UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No 12

RELATIONSHIP BETWEEN
ACCREDITATION DOCUMENT SET
AND
SECURITY TARGETS FOR EVALUATION

Issue 1.0
July 1999

This document must not be copied or distributed further by the recipient without the prior written approval of the Senior Executive of the UK IT Security Evaluation and Certification Scheme.

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 relates HMG Infosec Standard No 2 to the UK IT Security Evaluation and Certification Scheme. It is intended to offer information to accreditors and others with an interest in the evaluation of HMG IT systems. Particular focus is given to the relationship between the Accreditation Document Set and the Security Target required for evaluation.

P. M. Seeviour
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
1.0	First Issue	July 1999

TABLE OF CONTENTS

FIGURES

REFERENCES

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

also issued as HMG Infosec Standard No 2: Accreditation Documents, CESG Publications Department [1]

[b] Manual of Protective Security (MPS), Cabinet Office Security Division [2]

[c] 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 [1]

[d] CESG Infosec Memorandum No 19: Accreditation Documents – A Companion Guide to HMG Infosec Standard No 2, CESG Publications Department [1]

[e] CESG Guide to Accreditation, CESG Publications Department [1,3]

[f] Information Technology Security Evaluation Criteria, Commission of the European Communities, CD-71-91-502-EN-C, Version 1.2, June 1991 [4]

[g] ITSEC Joint Interpretation Library (ITSEC JIL), Joint Interpretation Working Group [4]

[h] Information Technology Security Evaluation Manual, Commission of the European Communities, Version 1.0, 10 September 1993 [4]

[i] Common Criteria for Information Technology Security Evaluation, Common Criteria Implementation Board [4]

[j] Common Methodology for Information Technology Security Evaluation, Common Evaluation Methodology Editorial Board [3,4]

[k] UK Scheme Publication No 6 - Certified Product List, UK IT Security Evaluation & Certification Scheme [4]

[1] General correspondence concerning references [a], [c], [d] and [e], including requests for copies, should be addressed to:

Communications-Electronics Security Group (X53A1)
Government Communication Headquarters
PO Box 144
Cheltenham
Glos GL52 5UF

Telephone: 01242 221491 Ext. 4577
Facsimile: 01242 261402

Technical correspondence concerning these references should be addressed to (X7A) at the above address.

[2] MPS [b] is a protectively marked document. Correspondence relating to this reference, including requests for copies, should thus be made to the appropriate Departmental Security Officer.

[3] Note that, at the date of publication of this issue of UKSP 12, formal release of references [e], [j] and [m] was still awaited.

[4] General correspondence concerning references [f], [g], [h], [i], [j], [k], [l] and [n], including requests for copies, should be addressed to the UK IT Security Evaluation & Certification Scheme Certification Body. Contact details are given on the 'FOREWORD' page of this document.

[l] UK Scheme Publication No 4 - Developers' Guide, UK IT Security Evaluation & Certification Scheme [4]

[m] PP and ST Guide, International Standards Organisation [3]

[n] UK Scheme Publication No. 16 - UK Certificate Maintenance Scheme, UK IT Security Evaluation & Certification Scheme [4]

ABBREVIATIONS

ADS	Accreditation Document Set
CB	Certification Body
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CMP	Certificate Maintenance Plan
CMS	Certificate Maintenance Scheme
COTS	Commercial Off The Shelf
CR	Certification Report
DSA	Developer Security Analyst
ETR	Evaluation Technical Report
HMG	Her Majesty's Government
ITSEC	Information Technology Security Evaluation Criteria
ITSEC	IT Security Evaluation and Certification
ITSEM	Information Technology Security Evaluation Manual
MPS	Manual of Protective Security
PP	Protection Profile
SEF	Security Enforcing Function
SOG-IS	Senior Officials Group for Information Security
SOPs	Security Operating Procedures
ST	Security Target
SyOPs	Security Operating Procedures
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication

I. Introduction

Objective

1. This document has been produced to accompany the newly published HMG Infosec Standard No 2 [a] (superseding CESG Infosec Memorandum No. 5), and relates it to the UK IT Security Evaluation and Certification (ITSEC) scheme to assist those considering evaluation. This document offers:

- An overview of the evaluation and certification processes for IT systems and their relationship to the accreditation process (see the ‘Process Overview’ section),
- An outline of the Security Target (ST) and other documentation required to support evaluation and certification within the UK, to either the IT Security Evaluation Criteria (ITSEC) or Common Criteria (CC), and its relationship to the Accreditation Document Set (ADS) (see the ‘Evaluation Documentation’ section)
- An overview of the assurance maintenance process, and an outline of the associated documentation and its relationship to the ADS (see the ‘Assurance Maintenance’ Section)
- References to sources of further information (see the ‘Related Documentation’ section)

Status

2. This is a new document, which does not replace any existing HMG publication. It is offered for information.

(This page is intentionally left blank)

II. Related Documentation

Scheme Documentation

3. A set of documentation which provides guidance on the UK ITSEC Scheme is available on the Scheme's web site at address: http://www.ITSEC.gov.uk. This guidance consists of the following types of material:
   - Introductory guides
   - Formal documentation
   - Certification Reports (CRs) and STs
4. The introductory guides exist to provide an overview of the ITSEC Scheme.
5. The formal documentation guides interested parties through both management and technical issues involved in the ITSEC Scheme.

Other Relevant Documentation

Manual of Protective Security

6. The Manual of Protective Security (MPS) [b] is the definitive source of information regarding national minimum standards and recommended procedures for the protection of HMG assets.

HMG Infosec Standard No 1

7. HMG Infosec Standard No 1 [c] 'Assurance Requirements for IT Systems' [5] is part of the MPS and is also published separately. It sets out the mandatory standard for performing a risk assessment for the technical security barriers within a system. The result of the risk assessment may give a value between ITSEC E1 and E6 (or CC EAL1 to EAL7). At these levels the Accreditor should consider evaluation under the ITSEC Scheme in order to provide assurance that the security barriers are effective and implemented correctly.
8. A risk assessment performed against HMG Infosec Standard No 1 [c] should be included in Part 2 of the system ADS.

HMG Infosec Standard No 2

9. HMG Infosec Standard No 2 [a] 'Accreditation Documents' is part of the MPS and is also published separately. It sets out a recommended format for compiling an ADS. It recommends a portfolio structure for an ADS, on the assumption that the accreditor is likely to need the entire document set, whereas individual items within it are likely to be of interest to others as well. Where individual components of an ADS are already published, the ADS need only include a reference rather than reproduce the document itself. The overall structure recommended is as follows:

- Part 1: Basic Information, including the scope of the accreditation (and thus of the ADS), a description of the resources covered, and a list of the personnel involved.
- Part 2: Risk management documents, including technical risk calculations as mandated in [c].
- Part 3: Security Operating Procedures (SyOPs or SOPs) and Interconnection Security Measures, giving instructions on how technical, procedural and other counter-measures are to be put into practice.
- Part 4: Inspection reports and the formal accreditation certificate.

[5] HMG Infosec Standard No 1 is sometimes referred to as ARFITS; however this is not part of the official document title.

Companion Guide to HMG Infosec Standard No 2

10. The companion ‘CESG Infosec Memorandum No 19: Accreditation Documents - A Companion Guide to HMG Infosec Standard No 2’ [d] gives further guidance about writing an ADS. It covers in particular the documentation of more complex accreditations, including those where a bespoke risk assessment and management exercise is needed.

CESG Guide to Accreditation

11. The guide ‘CESG Guide to Accreditation’ [e] defines accreditation and summarises the business justification, relating these to the production of an ADS. Under certain circumstances (e.g. the holding or processing of protectively marked material, or a proposed connection to the Government Secure Intranet) accreditation is mandatory.

