UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No 1

DESCRIPTION OF THE SCHEME

Issue 4.0

February 2000

Issued by:-

UK IT Security Evaluation & Certification Scheme

Certification Body

(This page is intentionally left blank)

FOREWORD

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

This document provides a high level description of the Scheme and the procedures applied under it. Other Scheme documents must be referred to for fuller detail. It is intended for use by potential customers (i.e. anyone concerned with the development, procurement or accreditation of IT systems or products in which security is a consideration) as well as those already involved in the Scheme (i.e. Scheme employees, current customers, contractors and security consultants).

Dr K Thacker
Senior Executive
UK IT Security Evaluation and Certification Scheme

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

Address:	UK IT Security Evaluation & Certification Scheme Certification Body PO Box 152 Cheltenham Glos GL52 5UF United Kingdom
Telephone:	+44 (0)1242 238739
Facsimile:	+44 (0)1242 235233
E-mail:	info@ITSEC.gov.uk
Website:	http://www.itsec.gov.uk

AMENDMENT RECORD

Amendments to this document will be published as and when required. All changes made since the last major update of the document will be outlined in the amendment record and marked in the document itself.

Issue Number	Major Changes	Date
4.0	Major update. (including changes to: - reflect current status of CC, - restructure chapters III and IV)	February 2000

TABLE OF CONTENTS

REFERENCES

[a] Mutual Recognition Agreement of Information Security Technology Security Evaluation Certificates, Management Committee of Agreement Group.

[b] Information Technology Security Evaluation Criteria (ITSEC), Commission of the European Communities.

[c] ITSEC Joint Interpretation Library (ITSEC JIL), Joint Interpretation Working Group.

[d] Information Technology Security Evaluation Manual (ITSEM), Commission of the European Communities.

[e] Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of Information Technology Security.

[f] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
Part 2: Security functional requirements,
Part 3: Security assurance requirements,
Common Criteria Interpretations Management Board.

[g] Common Methodology for Information Technology Security Evaluation,
Part I: Introduction and General Model,
Part II: Evaluation Methodology,
Common Evaluation Methodology Editorial Board.

[h] UK Scheme Publication No 2 - The Appointment of CommerciaL Evaluation Facilities, UK IT Security Evaluation & Certification Scheme.

[i] UK Scheme Publication No 4 - Developers' Guide, Part I: Roles of Developers in ITSEC, UK IT Security Evaluation & Certification Scheme.

[j] UK Scheme Publication No 4 - Developers' Guide, Part II: Reference for Developers, UK IT Security Evaluation & Certification Scheme.

[k] UK Scheme Publication No 4 - Developers' Guide, Part III: Advice to Developers, UK IT Security Evaluation & Certification Scheme.

[l] UK Scheme Publication No 5 - Manual of Computer Security Evaluation, Part I, Evaluation Procedures, UK IT Security Evaluation & Certification Scheme.

[m] UK Scheme Publication No 5 - Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools, UK IT Security Evaluation & Certification Scheme.

[n] UK Scheme Publication No 6 - Certified Product List, UK IT Security Evaluation & Certification Scheme.

[o] UK Scheme Publication No 11 - Scheme Information Notices Folder, UK IT Security Evaluation & Certification Scheme.

[p] UK Scheme Publication No 12 – Relationship between Accreditation Document Set and Security Targets for Evaluation, UK IT Security Evaluation & Certification Scheme.

[q] UK Scheme Publication No 16 - UK Certificate Maintenance Scheme, Part I: Description of the CMS, UK IT Security Evaluation & Certification Scheme.

[r] UK Scheme Publication No 16 - UK Certificate Maintenance Scheme, Part II: Impact Analysis and Evaluation Methodology, UK IT Security Evaluation & Certification Scheme.

[s] UK Scheme Publication No 16 - UK Certificate Maintenance Scheme, Part III DSA Reference Manual, UK IT Security Evaluation & Certification Scheme.

[t] CESG Infosec Memorandum No. 1: Register of CESG and UK ITSEC Scheme Documentation, CESG Publications Department.

[u] CESG Compusec Memorandum No 2, Handbook of Computer Security Evaluation, CESG Publications Department.

[v] CESG Compusec Memorandum No 3, UK Systems Security Confidence Levels, CESG Publications Department.

[w] CESG Compusec Manual A: Manual of Computer Security Evaluation, CESG Publications Department.

[x] Manual of Protective Security (MPS), Cabinet Office Security Division.

[y] Supplement A to Chapter 5 of MPS, Cabinet Office Security Division,

also issued as HMG Infosec Standard No 1: Assurance Requirements for IT Systems, CESG Publications Department.

[z] Supplement B to Chapter 5 of MPS, Cabinet Office Security Division,

also issued as HMG Infosec Standard No 2: Accreditation Documents, CESG Publications Department.

[aa] Information Security Assurance Guidelines for the Commercial Sector, DTI.

[bb] Protecting Business Information: Understanding the Risk, DTI.

[cc] Protecting Business Information: Keeping it Confidential, DTI.

[dd] BS7799
Part I: Code of Practice for Information Security Management,
Part II: Specification for Information Security Management Systems.

[ee] EN 45001, General Criteria for the Operation of Testing Laboratories.

[ff] EN 45011, General Requirements for Bodies operating Product Certification Systems.

[gg] ISO Guide 25 - ISO/IEC Guide 25: 1990, General Requirements for the Competence of Calibration and Testing Laboratories.

[hh] M10 – NAMAS Accreditation Standard, General Criteria of Competence for Calibration and Testing Laboratories, NAMAS (now UKAS).

[ii] M11 - NAMAS Regulations, Regulations to be met by Calibration and Testing Laboratories, NAMAS (now UKAS).

[jj] ISO Guide 65 - ISO/IEC Guide 65: 1996 General Requirements for Bodies Operating Product Certification Systems

ABBREVIATIONS

CB	Certification Body (of the UK Scheme)
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	CommerciaL Evaluation Facility
CMAR	Certificate Maintenance Audit Report
CMP	Certificate Maintenance Plan
CMS	Certificate Maintenance Scheme
CMSR	Certificate Maintenance Status Report
COTS	Commercial Off The Shelf
CR	Certification Report
DSA	Developer Security Analyst
DTI	Department of Trade and Industry
EPM	Evaluation Progress Meeting
ETR	Evaluation Technical Report
EWP	Evaluation Work Programme
HMG	Her Majesty's Government
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
JIL	ITSEC Joint Interpretation Library
MOD	Ministry of Defence
MPS	Manual of Protective Security
NATO	North Atlantic Treaty Organisation
Scheme	UK IT Security Evaluation and Certification Scheme
SIA	Security Impact Analysis
TIN	Task Initiation Notice
TOE	Target of Evaluation
UK	United Kingdom

UKAS	United Kingdom Accreditation Service
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

I. OVERVIEW OF THE UK SCHEME

Introduction

1. In December 1989 Her Majesty's Government (HMG) announced the creation of a new Scheme to evaluate and certify the trustworthiness of security features in Information Technology (IT) products and systems. It is called the UK IT Security Evaluation and Certification Scheme (hereafter referred to as "the Scheme").

2. The objective of the Scheme is to meet the needs of Industry and Government for cost effective and efficient security evaluation and certification of IT products and systems. The Scheme also provides a framework for the international mutual recognition of certificates [a], [e] in terms of the Information Technology Security Evaluation Criteria (ITSEC) [b] and the Common Criteria (CC) [f] respectively.

3. The Scheme became effective on 4 July 1990 and, following a preparatory stage, has been fully operational since the first quarter of 1991 from which time the detailed provisions of the Scheme became binding upon the participants entering the Scheme. In particular, the Scheme has been adopted by HMG where IT security evaluation and certification is required for UK systems and products used to store, process or forward national protectively-marked information.

4. This document describes the Scheme and the procedures applied under it. It is intended for use by potential customers (i.e. anyone concerned with the development, procurement or accreditation of IT systems or products in which security is a consideration) as well as those already involved in the Scheme (i.e. Scheme employees, current customers, contractors and security consultants).

5. This document will be updated when appropriate. In the first instance changes will be introduced into the softcopy on the Scheme web site, with sidebars used to indicate changes since the last major update. Hardcopy of selected versions, including major updates, will be published periodically.

The Scheme

6. The objective of the Scheme is to meet the needs of all sectors of Industry and Government, by offering evaluation and certification services to:

   a. vendors, to enable them to demonstrate the security claims of their products and systems;

   b. procurers, to allow them to satisfy themselves that their security objectives are met by the proposed products and / or systems;

   c. accreditors, to allow them to satisfy themselves that their security threats are addressed by the countermeasures in the products and / or systems protecting their information.

