such mechanisms.

84. **Previous evaluation results.** For the re-use of previous evaluation results, i.e. if a previously certified product is a component of a new TOE, or is to be re-evaluated after upgrade, the Sponsor should offer an analysis of where previous evaluation results may be re-used.

85. The validity of these results to the TOE can only be established during the preparation phase, as the complexity and variety of potential TOE compositions limits the detailed guidance that can be given in this document. The following general guidance can, however, be given:

a. If the assurance requirement of a previously certified component is greater than, or equal to, the target assurance requirement of the TOE, then the previous design and development results for that component can be used directly in the evaluation of the new TOE. If the assurance requirement of a previously certified component is below the target assurance level of the TOE, then it will not normally be possible to use the previous certification without further evaluation being performed.

b. If a certified product is used as a component of a new TOE, the context of its use may have changed. Hence, whilst the design and development results for the certified component with respect to its original Security Target are still valid, any vulnerabilities introduced in the context of its new use, or found since the previous certification, need to be tested.

c. If a certified product has been subjected to a major upgrade and the Sponsor wishes the later version to be certified, e.g. if it contains new or amended security functionality, a full re-evaluation would almost certainly be required.

d. If all of the changes in the previously certified component and its documentation are non security related then it is likely that the only evaluation activity required will be assessment of the guidance documentation together with functional and penetration testing.

### Security Target

<p>86. <b>The Sponsor must supply the Security Target for the TOE, based on the agreed scope of TOE.</b></p>
--

## **UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction**

87. The Security Target acts as the baseline for an evaluation and provides a detailed specification of security requirements against which a TOE will be evaluated. It identifies the scope of the evaluation in terms of the precise boundary of the TOE and its relationship with the TOE environment.

88. The Security Target must include the agreed scope of TOE. The Task Startup Meeting or Task Startup Review will have discussed the TOE Scope Information and may have given some advice on the content of the Security Target.

89. For the specified format of a Security Target, see the appropriate CC or ITSEC documentation<sup>9</sup>. It is recommended that the Security Target is produced with the assistance of experienced security evaluation consultants, in order to ensure an efficient evaluation.

90. As the first stage of the evaluation, the CLEF will evaluate the Security Target against the relevant criteria. The Evaluators will also check that the Security Target corresponds to the scope of TOE agreed at the Task Startup Meeting. On the basis of evidence from the CLEF, the CB will then carry out a Security Target Review and, if satisfied, will formally accept the Security Target as a basis for an evaluation. This ends the Preparation phase of the evaluation.

91. Any later changes to the Security Target will need a repetition of the Security Target Review process, although for straightforward changes this will be a simple review.

---

<sup>9</sup> For a Common Criteria Security Target see CC Part 1 (v3.1 Annex A or v2.3 Annex B). For an ITSEC Security Target see ITSEC (v1.2 Chapter 2).

## **IV. EVALUATION AND CERTIFICATION**

### **Introduction**

92. This chapter discusses the Evaluation and Certification processes. During the Evaluation process, the Evaluators perform the technical evaluation work (as defined by the criteria, methodology and Evaluation Work Programme) and they issue the Evaluation Technical Report which records the results of their work and identifies any unresolved issues, e.g. outstanding Level 4 Observation Reports. All issues identified are discussed between the relevant organisations; responsibility for resolving issues lies with the Sponsor.

93. The CLEF will provide the Evaluation Technical Report, as the final output of the evaluation process, to the Sponsor and the CB. The *final* Evaluation Technical Report must not have any outstanding Observation Reports at Level 1, 2 or 3.

### **Evaluation Process**

94. During the evaluation process, the Evaluators assess and analyse the deliverables (specified in the Deliverables List) and perform security functional and penetration testing (based on a list of potential vulnerabilities), to determine whether the TOE meets its Security Target and whether the TOE has adequate resistance to attack.

**95. The Sponsor must answer questions from the CLEF (within a reasonable time period, as agreed in advance), arising from detailed examination of the Security Target and other deliverables, and inform the CLEF about changes to the TOE during the course of the evaluation.**

96. Questions may arise in the form of Observation Reports or as a result of Evaluation Progress Meetings. Sponsors may also initiate changes to the product or its documentation during the evaluation.

### **Observation Reports**

97. During the course of an evaluation, the Evaluators may discover various issues relating to the TOE. Some of these issues may involve confirmed vulnerabilities, whilst others may involve failures to meet specific evaluation criteria. Once an issue has been confirmed in the TOE or its documentation, it will be raised as an Observation Report (OR) which is sent to the Sponsor and the CB.