ITSEC

12. The ITSEC [f] is the harmonised criteria set, produced by Germany, France, the Netherlands and the UK against which security evaluations can be performed.
13. The ITSEC is supported by the ITSEC Joint Interpretation Library [g] and IT Security Evaluation Manual [h], also produced by these nations.

Common Criteria

14. The Common Criteria for Information Technology Security Evaluation [i], adopted by International Standards Organisation as ISO15408, represents the outcome of an initiative to align existing European and North American criteria.
15. The CC is soon to be supported by the Common Evaluation Methodology (CEM) [j], as part of the same initiative.

Mutual Recognition Arrangements

16. Where a system requiring certification relies on Commercial Off The Shelf (COTS) products to provide security functionality, it is advisable to select those products from the evaluated products list [k]. Previous evaluation results should be reused where possible to decrease time and duration of an evaluation. It should be noted that the evaluated products list includes details of products certified under both the UK and other national IT security evaluation schemes, any of which may be of interest to the systems integrator.
17. The Senior Officials Group for Information Security (SOG-IS) of the European Commission approved the Mutual Recognition Agreement of Information Technology Evaluation Certificates based on ITSEC. The agreement came into force in March 1998. A list of countries subscribing to this agreement can be found in the evaluated products list [k].
18. A mutual recognition arrangement, dated October 1998, exists for countries performing evaluations to the CC. The scope of this arrangement can be found in the evaluated products list [k].
19. In both the SOG-IS Mutual Recognition Agreement and the CC Mutual Recognition Arrangement there is a clause which states that where national security is at stake, certificates issued by other countries will not necessarily be recognised. HMG Departments are advised to consult CESG when wishing to use products certified in other countries.

(This page is intentionally left blank)

III. Process Overview

Interested Parties

20. The following will be directly involved with the evaluation of a system under the ITSEC Scheme:

- Accreditor;
- Commercial Evaluation Facility (CLEF);
- UK Certification Body (CB);
- Developer;
- Evaluation Sponsor.

Accreditor

21. The Accreditor, supported by a CESG advisor and by the certifier, is responsible for ensuring that the system is suitable for use in the intended environment with the intended security operating procedures.

CLEF - Evaluation Team

22. Evaluations are carried out by independent third parties known as Commercial Evaluation Facilities or CLEFs, appointed by the CB of the Scheme. These CLEFs meet rigorous security and quality standards. Contact details of the CLEFs can be found on the ITSEC Scheme web page and in the evaluated products list [k]. A CLEF is subcontracted by the Sponsor of the evaluation.

UK Certification Body - Certifier

23. The CB exists to monitor the evaluation process performed by the evaluation facilities. It examines the results and, if appropriate, issues a Certification Report (CR) and certificate. It appoints one of its certifiers to act as its primary point of contact for each evaluation.

24. The CB provides technical advice and guidance on the conduct of the Scheme and verifies that evaluation techniques are applied consistently across the evaluation facilities, thus ensuring repeatability and reproducibility of evaluation results, a primary aim of the Scheme.

25. The CB maintains the Scheme documents and provides technical interpretations to the CLEFs.

26. The CR produced by the CB is a primary input to the accreditation process for a system submitted for evaluation.

27. Certification bodies in other countries which are recognised by the UK CB are of interest in respect of products they have certified. A current list of such products can be found in the latest copy of the evaluated products list [k] available on the Scheme's web site.

Developer

28. The developer is responsible for putting together the system to the required specification. The developer is also responsible for providing the evaluation deliverables and for providing technical support to the evaluators.

Evaluation Sponsor

29. The evaluation sponsor is not necessarily the main project sponsor. It is the evaluation sponsor's responsibility to:

- Subcontract the CLEF and fund the evaluation;
- (Optionally) Attend Evaluation Progress Meetings;
- Subcontract the CB and fund certification;
- Chair the Security Working Group;
- Liaise with the accreditor;
- Represent the project sponsor in respect of the security requirement and agreement of a security solution.