7. The Scheme is operated by the UK Government's Communications-Electronics Security Group (CESG) under the direction of a Management Board as described in Chapter II.

8. It establishes a single UK Certification Body (hereafter referred to as the CB), operating in all sectors of Industry and Government, to certify the results of evaluations of systems and

products and to deal with other nations on the mutual recognition of such certificates. To this end the CB will comply with the EN 45011standard [ff] as set out in the CB quality procedures. This standard is equivalent to ISO Guide 65 [jj].

9. The Scheme also establishes an organisational and procedural framework for the conduct of evaluations in the UK, including the appointment of CommerciaL Evaluation Facilities (CLEFs), who carry out the evaluations, and the establishment of approved techniques and procedures.

10. The appointment of a CLEF is dependent on the CLEF being accredited as a testing laboratory by the UK Accreditation Service (UKAS) in accordance with the NAMAS Accreditation Standard, M10 [hh], and NAMAS Regulations, M11 [ii], to perform tests or types of test specified in a prescribed Schedule.

11. The UKAS Accreditation Standard is consistent with the provisions of ISO Guide 25 [gg] and EN 45001 [ee]. Laboratories accredited by UKAS meet the requirements of ISO Guide 25 and EN 45001 and may also be considered as meeting those requirements concerned with the adequacy of testing contained in the ISO 9000, EN 29000 and BS 5750 series of specifications on quality assurance.

12. The scope of CLEF accreditation is limited to tests that meet UKAS requirements reflecting the following four principles:

impartiality - all evaluations must be free from bias (it must be possible to demonstrate that neither the CLEF, nor individual CLEF staff concerned with a particular evaluation, has a commercial or financial interest in the outcome of the evaluation);

objectivity - the property of a test whereby the result is obtained from the evidence provided, with the minimum of subjective judgement or opinion;

repeatability - the repeated evaluation of the same system or product against the same set of security requirements by the same organisation yields the same overall result as the first evaluation;

reproducibility - the evaluation of the same system or product against the same set of security requirements by a different organisation yields the same overall result as the first organisation.

13. It is not possible to accredit all tests performed by a CLEF, as some aspects of security testing may require subjective interpretation (e.g. on account of the nature of a specific Target of Evaluation (TOE) or where the criteria need clarification). In such cases the CB plays an active role to ensure consistent application of the critera and reporting of evaluations across all evaluations and CLEFs by:

a. agreeing UK interpretations;

b. maintaining and updating the UK evaluation methodology in order to reduce subjectivity (e.g. ITSEC [b], Joint Interpretation Library (JIL) [c] and IT Security

Evaluation Methodology (ITSEM) [d] are supported within the UK by UKSP 05 Part III [m], UKSP 11 [o] and UKSP 16 Part II [r]);

c. seeking further agreement, on interpretations and methodology, with its international mutual recognition partners.

14. In addition to the above UKAS requirements, which relate to the conduct of evaluations and the reporting of test results, CLEFs are required to meet the highest standards of confidentiality by:

a. operating policies and procedures to ensure the protection of proprietary rights and information, to protect commercial confidentiality,

b. meeting HMG security standards as laid down in the Manual of Protective Security [x], so that they are in a position to conduct evaluations bearing on national security.

15. The CB plays an active role in the evaluation process by:

a. determining whether a TOE will be certifiable in principle before accepting a proposed evaluation into the Scheme;

b. monitoring all evaluations conducted under the Scheme in a manner appropriate to the assurance level, holding periodic meetings with the CLEF as appropriate;

c. assessing all evaluation results, issuing certificates as appropriate.

16. Therefore, whilst the conduct of individual evaluations and the quality standards enforced are in general left to the CLEFs, the validity and consistency of evaluation results are endorsed by certification under the Scheme.

Certification

17. The objective of certification is independently to confirm the validity of evaluation results and thereby to ensure comparability of these results across all evaluations over all evaluation facilities.

18. Certification confirms that:

a. the TOE meets its Security Target (to the claimed assurance level);

b. the evaluation has been conducted in accordance with the standards of the Scheme.

19. Certification does not endorse a TOE in any other respects. Moreover it does not imply that the TOE is guaranteed to be completely free of exploitable vulnerabilities; there will remain a small probability (smaller with higher assurance levels) that some exploitable vulnerabilities remain undiscovered.

IT Security

20. Computer-based information systems now play an important and often vital role in all sectors of society. Whether it is for business, public sector or domestic use, the dependence on IT is becoming greater and more widespread. As a consequence the potential risks, such as those associated with unauthorised access, must increasingly be a cause for concern.

21. The DTI has produced a number of documents to help the commercial sector understand the risk [bb], how to keep data confidential [cc] and the level of assurance needed [aa]. For the government sector, the Cabinet Office with advice from CESG and others has laid down minimum standards for computer security in HMG Infosec Standard No 1 [y]. CESG has produced several other documents listed in CESG Infosec Memorandum No. 1 (Memo 1) [t].

22. A significant contribution to the security of an IT system can often be achieved through non-technical measures such as organisational and administrative controls. However, there is a growing tendency to use additional technical IT security measures. In many cases these provide the principal means of preventing the theft or destruction of valuable assets. A good overview is provided by the British Standard BS7799 [dd].

23. In the context of the Scheme, IT security means:

confidentiality -	the prevention of the unauthorised disclosure of information;
integrity -	the prevention of the unauthorised modification of information;
availability -	the prevention of the unauthorised withholding of information or resources.

Any or all of these aspects may be of importance in a particular case.

24. Those responsible for selecting IT products with security features appropriate to their needs face a difficult assignment. For example, lack of information about the strengths and weaknesses of particular products can result in over-investment in unnecessary features, or worse still, lead to an increased exposure to risk.

25. In particular, problems which can add to risks when purchasing products to meet security requirements include:

a. the security claims for a product may not be justified;

b. the security claims may be presented in a form which makes comparison between competing products difficult;

c. the products may have inadequate supporting documentation;

d. the products may interact with other products in a way that exposes a vulnerability;

e. the products may originate from a potentially unreliable source.

Security Evaluation

26. Users of products or systems need confidence in the security functionality provided. Users also need a yardstick to compare the security capabilities of products they are thinking of purchasing. Although users could rely on trust in the developers of the systems or products in question, or could test them themselves, it is likely that many will prefer to rely on the results of some form of impartial assessment by an independent body. This assessment is called Security Evaluation, while the IT system or product being evaluated is referred to as the "Target Of Evaluation" (TOE).

27. It is important that such evaluation should be carried out in accordance with widely recognised procedures and standards. In the case of IT products, the vendor's market will be

limited by customer recognition of the standards achieved. In the case of systems, universal recognition may not be so important, but, for example, where two separately evaluated systems are to be interconnected, the users of each system will need to recognise the validity of the other's evaluation.

28. The sets of evaluation criteria currently recognised by the Scheme and the methodologies associated with them are:

    a. CC [f] and the Common Evaluation Methodology (CEM) [g];

    b. ITSEC [b] and ITSEM [d];

    c. UK Confidence Levels [v] and the methodology in CESG Compusec Memorandum No. 2 (Memo 2) [u], and Manual A [w].

29. The lower the residual risk that is acceptable following evaluation, the greater the confidence required from evaluation will be. Each set of evaluation criteria therefore offers a choice of predefined assurance or confidence levels.

30. The UK Confidence Levels are included as they are still in use in a few system evaluations. The Scheme no longer accepts product evaluations against the UK Confidence Levels.

31. ITSEC and ITSEM represent the outcome of international effort within Europe to align and develop the criteria and methodology of the UK and other nations. Experience in the application of ITSEC has resulted in European agreement on the interpretation of a number points in the criteria, which have been published in the form of the JIL [c].

32. CC represents the outcome of subsequent international efforts to align and develop the existing European and North American criteria. CC is backwards compatible to ITSEC so ensuring that the investment in ITSEC evaluations is protected. CC is the latest of the sets of criteria to be developed and used by the Scheme. CC has become an ISO standard, ISO/IEC 15408, which will lead to CC being adopted as a world standard for IT security evaluations.

33. CC is the set of criteria recommended by CESG for product evaluations as CC certificates are recognised widely. However, Sponsors also have the choice of ITSEC which is still a legal requirement in some countries.

34. Version 1.0 of CEM, which addresses assurances levels EAL1 to EAL4 (including assurance packages comprising components taken from those assurance levels), has now been internationally agreed as the CC methodology.

