UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No. 16

UK CERTIFICATE MAINTENANCE SCHEME

PART I

DESCRIPTION OF THE CMS

Issue 1.0
31 July 1996

Issued by:-

UK IT Security Evaluation & Certification Scheme

FOREWORD

The UK IT Security Evaluation and Certification Scheme has been established to evaluate and certify the level of assurance which may be placed in security features of Information Technology (IT) products and systems.

UKSP 16 describes the Certificate Maintenance Scheme (CMS) which operates as an integral part of the UK IT Security Evaluation and Certification Scheme. The CMS has been designed to encourage sponsors to commit to certificate maintenance by reducing re-evaluation costs and timescales, and by recognising the maintenance of assurance in those versions of systems and products that are maintained under the CMS, but which are not subject to formal re-evaluation.

This document (Part I of UKSP 16) defines the requirements of the CMS that are independent of the evaluation criteria and methodology.

P. M. Seeviour
Senior Executive
UK IT Security Evaluation and Certification Scheme

Correspondence in connection with this document, including requests for additional copies, should be addressed to:

Senior Executive
UK IT Security Evaluation and Certification Scheme
Certification Body
PO Box 152
Cheltenham
Glos GL52 5UF

Telephone: +44 1242 238739

Facsimile: +44 1242 235233

All trademarks are acknowledged whether shown within the text or not.

AMENDMENT RECORD

Amendments to this document will be published as and when required. The amendment record shall be maintained so that it indicates all changes made to the latest issue of the document.

Amendment Instruction Number	Pages Affected (SINs incorporated)	Incorporated by NAME Signature	Date

CONTENTS

FIGURES

REFERENCES

ITSEC Information Technology Security Evaluation Criteria
Version 1.2, 28 June 1991

ITSEM Information Technology Security Evaluation Manual
Version 1.0, 10 September 1993

MEMO7 CESG Computer Security Memorandum No 7
Configuration Management for Secure Systems
Issue 1.0, August 1990

MEMO11 CESG Computer Security Memorandum No 11
Security Activities in the Project Life Cycle
Issue 2.0, June 1996

UKSP01 Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 2.0, 29 April 1994

UKSP02 The Licensing of Commercial Licensed Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 2.0, 1 May 1995

UKSP05-1 Manual of Computer Security Evaluation, Part I: Evaluation Procedures
UK IT Security Evaluation and Certification Scheme,
UKSP 05 (Part I), Issue 3.0, October 1994

UKSP05-2 Manual of Computer Security Evaluation, Part II: Standard Evaluation Work Programmes
UK IT Security Evaluation and Certification Scheme,
UKSP 05 (Part II), Issue 1.0, December 1994

UKSP05-3 Manual of Computer Security Evaluation, Part III: Evaluation Techniques and Tools
UK IT Security Evaluation and Certification Scheme,
UKSP 05 (Part III), Issue 1.0, June 1994

UKSP14 UK Certification Body Evaluation Work Programmes
UK IT Security Evaluation and Certification Scheme,
UKSP 14, Issue 1.0, March 1995

ABBREVIATIONS

CB	Certification Body
CLEF	Commercial Licensed Evaluation Facility
CMAR	Certificate Maintenance Audit Report
CMB	Configuration Management Board
CMP	Certificate Maintenance Plan
CMSR	Certificate Maintenance Status Report
CMS	Certificate Maintenance Scheme
DEA	Development Environment Assessment
DSA	Developer Security Analyst
EOR	Evaluation Observation Report
ESR	Evaluation Summary Report
ETR	Evaluation Technical Report
RAMP	Ratings Maintenance Programme
SAC	Security Assurance Co-ordinator
SFN	Security Fault Notification
SIN	Scheme Information Notice
SOR	Scheme Observation Report
TOE	Target of Evaluation
UKAS	United Kingdom Accreditation Service
UK Scheme	The UK IT Security Evaluation and Certification Scheme
UKSP	United Kingdom Scheme Publication
UKSP 06	UK Scheme Publication 06 - Certified Products List
VSA	Vendor Security Analyst

Chapter 1 Introduction to UKSP 16

1.1 General

1.1.1 This manual is divided into three parts:

a) Part I (this document), which describes the UK Certificate Maintenance Scheme;

b) Part II, which describes the application of the methodology for evaluation activities conducted under the UK Certificate Maintenance Scheme, and the required actions on the developer;

c) Part III, which is the Developer Security Analyst (DSA) Reference Manual.