30. The processes that each of these players are involved in are outlined in the following three sections.

Accreditation Process

31. All HMG Departments and Agencies are responsible for protecting their information resources. The process of accreditation is a key element in the discharging of this responsibility, and in certain circumstances it is mandatory.

32. As a result of performing the risk assessment required for Part 2 of the ADS the Accreditor may decide that the technical risks are such that it is appropriate to obtain additional assurance in the desired system configuration before determining whether to accredit it. Two options are then available:

- An approved IT Security Health Check;
- Evaluation and subsequent Certification under the ITSEC Scheme.

33. The health check is only applicable as an alternative where the assurance level calculation produced against HMG Infosec Standard No 1 [c] is EAL1 (for the barrier in question), and is not considered further here. This document exists to relate accreditation and the guidance presented in References [c] and [a] to the ITSEC Scheme.

34. Advice and guidance should initially be sought from the system's assigned CESG advisor and the CB. Details of other relevant contacts are provided by the scheme's web site.

Certification Process

35. Certification is essentially a two phase process and generally does not begin until after a Sponsor has placed a contract with a CLEF.

36. The first phase of the process begins with the Sponsor completing a questionnaire, a copy of which can be obtained from the CB. This questionnaire enables the CB to scope the evaluation, ensure that the ST and system are suitable for evaluation and assign a Certifier to oversee the conduct of the evaluation.

37. Should the system be deemed suitable for evaluation, the second phase will begin. This is the oversight of the evaluation proper and culminates with the review of the evaluation results and the production of the CR and certificate, where appropriate. The assigned Certifier will have a high level of contact with the evaluators throughout this process, attending evaluation progress meetings and making on site visits to oversee testing.

38. The sponsor is required to place a separate contract with the CB for each of these two phases.

39. Specific considerations may apply in respect of cryptographic mechanisms. These are outlined in UKSP 04 [l] Part III, and it is advisable to consult the CB to confirm the approach to be taken.

The Evaluation Process

Evaluation Phases

40. The activities for the evaluation can be grouped into two phases, preparation and evaluation, which correspond with the above certification phases. These evaluation phases are discussed

in the following sections. The phases and workpackages specific to each criteria are discussed in detail in the ITSEM [h] and the CEM [j].

41. The sponsor is also required to make contractual arrangements with their chosen CLEF.

Preparation

42. The preparation phase is standard for all evaluations in the UK. At the start of an evaluation a CLEF will notify the CB of the interest in evaluation and will draw up a Task Initiation Notice and Evaluation Work Programme.

43. The preparation phase usually includes a meeting, to agree the scope of the evaluation, which is generally held at the CLEF. This meeting is optional for certain types of shorter evaluation, including CC EAL1 evaluations.

Evaluation

44. Based on the assurance requirements in the ADS for the system under evaluation a set of evaluation work packages or activities will be selected. These work packages will increase in rigour depending upon the assurance level claimed. Although the activities associated with a CC evaluation will differ from those under the ITSEC evaluation, they can be grouped into the following areas:
    - Requirements Analysis
    - Development Representations Analysis
    - Development Environment Assessment
    - Operational Assessment
    - Operational Documentation Assessment
    - Vulnerability Analysis
    - Testing

45. Some re-work may be necessary if the first pass of the evaluation phase identifies security problems.

IV. Evaluation Documentation

46. Guidance is provided below, for ITSEC and for CC, on meeting the recommendations of HMG Infosec Standard No 2 [a] in a manner that will ease the evaluation process. Particular attention is given to the ST which has a close relationship with the ADS.