Security Target

35. It should be noted that evaluation of a product or system can only be performed, and certification given, against an explicit Security Target. Preparation of the Security Target is the responsibility of the Sponsor, although advice may be sought from a CLEF.

36. The Security Target serves as both a specification of the security functions, against which the TOE is evaluated, and as a description relating the TOE to the environment in which it will operate. It also specifies the assurance level against which the TOE is evaluated.

37. The Security Target should be specified in terms of the relevant set of criteria, drawing on the guidance given in the criteria on the presentation and content of Security Targets for systems and products.

a. In the case of a product evaluation, the Security Target includes a list of claims for the product, made by the Sponsor (usually the vendor of the product).

b. In the case of a system evaluation, the Security Target is dependent on the operational environment for the system. In determining the adequacy of the Security Target to represent the system's requirements, the Sponsor may draw on local or other standards and advice, principally from those involved in the accreditation process

38. Generic sets of evaluation requirements, which may be used as the basis for a Security Target, exist for ITSEC in the form of standard functionality classes, and for CC in the form of protection profiles prepared by communities of interest. Protection profiles may themselves be evaluated and certified, to confirm that they comply with the specification standards of CC [f].

Mutual Recognition

39. It is HMG's aim that the certificates issued under the Scheme should also be recognized, at least for commercial and non protectively-marked Government applications, throughout the European Union (and the European Economic Area) and North America and, as far and as soon as possible, in the wider international context.

40. In November 1997, the Senior Officials Group for Information Security (SOG-IS) of the European Commission approved the Recognition Agreement of Information Technology Security Evaluation Certificates based on ITSEC [a]. The agreement came into force in March 1998 and now covers Finland, France, Germany, Greece, Italy, Netherlands, Norway, Spain, Sweden, Switzerland and the United Kingdom. These nations agree to recognise ITSEC certificates from the Qualifying Certification Bodies which are SCSSI of France, BSI of Germany and CESG of the UK.

41. The agreement was extended to cover Common Criteria up to EAL7 in April 1999 and the above countries except Germany have signed up to the changes.

42. The CC Mutual Recognition Arrangement was signed in October 1998 [e] and includes Canada and the United States of America as well as France, Germany and the United Kingdom. The CC Mutual Recognition Arrangement is currently limited to assurance levels EAL1 to EAL4 (including assurance packages comprising components taken from those assurance levels). Australia and New Zealand joined this arrangement in 1999.

43. A memorandum of understanding has been agreed between CESG of the United Kingdom and DSD of Australia and GCSB of New Zealand to recognise each other's ITSEC certificates up to E6 and is expected to be signed in 2000.

44. A Harmonised Mutual Recognition Arrangement incorporating all the above is being negotiated and is expected to be signed in 2000.

45. The Scheme, by ensuring that the appropriate methodology is applied consistently and correctly in assessing a TOE against the relevant set of criteria, is an essential prerequisite for international mutual recognition of the certificates awarded.

46. It is also HMG's intention that certificates should be valid for both UK national security applications and in the context of NATO requirements.

47. In the above international agreements there is a clause which states that where national security is at stake, certificates issued by other countries will not necessarily be recognised.

Advice to HMG Departments

48. With regard to HMG systems and any system intended to process, store or forward national protectively-marked information, CESG has a special role and can act independently of the CB and the Scheme to advise on fitness for purpose. As the UK National Computer Security Technical Authority, CESG is available to advise HMG Departments and their contractors on the security of protectively-marked information. This activity is not covered by the Scheme and is not further referred to in this document.

(This page is intentionally left blank)

II. ORGANISATION AND MANAGEMENT

Introduction

49. This Chapter describes the roles of the principal participants in the process of security evaluation and certification. It also describes associated policy and approach. The principal participants in an evaluation under the Scheme are the:

    Management Board;

    Certification Body (CB);

    CLEF;

    Sponsor;

    Developer;

    Accreditor.

    The text is keyed to the diagram at Annex B, which is an overview of the organisation of the principal participants in evaluation, identifying the flow of key documents.

Management Board

50. The Scheme Management Board exists to provide the CB with top level direction to ensure the Scheme continues to provide a cost effective and efficient IT security evaluation and certification service to UK Government and industry alike by:

    a. setting and reviewing policy;

    b. monitoring the performance of the CB and the Scheme overall;

    c. arbitrating over appeals, complaints and disputes.

51. All new policies, and any significant interpretations of policy, will be promulgated as part of the general Scheme documentation.

52. As a minimum, to ensure that matters affecting national security, industry and defence procurement are addressed, the Board includes the Senior Executive of the Scheme and the Head of the CB, other members of senior management from CESG, DTI and MOD, and other representatives from Civil Government Departments and industry. The Board is normally chaired by the senior representative of CESG.

53. The terms of reference of the Management Board are:

    a. to set policy and objectives for the operation of the Scheme, taking account of the identified requirements of vendors, procurers, accreditors and other interested parties, as represented by the individual members;

    b. to consider, approve and keep under review the rules for:

    – the operation of the CB

    – the operation of the Scheme as a whole

- the appointment of CLEFs
- the Scheme appointment programme;

c. to make recommendations to the appropriate HMG committees on the financing and resourcing of the CB;

d. to receive and consider an annual report from the CB on its operation;

e. to keep the appropriate HMG committees informed;

f. to publish an annual report;

g. to arbitrate in disputes arising in the context of the Scheme.

54. The Management Board is responsible for providing sufficient resources for the CB. The quality of evaluations is influenced by the Management Board, through the rules of the Scheme, including the appointment conditions.

55. The provision of CLEFs is in general left to the operation of market forces, but may be influenced through appointment policy. An objective of this policy will be to encourage competition by discouraging monopolies.

Certification Body

56. The Certification Body (CB) for the Scheme is under the direction of the Management Board. It is based at CESG in Cheltenham, where it is able to draw on a considerable wealth of experience and expertise in computer security from a number of government bodies. It operates under a Senior Executive from CESG, with staff drawn from CESG and contractors to CESG.

57. To meet the requirements of Industry and Government, the terms of reference of the CB are:

a. to appoint CLEFs and keep their appointments under review, by drawing on accreditations by UKAS, and by directly monitoring the work and performance of the CLEFs;

b. to provide advice, support and the standards for training to CLEFs;

c. to register the evaluation status of CLEF staff;

d. to confirm the suitability of Security Targets and agree Evaluation Work Programmes for certification purposes;

e. to register all evaluations under the Scheme for certification;

f. to certify the results of evaluations conducted under the Scheme, and to provide details of certified and CMS Approved products in UKSP 06 [n];

g. to approve press releases and similar statements relating to the Scheme;

h. to liaise with the appropriate national and international agencies on the mutual recognition of certificates;

i. to provide reports to each meeting of the Management Board;

j. to develop and maintain the UK evaluation methodology described in UKSP 05 Part III [m], UKSP 11 [o] and UKSP 16 Part II [r], ensuring consistency with evolving international criteria and methods.

58. The quality of evaluations is influenced by the CB through the rules of the Scheme and by its continuous oversight of the detailed work of the CLEFs.

CLEF

59. CLEFs contract with CESG to operate under the Scheme. CLEFs are obliged as a condition of their appointment to observe all rules of the Scheme as laid down by the Management Board.

60. As described under "The Scheme" in chapter I, CLEFs are obliged to observe the highest standards of impartiality and commercial confidentiality and to meet HMG's national security standards as laid down in the Manual of Protective Security [x].

61. The CLEF is obliged to have the status of each of its individual evaluators recognised by the CB. All evaluators are required to undertake a training programme and to gain supervised evaluation experience.

62. The CLEF is subject to scrutiny, by both the CB and UKAS as appropriate, to ensure that it meets its obligations. The CLEF takes an active role in this process, and is obliged to keep the CB informed of all relevant factors (e.g. by supplying the CB with regular summaries of evaluation and related work being undertaken and the deployment of its staff on such work).

63. Further details of the appointment and operating arrangements for CLEFs are documented in UKSP 02 [h] and UKSP 05 Part I [l].

Sponsor

64. The term "Sponsor" is used to refer to the person or organisation that requests an evaluation and is entitled to receive the reports produced. The relationship of a Sponsor to a TOE may vary depending on the nature of the TOE and other factors. The Sponsor may, for example, be the vendor of an IT product or the procurer of an IT system. Often the relationship may be less straightforward: for example the Sponsor may be a developer/integrator contracted by a procurer and required to deliver a secure system. The Sponsor may be a consortium where one point of contact is nominated to represent a number of developers and vendors.