98. Each OR raised is assigned a severity level as follows:

- *Level 1* – For any failure of the TOE to comply with its security objectives and security requirements that constitutes an exploitable vulnerability.
- *Level 2* – For any inability to comply with assurance requirements which increases the risk of an exploitable vulnerability remaining undetected; or for

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

any inability to comply with security functional requirements which constitutes a potential vulnerability. A Level 2 OR will also be used where an unacceptably high number of Level 4 ORs would otherwise exist.

- *Level 3* – For requesting clarification from the Sponsor or Developer, in order to confirm whether a Level 2 or Level 4 OR is required.
- *Level 4* – For reporting any inability to comply with the assurance requirements which does not warrant a Level 2 OR.

### **99. The Sponsor and Developer must provide resolutions for any Level 1, 2 or 3 Observation Reports raised.**

100. An OR at Level 1, 2 or 3 will, if not resolved, prevent certification of the TOE. Such ORs require a response from the Sponsor. The existence of unresolved Level 4 ORs will not prevent certification, but a response is desirable.

101. An OR will be cleared once the Sponsor's or Developer's resolution has been evaluated and confirmed as acceptable by the Evaluators. An OR may also be withdrawn if it is agreed that the issue raised is no longer of concern.

102. The Observation Report Status Register (ORSR) contains a summary of all ORs raised during an evaluation. The ORSR is maintained by the Evaluators. The ORSR will identify and summarise each OR, note its status and, where applicable, the body currently responsible for progressing its resolution.

### **Evaluation Progress Meetings**

### **103. When required by the CB, the Sponsor should attend Evaluation Progress Meetings with the CLEF and CB to review progress and technical issues.**

104. Evaluation Progress Meetings are meetings between the CB and the Evaluators to monitor and review aspects of the evaluation. In some cases Evaluation Progress Reviews perform the same function as Evaluation Progress Meetings, but without the need for a meeting.

105. These Evaluation Progress Meetings may be planned by the CB, but can also arise from unexpected issues. Sponsors are not usually expected to attend Evaluation Progress Meetings, but should be prepared to do so if required.

### **Evaluator Testing**

### **106. The Sponsor and Developer must ensure that the TOE is available for Evaluator Testing.**

107. Evaluator testing is performed on the evaluated configuration(s) of the TOE, which must be provided or made available by the Sponsor. The Sponsor and

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

Developer may be asked to provide the TOE either as a completely built product or as delivered to customers (to allow the Evaluators to exercise the guidance documentation; and to evaluate the delivery and installation process).

108. Evaluator testing may be performed in a standalone, representative environment. Where the TOE needs to be connected to a live system for testing, then the Sponsor should be aware that testing may expose vulnerabilities. Under these circumstances, it is the responsibility of the Sponsor to arrange to recover or fix the TOE.

109. The Sponsor should therefore arrange for appropriate backups prior to the start of the Evaluators' testing. Any potentially damaging tests should be arranged at a mutually convenient time to minimise potential inconvenience.

### Certification Process

110. A draft version of the Certification Report is produced by the Evaluators and reviewed by the CB and Sponsor. The final version will be issued by the CB, and published on the <http://www.cesg.gov.uk> and <http://www.commoncriteriaportal.com> websites.

**111. The Sponsor must confirm to the CB that the Certification Report fairly represents the Security Target and the outcome of the evaluation and does not contain proprietary information.**

112. It is important that the Sponsor agrees that the Certification Report is fair and correct. To ensure this, the draft Certification Report is issued to the Sponsor by the CLEF, so that the Sponsor can confirm to the CB that:

- the report fairly represents the Security Target;
- the report fairly represents the conduct and outcome of the evaluation;
- the conclusions of the report are accurate;
- the Sponsor is not aware of any factors which could invalidate the report.

113. The Sponsor must also confirm that the Certification Report does not contain proprietary information.

### Validity of Certificates

**114. The Sponsor and Developer should consider whether to maintain assurance in the TOE after certification.**

115. The Certification Report will identify the evaluated configuration of the certified TOE. However the validity of its certification may subsequently be eroded by any modifications made. For example these may take the form of:

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

- patches for vulnerabilities and other flaws;
- a new version or variant of the TOE;
- a sequence of new releases at periodic intervals.

116. The Sponsor is encouraged to maintain the assurance in the TOE. A number of services are offered by the Scheme to enable this. The type of service appropriate in a particular case will depend on the nature of the changes made and the evaluation criteria. The services offered are summarized in UKSP 01.

117. Sponsors are advised to keep evaluation deliverables material. The continued availability of such material will be useful if, in future, re-evaluation or re-use of the evaluation results is required.