ITSEC Evaluation Documentation

Introduction

47. ITSEC evaluations require a specified set of documents. There is a core set of documentation required for all levels of evaluation, this core set comprising:
    - a Security Target;
    - a Suitability Analysis;
    - a Binding Analysis;
    - a Strength of Mechanisms Analysis;
    - an Ease of Use Analysis;
    - a Construction Vulnerability Analysis;
    - an Operation Vulnerability Analysis;
    - a Configuration List;
    - Architectural Design;
    - Operational Documentation (User and Administrator Documentation);
    - Delivery and Configuration Documentation;
    - Start-up and Operation Documentation.
48. In addition to the core set of documents the following documentation may be required for higher evaluation levels:
    - Security Policy Modelling documentation
    - Detailed Design
    - Implementation Representation
    - Development tools documentation
    - Development Security documentation
49. Also, as the evaluation level increases, the information detail increases and in some areas is required to be of a formal nature. Further information can be found in ITSEC [f] and UKSP 04 [l] Parts II and III.
50. The ADS is related to the ST, Suitability Analysis, system documentation, Evaluation Technical Report (ETR) and Certification Report (CR). ITSEC requirements should thus be considered alongside the recommendations of HMG Infosec Standard No 2 [a]. The remainder of this section focuses on this relationship.

Security Target

51. There are two types of STs: those written for products and those written for systems. Product STs are aimed at specific products that are to be used in various different environments. System STs are aimed specifically at systems within a known environment. The requirements for an ITSEC ST are as follows:
    - a description of the Target of Evaluation (TOE);
    - security objectives that the TOE will met;
    - threats that the TOE has to counter;

- associated physical, personnel or procedural security measures;
- a description of the Security Enforcing Functions (SEFs) of the TOE;
- a target evaluation level (E level) of the TOE;
- a claimed minimum strength of mechanisms (where appropriate);
- information that shows how each security objective is provided by the SEFs;
- information that shows how each SEF helps to counter the threats to the TOE.

52. In addition, the ST can (optionally) identify required security mechanisms (such as password encryption algorithms). Details are provided in ITSEC [f] as to the content required by each of the components of a ST.

53. For ease of evaluation it is recommended that the ITSEC ST be provided as a single document , which can be filed under 'ADS Part 2: Risk Management Documents'. Table IV-1 below identifies the components of an ST which are addressed by HMG Infosec Standard No. 2 [a].

Security Target Requirement	**Correlation with HMG Infosec Standard No 2.**
Description of the TOE	In discussing accreditation scope under 'ADS Part 1: Basic Information' HMG Infosec Standard No. 2 [a] recommends sufficient information for a TOE to be specified for evaluation.
Security Objectives of the TOE	Security Objectives are not addressed by HMG Infosec Standard No 2 [a]. Information about Security Objectives can be found in UKSP 04 [l] Part III.
Threats that the TOE has to counter	HMG Infosec Standard No 2 [a] addresses threats in discussing ADS Part 2. Care should be given to ensure that threats meet the ITSEC [f] requirements as identified in UKSP 04 [l] Part III.
Physical, personnel or procedural security measures	HMG Infosec Standard No 2 [a] addresses countermeasures in discussing ADS Part 2.
Description of SEFs	HMG Infosec Standard No 2 [a] addresses countermeasures in discussing ADS Part 2. See UKSP 04 [l] Part III for guidance on writing SEFs. To ensure ease of evaluation, it is recommended that the author should separate the countermeasures into their separate categories (such as access control, identification & authentication and audit measures).
Target Evaluation Level	The results of the Assurance calculations, through the use of HMG Infosec Standard No 1 [c], will provide a specified assurance level for each component entity within the scope of the Accreditation. These results can be used to specify a target assurance level for the TOE in the ST.

Security Target Requirement	Correlation with HMG Infosec Standard No 2.
Claimed Minimum Strength of Mechanisms	HMG Infosec Standard No 2 [a] does not address a minimum strength of mechanism. Guidance on strength of mechanisms can be found in UKSP 04 [l] Part III. Note the various types of statement which may be made about mechanism strengths.
Justification of suitability of the SEFs meeting the security objectives.	HMG Infosec Standard No 2 [a] does not address this justification. It can be incorporated within the ST as a table (see Suitability Analysis below).
Justification of the suitability of the SEFs to counter the threats.	HMG Infosec Standard No 2 [a] does not address this justification. It can be incorporated within the ST as a table (see Suitability Analysis below).