65. The motives of a Sponsor of an evaluation may thus vary widely. The Scheme does not normally concern itself with the motivation of the Sponsor, provided that they are acting in good faith, are prepared to abide by the rules of the Scheme, and do not intend to exploit the Scheme for illegal or other undesirable purposes, or attempt to bring the Scheme into disrepute.

66. In many cases the Sponsor may be the developer of the TOE. But this will not always be so, and the procedures need to allow for the case where the TOE was developed by a third party. The procedures therefore differentiate between the Sponsor and Developer roles where appropriate.

67. The obligations of the Sponsor of an evaluation are described in UKSP 04 Part I [i].

Developer

68. The term "Developer" is used to refer to the organisation (or organisations) which has produced the TOE (or component parts of the TOE). Where the Developer is not the Sponsor, it will usually be necessary for the Developer to be prepared to co-operate with the Sponsor and agree to support the evaluation. The exception to this is the CC EAL1 assurance level, where the aim is to perform an evaluation purely on the strength of the TOE itself, including its accompanying guidance documentation. Typically however the Developer's co-operation will be needed, for example by providing technical evaluation deliverables to the CLEF (such as those needed to justify strength of mechanism/function claims or those associated with security relevant Commercial Off The Shelf (COTS) products).

69. In some instances there may be more than one Developer involved in an evaluation, for example in cases where sub-contractors are involved. There is an increased need in such cases for the Sponsor to ensure the co-operation of all parties.

70. The obligations of the Developer are described in UKSP 04 Part I [i].

Accreditor

71. The term "Accreditor" is normally used in the system context. An Accreditor is typically an individual, or organisation, responsible for the security of a system. In addition to those technical features provided by an IT system, accreditation will address the physical, personnel and procedural security features.

72. The main involvement of an Accreditor in the lifecycle of a system occurs :

    a. during the initial definition of the security requirements which will define the evaluation scope;

    b. when approval is needed for a system to become operational;

    c. whenever the system or its environment is changed or upgraded.

73. For the benefit of HMG accreditors UKSP12 [p] relates the recommendations of HMG Infosec Standard No 2 [z] to the Scheme, giving particular focus to the relationship between the Accreditation Document Set and the Security Target required for evaluation.

Appointment Policy

74. Appointment policy is determined from time to time by the Management Board, and covers:

    a. the number of CLEF appointments in existence under the Scheme at any time and their duration;

    b. the terms of CLEF appointments, as specified in UKSP 02 [h];

    c. selection procedures for appointees and any charges payable.

    In doing this, the aim of the Management Board is to ensure the viability and effectiveness of the Scheme as a whole, including the adequate provision of CLEFs to meet the demand for evaluation services, the commercial viability of existing CLEFs, and the adequate provision of certification resources.

75. The Management Board will provide notice of any major change to general appointment policy affecting the terms, conditions and duration of current appointments. Such changes will be promulgated as part of the general Scheme documentation.

76. The CB shall provide notice of withdrawal, non-renewal or intention to vary the terms of an appointment and expects notice of a CLEF's intention to withdraw from the Scheme. The CB may suspend or withdraw appointed status at short notice if a CLEF fails to meet the conditions of appointment. Full details of appointment policy are provided in UKSP 02 [h].

Publications and Publicity

77. A series of UK Scheme Publications (UKSPs), including this document "Description of the Scheme" (UKSP 01), is provided by the CB. Other documents of particular interest to the Sponsor and Developer include:

    a. The "Developers' Guide" (UKSP 04). Part I [i] is criteria independent, while Parts II [j] and III [k] are currently specific to ITSEC.

    b. The UK "Certified Product List" (UKSP 06) [n].

    c. The description and methodology for the "UK Certificate Maintenance Scheme" (UKSP 16). Part I (description) [q] is criteria independent, while Part II (methodology) [r] is currently specific to ITSEC.

78. Additional press releases and similar statements referring to evaluation or certification may be made provided that CB agreement is first obtained (the CB will wish to satisfy itself that such statements will not misrepresent the conclusions of the evaluation or certification or otherwise bring the Scheme into disrepute).

Appeals Procedure

79. Any dispute concerning the operation of the Scheme may be referred to the CB by any party - Sponsor, Developer or CLEF. If this course of action is considered to be ineffective, or if the CB itself is involved in the dispute, the party may appeal to the Management Board for resolution.

80. An appeal hearing by the Management Board shall be attended by the Chairman, the Senior Executive of the Scheme and at least one other Board member. The Head of the Certification Body and no more than two representatives of each party to the dispute shall have a right to be heard at the appeal hearing. The decision of the Management Board shall be final.

(This page is intentionally left blank)

III. PREPARATION FOR SECURITY EVALUATION

Introduction

81. This Chapter provides an overview of the first phase in the process of evaluation and certification. A diagrammatic overview of the preparation for security evaluation activities is provided in Annex C (Part C1). More detailed guidance for the Sponsor and Developer is provided in UKSP 04 Part I [i].

Contractual Considerations

82. The Sponsor will need to obtain quotations for the cost of both the evaluation and certification services from the CLEFs and the CB respectively.

83. The CB requires the Sponsor to enter into contracts with CESG covering the preparation phase services and the evaluation and certification phase services (further contracts will be necessary if certificate maintenance is subsequently required).

84. Sponsors and potential sponsors should thus approach the CB for a certification quotation at the same time as they contract with the CLEFs, and should enter into a contract with CESG to enable the CB to commence its certification activity in a timely manner.

85. It is common practice for the Sponsor to contract the same CLEF to perform the evaluation activities in both phases, and also to provide consultancy where required. However other options are available to the Sponsor; for example a consultant might be employed to prepare a Security Target which could then be used to obtain quotes from CLEFs for evaluation services.

86. Note however that, if the evaluation is sufficiently limited, for example for evaluation of a CC protection profile, it is possible that a single phase will be appropriate to include all evaluation and certification activities.

87. The Sponsor is advised to:

a. give due consideration to the requirements which evaluation may impose on other parties, particularly the Developer where different from the Sponsor (see below under "Deliverables");

b. arrange access to relevant outputs from any component product evaluation, particularly the Security Target and Certification Report, (where the TOE contains component products which have previously been certified, use of such results should assist the evaluation of the TOE);

c. give timely consideration to the cost of maintaining the certificate, if appropriate (see the "Certificate Maintenance" chapter. Note also that, to minimise future evaluation effort, it is possible to arrange for the CLEF to take re-evaluation requirements into account when performing the first evaluation);

d. obtain ownership of outputs from the evaluation process (availability of these outputs can assist re-evaluation or any other re-use).

Objective

88. The objective of the preparation phase is to determine the suitability and readiness of the TOE for evaluation prior to the evaluation conduct phase. This is a risk reduction exercise which is supported by the following activity:

    a. determination of the Security Target;

    b. determination of the deliverables needed to support the evaluation;

    c. agreement of an Evaluation Work Programme for the evaluation;

    d. determination of the purpose and scope of evaluation, and discussion to ensure that all parties are aware of their responsibilities;

    e. arrangement of the formal acceptance of the evaluation into the Scheme.

Security Target

89. The sponsor is required to provide the Security Target (as described in chapter I).

Deliverables

90. Evaluation deliverables, required in accordance with the assurance level of the criteria, and needed by the evaluators for the successful conduct of an evaluation, may comprise:

    a. items of hardware, firmware or software which constitute the TOE itself;

    b. guidance documentation provided for the user of the TOE;

    c. supporting technical documentation, generated either during the development of the TOE or to support the evaluation process;

    d. access to the operational site (in the case of a system);

    e. access to the development site;

    f. technical support from the developer.

    The process of evaluation can be eased if the TOE is developed with the required evaluation deliverables in mind. This is particularly relevant at higher assurance levels.

91. As part of their preparation for evaluation the Sponsor should ensure that they are able to arrange the supply of evaluation deliverables in a timely manner. The Sponsor should note however that this may require the co-operation of other parties. In particular many deliverables may be the property of the Developer of the TOE and may not be automatically available to the Sponsor.

92. The Developer may wish to limit the Sponsor's access to proprietary information. The CLEF and CB will however need sufficient access to proprietary information to perform their evaluation and certification activities. In so doing they will need to ensure that the integrity of the evaluation is not compromised, that is to say that the Developer is not able to inhibit the accurate and fair reporting of the findings of the evaluation.

93. The full set of deliverables required should be agreed between the Sponsor, CLEF and any other interested parties subject to the requirement that the set of deliverables is sufficient for the set of evaluation criteria to be satisfied. The CLEF may find it helpful to prepare a Deliverables List to identify the deliverables required and the time at which they are required.