### Vulnerabilities

**118. The Sponsor must inform the CB of any vulnerabilities in a product which is undergoing evaluation or after it has been certified.**

119. Once the Evaluators' testing has been completed by the CLEF, there is a period of time before the issue of a Certification Report in which new vulnerabilities may become known. During this time neither the Evaluators nor the CB will be actively searching for additional vulnerabilities but, if they become aware of any, they must raise the issue with the Sponsor. Likewise it is the responsibility of the Sponsor to inform the CB of vulnerabilities that come to their attention.

120. Should such vulnerabilities be found, then the Sponsor must propose a solution to the CB before certification can be completed. This may oblige the Sponsor to require extra evaluation work to be done by the CLEF.

121. The CB reserves the right to withdraw a certificate if a TOE is subsequently found to contain vulnerabilities that undermine its certification.

## **V. ASSURANCE MAINTENANCE**

122. Minor changes can be cost-effectively evaluated using an assurance maintenance approach agreed by the CB. See [UKSP01] and [UKSP03-II] for details.

**UK IT Security Evaluation & Certification Scheme  
Sponsor's Guide Part I – General Introduction**

**ANNEX A  
SUMMARY GUIDANCE FOR TOE SCOPE INFORMATION**

This annex provides a summary of the guidance for TOE Scope Information. Please refer to UKSP 01 and UKSP 02 Parts I & II for further details. Alternatively, contact the IA Delivery Office or one of the UK CLEFs for further guidance.

The last column in Table 1 below is intended to be a check (or tick) box so that all guidance points can be systematically “checked off”. The word “Define” is used to indicate that it is possible and necessary to provide a relatively greater level of precision for the associated item.

**Table 1 – Check List for TOE Scope Information**

#	Summary Guidance to Sponsors for TOE Scope Information	“✓”
1.	Provide an <i>informal</i> high level description of the whole product (or system <sup>10</sup> ) and its security functionality.	
2.	Describe the <i>architectural design</i> , including functional separation and interaction of the product components.	
3.	Describe the security contribution of each of the product components in software, hardware, and firmware.	
4.	Describe the interaction of the product with its environment in terms of interfaces & communication channels.	
5.	<b>Define</b> the <i>Target of Evaluation</i> (TOE) as either the whole product or a coherent set of product components.	
6.	Describe how the security functionality of the TOE is <i>self contained</i> in the context of the product.	
7.	Describe why the scoped out components cannot compromise the security functionality of the TOE.	
8.	<b>Define</b> the <i>TOE boundary</i> preferably with the assistance of a diagram clearly showing the TOE boundary.	
9.	<b>Define</b> the <i>secure configuration</i> of the TOE, by reference to a lockdown/hardening document if it exists.	
10.	Describe why the secure configuration of the TOE is reasonable and would be commonly used in practice.	
11.	<b>Define</b> the TOE <i>Evaluation Assurance Level</i> (EAL), including Protection Profiles, augmentations and extensions.	
12.	Describe why the chosen EAL is suitable and appropriate for the TOE and the TOE consumers.	
13.	Describe any relevant complementary assurance certificates (such as FIPS 140 for cryptographic modules).	

<sup>10</sup> For efficiency, from this point onwards, Tables 1 and 2 assume that “product” means “product (or system)”.

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

14.	<b>Define</b> the <i>assets</i> being protected by the TOE (excluding the TOE, which is not an asset in this context).	
15.	Describe the <i>threats</i> to the assets (excluding any threats to the TOE).	
16.	Describe the <i>threat agents</i> and their attack potential including time, money, skill, and other resources.	
17.	<b>Define</b> the <i>secure usage assumptions</i> for the TOE, including physical, procedural, and personnel.	
18.	<b>Define</b> the <i>security objectives</i> of the TOE, such as confidentiality, integrity, availability, authentication, etc.	
19.	<b>Define</b> a set of mutually supporting <i>Security Functional Requirements</i> (SFRs), for example from CC Part 2.  (This is not applicable to ITSEC evaluations.)	
20.	Describe any <i>security dependencies</i> on (and interfaces to) underlying operating system, database, networking, etc.	
21.	Describe the configuration of the intended <i>IT environment</i> and its associated security components.	
22.	Describe why the IT environment does not introduce any <i>obvious</i> security vulnerabilities to the TOE.	
23.	<b>Define</b> TOE <i>Security Functionality</i> (TSF) that satisfies the SFRs & objectives, and protects the assets from the threats.	
24.	Describe how the TSF prevents, detects, and corrects different types of attack on the security of the assets.	
25.	<b>Define</b> the <i>modes of operation</i> , such as: (re)booting, (re)configuration, normal, maintenance, backup, debug, etc.	
26.	Provide a mode transition diagram. Then identify and describe any attack points.	
27.	Describe the <i>update and patching</i> procedures, especially if these involve communications over untrusted networks.	
28.	Provide information on <i>potential</i> or <i>exploitable</i> vulnerabilities and security related bugs, or claim that there are none.	
29.	Provide some initial ideas on <i>penetration testing</i> , if it is possible, based on the Developer's vulnerability analysis.	