Table IV-1 Correlation of ITSEC ST Requirements with HMG Infosec Standard No. 2

Suitability Analysis

54. A Suitability Analysis provides a justification that the SEFs provided by the TOE are suitable to counter the threats to the TOE. Although similar to information provided as part of a ST, the suitability analysis contains more detailed information justifying why the SEFs associated with each threat are sufficient for countering the threat. UKSP 04 [l] Part III contains details as to the contents of a Suitability Analysis.

55. As part of the risk assessment process, countermeasures are identified for specific threats to the system identified by the ADS. As a result of this process a level of analysis will be required to justify why a set of IT countermeasures sufficiently mitigates each threat. It is recommended that the Suitability Analysis be filed in ADS Part 2.

System Documentation

56. The operational documentation required for an ITSEC [f] evaluation comprises user documentation and administration documentation. Details of the information they should contain is provided in UKSP 04 [l] Part III. Invariably the Security Operating Procedures (SyOPs or SOPs) for an accreditation, together with the user and administration guides for component products, contain most, if not all, the information required to meet the ITSEC evaluation requirements for operational documentation. The guidance provided in UKSP 04 Part III should be followed to ensure that this set of documentation covers all aspects required for an ITSEC evaluation.

Evaluation and Certification Reports

57. The ETR produced by the CLEF and CR produced by the CB are both forms of ‘inspection reports’ in the sense of HMG Infosec Standard No 2 [a] and it is recommended that they be filed in Part 4 of the ADS.

Common Criteria (CC) Evaluation Documentation

Introduction

58. CC evaluations are similar to ITSEC [f] evaluations in that the documentation requirements increase as assurance requirements rise. A core set of documentation required for all levels of evaluation comprises:

- Security Target;
- Configuration Details;
- Installation, Generation and Start-up procedures;
- Functional Specification;
- Representation Correspondence documentation;
- Administrator Guidance;
- User Guidance.

59. In addition to the core set of documents the following documentation may be required for higher evaluation levels:

- Delivery and Configuration Documentation;
- High Level Design;
- Low Level Design;
- Design Security Internals documentation;
- Implementation Representation;
- Security Policy Modelling documentation;
- Development Security documentation;
- Life Cycle Definition documentation;
- Tools and Techniques documentation;
- Test Documentation;
- Covert Channel Analysis;
- Misuse documentation;
- Strength of TOE security functions;
- Vulnerability Analysis documentation.

60. Further information on all CC evaluation documents can be found in CC [i], CEM [j] and the PP/ST Guide [m].

61. The ADS is related to the ST, the Administrator Guidance and User Guidance, system Evaluation Technical Report (ETR) and Certification Report (CR). ITSEC requirements should thus be considered alongside the recommendations of HMG Infosec Standard No 2 [a]. The remainder of this section focuses on this relationship.

Security Target

62. The CC terminology varies from that used in ITSEC, and the ST required for a CC evaluation has some significant differences to that needed for an ITSEC evaluation.

63. As identified in CC [i], an ST for a CC evaluation must contain the following:

- an introduction that contains specific information;
- a Target of Evaluation (TOE) description;
- details as to the security environment;
- security objectives of the TOE;
- IT security functional requirements of the TOE (usually from Part 2 of CC [i]);

- a TOE summary specification (primarily giving a TOE-specific elaboration of the IT security functional requirements);
- a target assurance requirement (usually in the form of an evaluation assurance level) of the TOE;
- strength of function claims (where appropriate);
- rationale to demonstrate consistency of the various ST components.