Evaluation Work Programme (and Task Initiation Notice)

94. The Evaluation Work Programme (EWP), which is prepared by the CLEF and agreed by the CB, outlines the work to be undertaken by the CLEF during the evaluation. It gives opportunity to address any issues regarding the application of the criteria and methodology to the specific TOE, and to present management information such as the proposed evaluation timescales.

95. The CLEF selected to perform the evaluation notifies the CB by means of a Task Initiation Notice (TIN) that an evaluation is to be performed and in so doing requests that the evaluation is formally accepted into the Scheme. The TIN and EWP may be combined into a single document.

Task Startup Meeting

96. The CLEF usually arranges a Task Start-up Meeting (TSM), also involving the Sponsor, CB and any other interested parties, to discuss any issues relating to the evaluation and certification process and the specific TOE prior to the completion of the preparation phase. The TSM is optional for certain types of shorter evaluation, including CC EAL1 evaluations.

97. The timing of a TSM will normally be arranged to meet the requirements of the Sponsor; however it is typically held after the CB's consideration of the Security Target and EWP.

Formal Acceptance of Evaluation

98. As part of its preparation phase activities the CB checks that the Security Target is fit for purpose, agrees the EWP and attends the TSM (where a TSM is held).

99. The evaluation will be formally accepted if the CB is satisfied that the TOE will be certifiable in principle under the Scheme, a contract is in place between the Sponsor and the CB for the CB's preparation phase activities and the Sponsor has agreed to pay the CB's charges for those activities.

Advice and Consultancy

100. The CLEF chosen to conduct the evaluation will wish to first assist the Sponsor by helping them to assess the likelihood of a successful certification. For example the CLEF might perform an initial review of the Security Target and the availability of the necessary deliverables.

101. The Sponsor also has the option of engaging a security consultant, which may be a CLEF, to assist with the preparation phase activities. For example the Sponsor might contract a consultant to prepare the Security Target.

102. The scope of any such advice or consultancy during the preparation for evaluation is a matter for negotiation between the Sponsor and the CLEF or any other consultant. However, where a CLEF provides both consultancy and evaluation services for a particular TOE, it is obliged to define the scope of the consultancy to ensure that the advice given does not affect evaluator independence or impartiality in the evaluation, and to demonstrate this to the satisfaction of the CB.

103. On becoming aware of the Sponsor's interest in certification the CB will ask the Sponsor to complete a short questionnaire. The answers provide the CB with an initial awareness of the nature of the TOE, sufficient for quoting for its preparation phase services.

104. If the evaluation Sponsor wishes, the CB can arrange an informal meeting with the Sponsor to explain what is involved in an evaluation before contracts are entered into. This may be particularly useful if the Sponsor has any questions regarding whether the TOE would be certifiable in principle.

IV. EVALUATION AND CERTIFICATION

Introduction

105. This Chapter provides an overview of the second phase in the process of evaluation and certification. A diagrammatic overview of the evaluation and certification activities is provided in Annex C (Part C2). More detailed guidance for the Sponsor and Developer is provided in UKSP 04 Part I [i].

Objective

106. The objective of the evaluation and certification phase is to determine whether the TOE meets its Security Target and is free from exploitable vulnerabilities. This involves the following activity:

a. evaluation of the TOE;

b. interaction between the various parties to ensure effective operation of the evaluation process;

c. production by the CLEF of the Evaluation Technical Report;

d. production by the CB of the Certification Report (CR).

Evaluation Work

107. The evaluators perform the technical work as defined in the Evaluation Work Programme (EWP). Evaluation involves the impartial and detailed assessment of the TOE against defined evaluation criteria, with the objective of determining how well it upholds the Security Target and identifying any exploitable vulnerabilities.

108. If, in the course of performing the evaluation work, errors or vulnerabilities are discovered, observation reports shall be raised. The results of the evaluation are documented as the evaluation proceeds.

Interaction

109. The CLEF will normally hold regular Evaluation Progress Meetings (EPMs) with the Sponsor and other interested parties. These are management meetings which allow the progress of the evaluation and any issues raised by it to be addressed.

110. During the course of an evaluation, the CLEF often needs to interact directly with the Developer (who may or may not also be the Sponsor), but will seek the agreement of the Sponsor before doing so.

111. The CB monitors every evaluation, to confirm that it is conducted according to the criteria, methods and procedures required by the Scheme. At this stage the CB is involved in the following activities:

a. attending the EPMs;

b. agreeing with the CLEF the manner in which the criteria and methodology should be applied to the specific TOE, where necessary;

c. reviewing technical reports produced by the evaluators during the course of the evaluation;

d. reviewing any observation reports generated by the evaluators to record problems found in the TOE;

e. reviewing evaluation deliverables, where appropriate;

f. witnessing the development environment assessment, where appropriate;

g. witnessing evaluator testing, where appropriate;

h. making arrangements for inclusion of the TOE's entry in the Certified Products List (UKSP 06) [n], where desired.

112. The CLEF will inform the Sponsor of any problems found in the TOE at the same time that it informs the CB. The CB and CLEF will discuss such problems with the Sponsor and / or Developer as appropriate to ensure resolution at an early stage. If it is not possible to resolve a problem, and the CB decides that certification will be affected, the CB will formally contact the Sponsor and inform them of the impact. The Sponsor may then (subject to their contract with the CLEF):

a. abandon the evaluation;

b. continue the evaluation while accepting the problem and its implications for certification;

c. reschedule the evaluation and, in consultation with the CB, instruct the Developer to modify the TOE in an agreed way.

Evaluation Technical Report

113. The evaluators document their findings in an ETR, which represents the final output from the CLEF evaluation. The conclusions documented in the ETR state the degree to which the evaluation criteria and security functionality have or have not been met, with supporting evidence. The presentation and contents of the ETR are in accordance with the requirements of the evaluation methodology.

114. The CLEF releases the ETR to the Sponsor after sanitising it by removing any material proprietary to the CB, CLEF or Developer, and notifies the Sponsor of the status of the CB review. Release of the ETR to the Sponsor is usually delayed until it has been reviewed by the CB (prior to production of the Certification Report – see below); however the CLEF may release the ETR to the Sponsor at an earlier time on the understanding that its contents represent the views and judgements of the CLEF alone.

115. The Sponsor may make representations to the CLEF and CB concerning any statements in the ETR which the Sponsor believes to be misleading, unjustified or inaccurate.

116. The sanitised ETR is released to the Sponsor in confidence and without prejudice to the Certification Report:

a. The ETR is marked "Evaluation in Confidence" and is released to the Sponsor on the understanding that it will be restricted to a limited circle of the Sponsor's staff and will not be distributed to other parties without the agreement of the CB.

b. The final evaluation results are implicitly accepted by the CB, and the evaluation completed, upon the agreement of the Certification Report by all of its reviewers (ie the CB, the CLEF and the Sponsor).

Certification Report

117. The CLEF releases the ETR to the CB, to enable the CB to formally document the findings of the evaluation in the Certification Report.

118. The CB first reviews the ETR to confirm that it provides a suitable basis for the certification report. The CB may contact the CLEF to make reasonable requests for access to specific technical evidence and results to support any conclusions presented in the ETR.

119. The purpose of the Certification Report is to:

a. provide a statement of how well the TOE conforms to its Security Target;

b. confirm the assurance level;

c. identify any exploitable vulnerabilities in the TOE (the Certification Report may recommend measures to prevent the security of the installed TOE being breached);

d. confirm that the evaluation has been conducted in accordance with the provisions of the Scheme and that the conclusions drawn from the evaluation are consistent with the facts presented.

120. The draft Certification Report is issued to the Sponsor and the CLEF for confirmation that:

a. the report fairly represents the Security Target;

b. the report fairly represents the conduct and outcome of the evaluation;

c. the conclusions of the report are accurate;

d. the Sponsor and CLEF are not aware of any factors which could invalidate the report.

121. Once the Certification Report has been finalised, both the Certificate and Certification Report are signed by the CB to indicate its acceptance of the above. Where the TOE is included in UKSP 06 [n], its certification will be confirmed in the next update.

122. Copyright of Certificates and Certification Reports remains the property of the CB. Their reproduction and distribution by the Sponsor is authorised provided the report is copied in its entirety.

Maintenance of Certificates

123. Procedures for the maintenance of Certificates (e.g. their extension to later releases or versions of the TOE) are described in the following chapter.

(This page is intentionally left blank)

V. CERTIFICATE MAINTENANCE

Introduction

124. This Chapter briefly describes the UK Certificate Maintenance Scheme (CMS). A diagrammatic overview of CMS activities is provided in Annex C (Parts C3 and C4). UKSP 16 Part I [q] provides a full description of the CMS.