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

### Table 2 – General Advice for TOE Scope Information

1.	<p><i>Core functionality</i> supplied by the product <b>must</b> be scoped into the TOE.</p> <p><i>Management</i> functionality supplied as a part of the product should be scoped into the TOE.</p> <p><i>Client</i> functionality which is supplied as part of the product and commonly used to access claimed server security functionality should be scoped into the TOE.</p> <p><i>Third party products</i> used to access product management functionality (e.g. a browser) may be scoped out of the TOE, but should be present in the IT Environment during the evaluation tests.</p>	
2.	<p>The <i>TOE Security Policy</i> (TSP) is defined by the set of SFRs claimed for the TOE.</p> <p>The <i>TOE Security Functionality</i> (TSF) is defined by the TOE components which enforce the TSP.</p> <p>The <i>TOE Security Functionality Interface</i> (TSFI) resides at the TSF boundary.</p> <p>The TSF boundary and the TOE boundary should have some common segments (i.e. the TOE Security Functionality should never be “completely inside” the TOE).</p>	
3.	<p>In the following three table entries, which simply reproduce essential Scheme principles from [GTS] and [TSI], the following acronyms are used:</p> <ul style="list-style-type: none"> <li>• CCP<math>n</math> = Common Criteria Principle <math>n</math></li> <li>• SP<math>n</math> = Sponsor Principle <math>n</math></li> <li>• EP<math>n</math> = Evaluation Principle <math>n</math></li> </ul> <p>The principles are quite general and hence are applicable to any version of CC and ITSEC.</p>	
4.	<p>CCP1 The TOE must be well integrated in its scope; in effect it will correspond to the product or a self-contained coherent product subset.</p> <p>CCP2 Many IT security solutions comprise compositions of component products, typically from different Developers. In such situations it will often be appropriate for a base component to be individually certified, potentially before certification of its composition with a dependent component.</p>	
5.	<p>SP1 The TOE must reflect a common method of deployment of the product.</p> <p>SP2 The TOE must make a meaningful contribution to countering the identified security threats.</p> <p>SP3 There may be limitations on the degree of influence which the Sponsor has over the Developer of environmental IT components needed to support the TOE. Approaches exist for pragmatic consideration of an environmental IT component where its Developer does not wish to directly support the evaluation of the TOE.</p> <p>SP4 In some situations the Sponsor may demonstrate a complementary non-CC form of assurance for certain aspects of product security functionality, e.g. FIPS-140 for cryptographic functionality.</p> <p>SP5 In some situations the scope of what can feasibly be evaluated may be subject to the state of the art, e.g. content checking.</p> <p>SP6 Questions may arise in relation to the consistency of either attack potential or assurance claims.</p>	

## UK IT Security Evaluation & Certification Scheme Sponsor's Guide Part I – General Introduction

6.	<p>EP1 The evaluation is required to focus on components and interfaces related to the claimed SFRs within the boundary of the TOE.</p> <p>EP2 The contribution which it is claimed the TOE makes in countering the identified security threats must be realised, within the constraints of the chosen Evaluation Assurance Level (EAL).</p> <p>EP3 The contribution which it is claimed environmental IT products make in countering the identified security threats must be realised, within the constraints of the visibility of the environmental IT products, and their dependencies, as allowed by the evaluation.</p>	
7.	<p>A Security Target may be provided to satisfy the requirement for <i>TOE Scope Information</i>. If the Security Target was from a previous evaluation then details of any changes should also be indicated (using <i>Track Changes</i>, if possible). If the Security Target is a draft then additional supporting information may also be required (see Table 1).</p>	
8.	<p>The Security Target is essential to the success of the evaluation process. Therefore, it is highly recommended that a professional security consultant (e.g. from one of the CLEFs or from the CLAS community) either produces, or at least reviews, the draft Security Target before submitting it into the evaluation process.</p>	
9.	<p>Information about the TOE may be provided by various means, such as website entries, Security Targets, and Certification Reports. This information should be factual, informative, concise, unambiguous, consistent, not misleading, and not contain "marketing hype".</p>	
10.	<p><b>The <i>TOE Scope Information</i> is required from the Sponsor at least 10 working days in advance of the Task Startup Meeting/Review. The Certification Body will determine whether to provide approval for the continuation of the evaluation based on the <i>TOE Scope Information</i>.</b></p>	