64. In addition, an ST may have:

- Explicitly stated IT security functional requirements (at a similar level of abstraction to, but not taken from, those of Part 2 of CC [i]).

65. Some ST components may be specified in the form of one or more Protection Profile (PP) conformance claims. PPs are implementation-independent sets of security requirements for a category of TOEs that meet specific consumer needs.

66. Details are provided in CC [i] and the PP/ST Guide [m] as to the content required by each of these components of an ST or ease of evaluation it is recommended that the CC ST be provided as a single document , which can be filed under ‘ADS Part 2: Risk Management Documents’. Table IV-2 below identifies the components of an ST which are addressed by HMG Infosec Standard No 2 [a].

Security Target Requirement	**Correlation with HMG Infosec Standard No 2**
ST introduction	In discussing accreditation scope under ‘ADS Part 1: Basic Information’ HMG Infosec Standard No 2 [a] recommends part of the information required. Further guidance on the information required can be found in CC [i] and the PP/ST Guide [m].
TOE description	In discussing accreditation scope under ‘ADS Part 1: Basic Information’ HMG Infosec Standard No 2 [a] recommends sufficient information for a TOE to be specified for evaluation. Writers of the CC ST should ensure that the level of detail given is sufficient.
TOE security environment	HMG Infosec Standard No 2 [a] addresses both threats and physical, personnel and procedural security measures in discussing ADS Part 2. See CC [i] and the PP/ST Guide [m] for guidance on CC requirements.
Security Objectives of the TOE	Security Objectives are not addressed by HMG Infosec Standard No 2 [a]. Information about Security Objectives can be found in CC [i] and the PP/ST [m] Guide.
IT Security functional requirements of the TOE	Whilst HMG Infosec Standard No 2 [a] addresses countermeasures in discussing ADS Part 2, the form of specification required for a CC ST should be appreciated. Details of the CC requirements are contained within CC [i] and the PP/ST [m] Guide.

Security Target Requirement	Correlation with HMG Infosec Standard No 2
TOE summary specification	In discussing countermeasures under ADS Part 2 HMG Infosec Standard No 2 [a] recommends part of the information required. CC [i] and the PP/ST [m] Guide provide guidance on the additional information required.
Target Assurance requirement	The results of the Assurance calculations, through the use of HMG Infosec Standard No 1 [c], will provide a specified assurance level for each component entity within the scope of the Accreditation. These results can be used to specify a target evaluation assurance level for the TOE in the ST.
Strength of Function claims	HMG Infosec Standard No 2 [a] does not address strength of functions. See CC [i], CEM [j] and the PP/ST Guide[m] for guidance. Note however the various types of statement which may or may not be made about function strengths – see the corresponding ITSEC strength of mechanism guidance in UKSP 04 [l] Part III.
Rationale	Rationale is required to justify why objectives, security functional requirements and TOE-specific security functions are sufficient for countering the identified threat. This is not addressed by HMG Infosec Standard No 2 [a]. See CC [i] and the PP/ST [m] Guide for guidance.
Explicitly stated IT security functional requirements	Whilst HMG Infosec Standard No 2 [a] addresses countermeasures in discussing ADS Part 2, the form of specification required for a CC ST should be appreciated. Details of the CC requirements are contained within CC [i] and the PP/ST [m] Guide.
Protection Profile claims	This is not addressed by HMG Infosec Standard No 2 [a]. See CC [i] and the PP/ST [m] Guide for guidance.

Table IV-3 Correlation of CC ST Requirements with HMG Infosec Standard No. 2

Administrator and User Guidance

67. Details as to the requirements of the Administrator and User Guidance documentation required for a CC evaluation are contained in CC [i]. The Security Operating Procedures (SyOPs or SOPs) for an accreditation will contain some of the information required to meet the CC evaluation requirements for operational documentation. The information provided in CC[i] should be used to ensure that the SyOPs and the Administrator and User Guidance covers all aspects required for a CC evaluation.