125. The certificate awarded after a first evaluation is only valid for a specific version of a TOE. However, most TOEs are subject to changes which are outside the scope of this certificate (e.g. resulting from security-relevant patches to products). The CMS provides a means of establishing confidence that the assurance in a TOE is maintained without always requiring a formal re-evaluation. Under this scheme the Sponsor is therefore able to maintain their TOE without incurring the costs associated with re-evaluating each change and at the same time minimise the cost of future re-evaluation.

126. For a TOE entered into CMS, versions produced during the certificate maintenance phase that have not been subject to formal re-evaluation are given CMS approved status. However, the CB confirms that an end user can have equal confidence in a CMS approved version of the TOE as in the original certified version, and CMS approved versions of products are recognised in UKSP 06 [n].

127. Membership of CMS is optional, and if a TOE not entered is modified, it can still be re-evaluated. However recognition will then only be given to the evaluated versions. The evaluation approach will be similar to that of an initial evaluation. However a clear identification of modifications made will enable efficiency through focus on the changes and their impact on security.

Gaining Membership of the CMS

128. A Sponsor can apply for a TOE to gain full membership of the CMS if there has been, or is ongoing, an evaluation of the TOE under the Scheme. A completed evaluation must have successfully resulted in the award of a certificate.

129. Formal application is signified by submission of a Certificate Maintenance Plan (CMP) to a CLEF for review (normally the CLEF who evaluated the TOE). The Sponsor must also appoint a Developer Security Analyst (DSA) who has prime responsibility for ensuring that the assurance of the TOE is maintained whilst the TOE is under the CMS.

130. If a DSA has not been appointed during the initial evaluation and certification, then the CMP must take into account the possible impact of changes made to the certified TOE during the period between certification and the appointment of a DSA. If significant changes have been made to the TOE, the CB may require a CMS re-evaluation earlier than may otherwise have been necessary. Alternatively, the CB may rule that the CMP can only be approved once evidence has been provided that the assurance of the TOE has been maintained.

131. Thus, full membership of the CMS is granted once the following conditions have been met:

a. the TOE has been certified;

b. the CMP has been approved by the CB;

c. a DSA has been appointed for the TOE.

132. A TOE will retain full membership of the CMS provided that the CMP, and the requirements of the CMS, are followed. In some cases deviation from the CMP may be permitted, but only with the agreement of the CB.

The Certificate Maintenance Plan

133. The CMS requires a commitment from the Sponsor to maintain the certified status of products and systems, in the form of the CMP.

134. The CMP justifies why the proposed CMS re-evaluation schedule is appropriate (i.e. why it is not necessary or appropriate to submit any interim releases for CMS re-evaluation). The period between evaluations, which will not normally be more than three years, will reflect the level of updates expected to the TOE. For example, TOEs that are subject to frequent changes (i.e. several releases a year) should be subject to annual CMS re-evaluations, whereas TOEs that defend against a static threat and which are expected to change infrequently may be subject to a CMS re-evaluation every three years.

135. The Sponsor is required to provide an annual Certificate Maintenance Status Report (CMSR), reporting progress against the CMP. The CMSR thus provides a means by which the continued validity of the CMP can be checked. In particular, it includes a report on the changes relevant to security and the vulnerabilities discovered in the TOE over the period.

CLEF, Sponsor and Developer Activities under the CMS

136. The Sponsor is required to provide evidence to the selected CLEF demonstrating that the assurance of the TOE is being maintained. As well as the CMP and annual CMSRs, the main input deliverable is the Security Impact Analysis (SIA). The SIA must describe each change affecting the TOE, and provide a justification as to why the assurance that the TOE meets its Security Target has been maintained. The justifications in respect of changes to the TOE implementation must always be supported by security test evidence.

137. The development site is visited by the CLEF and (optionally) the CB in accordance with a schedule laid down in the CMP. The first of these visits, or Certificate Maintenance Audits ("CM Audits"), for a TOE will take place no more than six months after approval of the CMP or certification of the TOE, whichever is the later. Thereafter, CM Audits will occur annually (unless the CMP states otherwise) until the next CMS re-evaluation of the TOE. The CM Audits are undertaken to establish confidence that the DSA is following the CMP and the requirements of the CMS. Part of this work involves checks on the SIA and CMSR by the CLEF. The CLEF reports the results of the CM Audit in a CM Audit Report (CMAR). Whilst the CB may not necessarily attend the CM Audits, it will monitor the CM Audits and review the CMAR.

138. Any new version of the TOE produced whilst the TOE has full membership of the CMS is automatically designated as "CMS Approved" subject to the following:

a. the Security Impact Analysis shows that the changes are within the scope of CMS Approval;

b. there are no outstanding non-compliancies with the CMS or CMP.

139. This means that if the above conditions are met, there is no requirement for a formal evaluation or CMS re-evaluation, beyond that planned in the CMP, in recognition that the assurance of the TOE has been maintained.

140. A CMS re-evaluation addresses the changes to the TOE and/or its security target since the most recent evaluation of the TOE. The SIA is the principal input to a CMS re-evaluation; the evaluators independently check the validity of the analysis, and perform penetration testing where necessary. The evaluation effort is directed at changes which have a critical impact on the security of the TOE, guided by the SIA. In this way, the cost and timescales of CMS re-evaluations are significantly reduced, compared with non-CMS re-evaluations.

Roles and Responsibilities under the CMS

141. The Sponsor or Developer is obliged to appoint a DSA who is familiar with the TOE, the evaluation results, the evaluation criteria, the evaluation methodology, relevant UKSPs, and the CMS. The DSA should seek training if necessary to compensate for any lack of experience in any particular area. Subject to these requirements, the DSA role may be assumed by a CLEF or an independent security consultant. If the DSA is contracted from a CLEF, then it is necessary for the CM Audits to be carried out by a different CLEF or directly by the CB, in order to preserve independence.

142. The Sponsor has considerable flexibility in its use of CLEFs for the original evaluation, the CM Audits and the CMS re-evaluations. Each activity can be performed by a different CLEF, or the same CLEF, or any combination thereof, subject to the exception stated in paragraph 141 above. In the event of a Sponsor deciding to contract a new CLEF to perform the CMS re-evaluation and CM Audits, the Sponsor should arrange for transmission of deliverables to the new CLEF.

143. As in the case of the original evaluation, a CLEF providing consultancy to Sponsors and Developers involved in the CMS is obliged to ensure that its independence is not compromised if the CLEF is also contracted to carry out the review, audit and re-evaluation activities under the CMS.

144. Useful guidance to Sponsors and Accreditors is provided in UKSP 16 Part I [q], Annex B. Guidance to DSAs is provided in UKSP 16 Part II [r] and training material is provided in UKSP 16 Part III [s].

(This page is intentionally left blank)

Annex A. GLOSSARY AND TERMINOLOGY

The following terms have special meaning within the context of the Scheme.

Accreditation:

has two definitions according to circumstances:

a. the procedure for accepting an IT system for use within a particular environment (system accreditation);

b. the procedure for recognising both the technical competence and the impartiality of a test laboratory to carry out its associated tasks (laboratory accreditation).

Certificate / Certification Report (CR):

the document issued (usually publicly) by a CB as a formal statement confirming the results of the evaluation and that the evaluation criteria were correctly applied; the CR includes appropriate details about the TOE and the evaluation.

Certification:

the issue of a formal statement confirming the results of an evaluation and that the evaluation criteria were correctly applied.

Certification Body (CB):

an independent and impartial organisation that performs certification.

CommerciaL Evaluation Facility (CLEF):

an organisation accredited in accordance with agreed standards (e.g. EN 45001 and ISO Guide 25) and appointed by the CB to perform security evaluations (previously referred to as a Commercial Licensed Evaluation Facility); this is the Scheme equivalent of an IT Security Evaluation Facility (ITSEF).

Deliverable:

A document, item or resource (often produced or used during development of a TOE) that is required to be made available to the evaluators for the purpose of evaluation.

Deliverables List:

a document which may be produced by a CLEF to define the deliverables needed to meet the work specified in the EWP.

Developer:

the person or organisation that manufactures a Target of Evaluation.

Evaluation:

the assessment of an IT system or product against defined evaluation criteria.

Evaluation Technical Report (ETR):

a report produced by a CLEF and submitted to the CB detailing the findings of an evaluation and forming the basis of the certification of a TOE.

Evaluation Work Programme (EWP):

a document produced by a CLEF and submitted to the CB providing a description of the work planned for an evaluation.