Evaluation and Certification Reports

68. The ETR produced by the CLEF and CR produced by the CB are both forms of ‘inspection reports’ in the sense of HMG Infosec Standard No 2 [a] and are thus appropriate for filing in Part 4 of the ADS.

V. Assurance Maintenance

Approach

69. The UK Certificate Maintenance Scheme (CMS), as documented in UKSP 16 [n] offers a cost effective approach such that the investment made in the evaluation and certification of a system can be maximised, and so that the assurance in the security of the system is maintained. The requirements for re-evaluation and commitment to a re-evaluation programme should be documented in Part 1 of the ADS. The CMS can be applied to both ITSEC and CC evaluations.

70. CMS defines an approach that:
    - should ensure that the assurance in the security of a Target of Evaluation (TOE) is maintained;
    - provides recognition that the assurance in the TOE has been maintained;
    - provides a method for quick and cost-effective re-evaluations.

71. CMS provides a means for establishing confidence that the assurance in the TOE has been maintained by:
    - requiring a Developer Security Analyst (DSA) to analyse the security impact of all changes to the system;
    - committing the system to a programme of audits and re-evaluation.

72. If a system not entered into the CMS is modified, it can be re-evaluated. 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.

Overview of CMS

73. The principal CMS features are:
    - the Certificate Maintenance Plan (CMP);
    - the Certificate Maintenance Status Report;
    - the Developer Security Analyst;
    - the Categorisation Report;
    - the Security Impact Analysis;
    - Certificate Maintenance Audits;
    - Certificate Maintenance Re-evaluation.

74. The **Certificate Maintenance Plan**, produced by the sponsor, reviewed by the CLEF and approved by the CB, justifies the proposed audit and re-evaluation schedules in terms of the anticipated changes to the system and their likely impact over the period of the plan. It should define a policy for accepting or rejecting upgrades to component products of the system. Where such component products are significant to the security of the system it is desirable that products which themselves are covered by CMS are employed. It is recommended that the CMP be filed under the ‘ADS Review and Re-accreditation’ heading of ADS Part 1.

75. The **Certificate Maintenance Status Report**, is produced by the sponsor, and is reviewed by the CLEF and CB. This document contains a report of the progress against the CMP and is submitted annually.

76. The **Developer Security Analyst**, is a developer representative (or security consultant) who is expected to be familiar with the system, the evaluation results and the requirements of the evaluation criteria being used. The DSA may require training. Due to independence

requirements, the DSA cannot be supplied by the CLEF performing the audits, however, CLEFs will be able to provide training for the proposed DSA, should the need arise. It is recommended that the DSA be identified in Part 1 of the ADS.

77. CMS requires the production of a **Categorisation Report**. This task is typically performed by the DSA. The report shall assign each component of the system a category to indicate its significance to the security of the TOE.

78. The **Security Impact Analysis** is produced by the DSA and is the principal input to CMS. The evaluators independently check the validity of the analysis and perform penetration testing where necessary.

79. **Certificate Maintenance Audits** are to be performed periodically (typically annually) by the CLEF. The first audit is required to take place no more than six months after the certification of the system. The purpose of the audit is to establish confidence that the requirements of CMS are being met. It is recommended that the accreditor recognise the CMS audit as a ‘compliance audit’ in the sense of HMG Infosec Standard No 2 [a] and that audit reports be filed in Part 1 of the ADS.

80. **Certificate Maintenance Re-evaluations** are to be performed by the CLEF, either periodically (typically once every three years) or when changes of certain security significance have been made to the TOE. They involve a more thorough assessment than that which is involved in audit. However they are required less frequently than re-evaluations for TOEs for which no CMS commitment is made, and the CMS work of the DSA enables re-evaluation to be performed more efficiently than would otherwise be possible. It is recommended that the Evaluation Technical Reports and Certification Reports resulting from CMS re-evaluations be filed in Part 4 of the ADS.