Product:

a package of IT software and / or hardware, providing functionality designed for use or incorporation within another product or a multiplicity of systems.

Security Target:

a specification of the security required of a Target of Evaluation (TOE), used as a baseline for evaluation. The Security Target will specify the assurance requirement for the evaluation, the security objectives and security functions of the TOE, and optionally specific security mechanisms employed by the TOE.

Sponsor:

the person or organisation that requests an evaluation.

System:

a specific IT installation, with a particular purpose and operational environment.

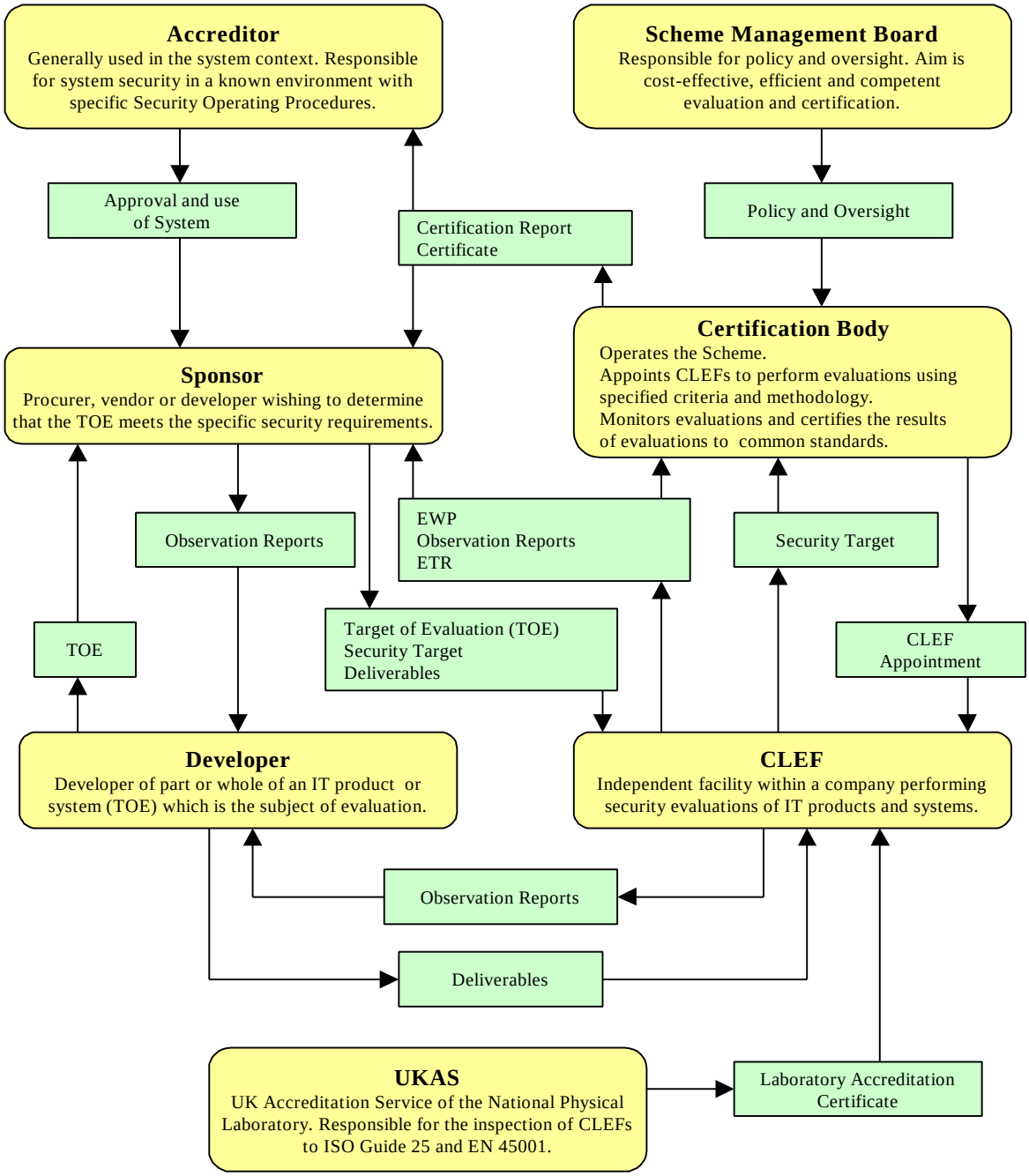
Target of Evaluation (TOE):

an IT system or product which is subjected to security evaluation.

Task:

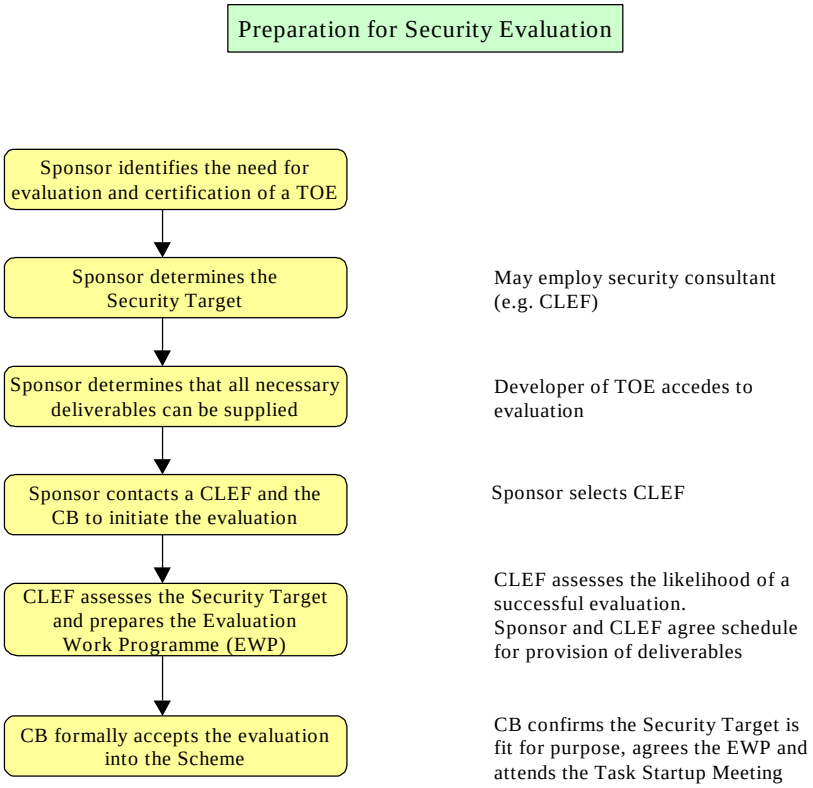
corresponds to the evaluation work performed by a CLEF on a single TOE.

Annex B. ORGANISATION AND MANAGEMENT CONTEXT DIAGRAM

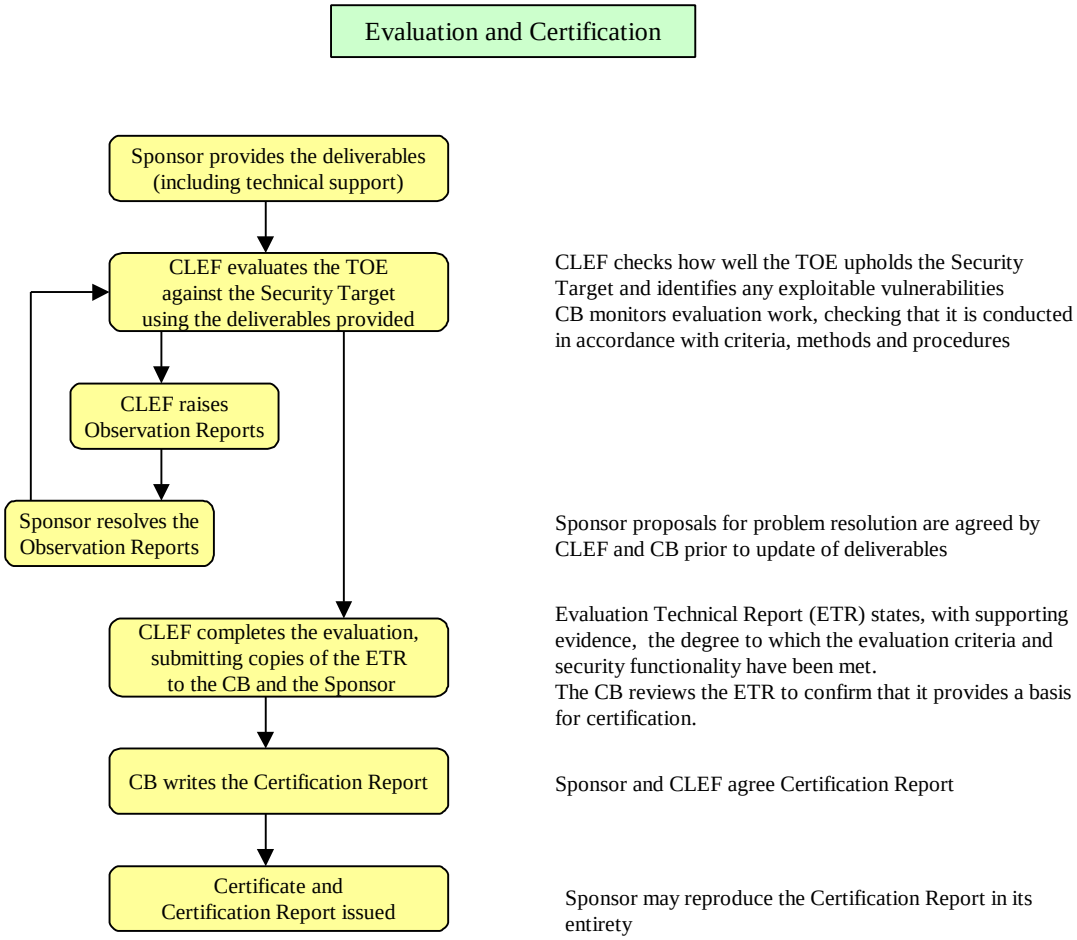


(This page is intentionally left blank)

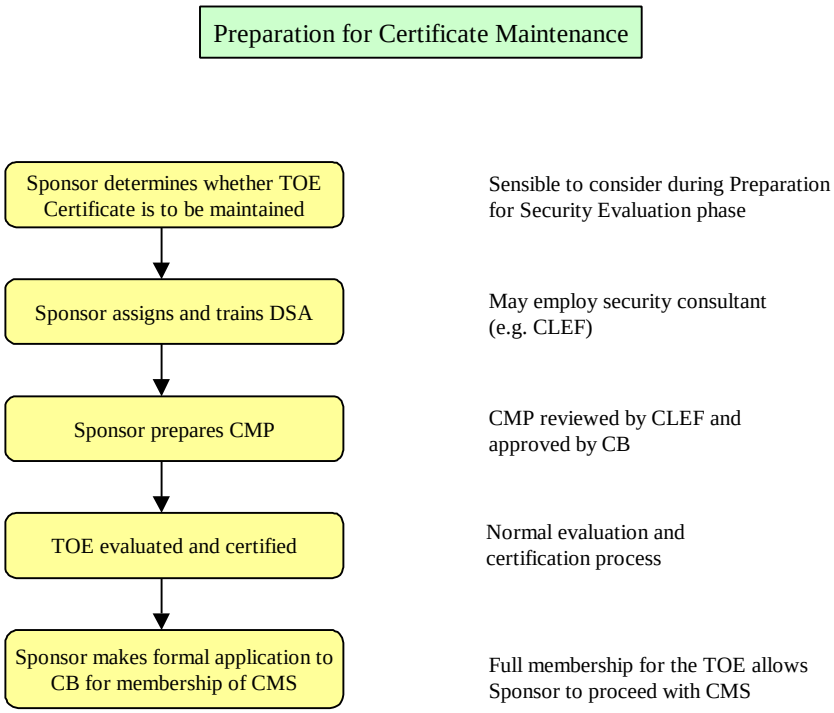
Annex C. SECURITY EVALUATION AND CERTIFICATION ACTIVITIES



(This page is intentionally left blank)

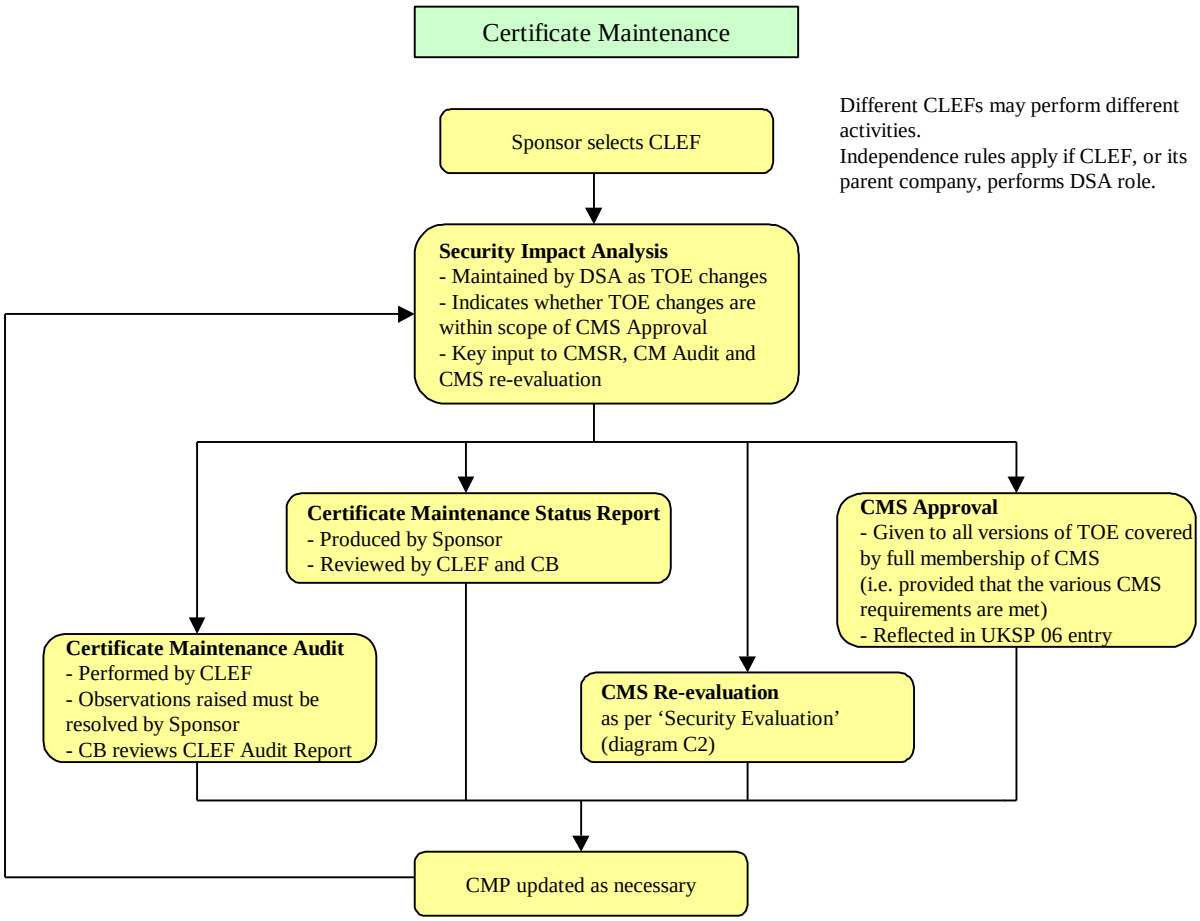

Evaluation and Certification
Sponsor provides the deliverables (including technical support)
CLEF evaluates the TOE against the Security Target using the deliverables provided
CLEF raises Observation Reports
Sponsor resolves the Observation Reports
CLEF completes the evaluation, submitting copies of the ETR to the CB and the Sponsor
CB writes the Certification Report
Certificate and Certification Report issued
CLEF checks how well the TOE upholds the Security Target and identifies any exploitable vulnerabilities
CB monitors evaluation work, checking that it is conducted in accordance with criteria, methods and procedures
Sponsor proposals for problem resolution are agreed by CLEF and CB prior to update of deliverables
Evaluation Technical Report (ETR) states, with supporting evidence, the degree to which the evaluation criteria and security functionality have been met.
The CB reviews the ETR to confirm that it provides a basis for certification.
Sponsor and CLEF agree Certification Report
Sponsor may reproduce the Certification Report in its entirety

(This page is intentionally left blank)


Preparation for Certificate Maintenance
Sponsor determines whether TOE Certificate is to be maintained
Sponsor assigns and trains DSA
Sponsor prepares CMP
TOE evaluated and certified
Sponsor makes formal application to CB for membership of CMS
Sensible to consider during Preparation for Security Evaluation phase
May employ security consultant (e.g. CLEF)
CMP reviewed by CLEF and approved by CB
Normal evaluation and certification process
Full membership for the TOE allows Sponsor to proceed with CMS

(This page is intentionally left blank)

Annex C (C4) of UKSP 01



(This page is intentionally left blank)