1.2 Background

1.2.1 The UK IT Security Evaluation and Certification Scheme (referred to in this document as the 'UK Scheme'), which is described in [UKSP01], was set-up to evaluate the security features of IT products and systems and certify the level of assurance which may be placed in them. The Scheme is administered by a Certification Body, who issue certificates following successful evaluation of an IT product or system.

1.2.2 Certificates are only valid for a specific version of a Target of Evaluation (TOE). However, most TOEs are subject to changes which are outside the scope of the certificate, and there is therefore a need for an effective process by which TOE certificates can be maintained. The UK Certificate Maintenance Scheme has been designed to meet that need.

1.3 Objectives

1.3.1 The objective of UKSP 16 is to define the requirements and obligations of the UK Certificate Maintenance Scheme (CMS).

1.3.2 The CMS operates as an integral part of the UK Scheme, the objectives of which are to meet the needs of both industry and UK government for security evaluation and to provide a basis for the mutual recognition of certificates. The UK Scheme is therefore intended to promulgate the availability of certified IT products. The CMS has been designed to further this aim by encouraging sponsors to commit to *maintaining* the certification status of products and systems.

1.3.3 The CMS has therefore been designed to encourage this commitment by meeting the following objectives:

a) defining an approach that will ensure that the assurance in the security of a TOE is maintained;

b) providing recognition of the fact that the assurance in versions of the TOE *has* been maintained between evaluated versions;

c) providing a method for quick and cost-effective re-evaluations;

d) ensuring that mutual recognition of certificates maintained under this scheme is not jeopardised.

1.3.4 The CMS strikes an appropriate balance between these objectives. Its underlying principles and philosophy are founded in the evaluation criteria and methodology (at the time of issue of this document, the ITSEC and ITSEM), thereby addressing the first and fourth objectives. The CMS addresses the second and third objectives by placing more trust in the work of the developer, whilst at the same time ensuring that this trust can be justified, and that the developer's work is always subject to an independent check.

1.3.5 In this way the CMS ensures that a TOE which has been subject to changes can be certified as remaining secure (with respect to its security target).

1.4 Scope of the CMS

1.4.1 All TOEs that are accepted into the UK Scheme must follow the requirements of the CMS as defined in UKSP 16. (The CMS requires a formal statement from the sponsor as to whether the TOE certificate is to be maintained under the CMS, or whether there is no such commitment.)

1.4.2 The CMS is equally applicable to certificate maintenance for both systems and products. In some areas, however, specific interpretation of the requirements is necessary in order to apply the CMS to secure systems and composed TOEs. Such interpretations are provided in Annex A.

1.4.3 The CMS requirements are independent of the evaluation criteria and methodology, except of course in respect of the details of the CMS re-evaluation approach and methodology. The criteria-dependent aspects of the CMS are detailed in Part II; those aspects that are not dependent on the evaluation criteria are detailed in Part I. Part II will be updated in the event of the UK Scheme adopting the Common Criteria in place of the ITSEC.

1.5 Intended Audience

1.5.1 Part I is intended to be read by any party that has an interest in certificate maintenance, namely:

a) *sponsors*, who bear the cost of re-evaluations and other certificate maintenance activities (e.g. audits), and receive evaluation and certification reports produced under the CMS;

b) *developers* (including system integrators), who are responsible for development and maintenance of the TOE and associated deliverables (it is possible that different organisations are responsible for production and maintenance);

c) *accreditors*, who are ultimately responsible for the security of an evaluated system;

d) *evaluators*, who perform re-evaluations and audits under the CMS;

e) the *project office* responsible for procuring a secure system;

f) the *Certification Body* (CB), which monitors re-evaluations and other certificate maintenance activities (e.g. audits), and re-issues certification reports.

1.5.2 For some evaluations (especially products), the sponsor and developer may be the same organisation.

1.5.3 Part II is intended to be read by developers, evaluators and the Certification Body, and may also be of interest to sponsors.

1.5.4 Part III is intended to be read by individuals who are to assume the role of the Developer Security Analyst (DSA) as described in UKSP 16.

1.6 Terminology

1.6.1 Throughout this document, mandatory CMS requirements are indicated by use of the words *shall* and *must*. The word *should* is used to indicate a preferred (but not mandatory) approach. The word *will* is used to express actions to take place in the future.

1.6.2 The document uses terminology as defined in the ITSEC and ITSEM, unless otherwise stated. In particular it should be noted that the terms *security enforcing* and *security relevant* are used within UKSP 16 with slightly different meanings from those given in [ITSEC].

1.6.3 The term *CMS re-evaluation* is used to refer specifically to re-evaluations carried out in accordance with the methodology defined in UKSP 16. The term *re-evaluation* (not prefixed) is used to refer to re-evaluations in general.

1.7 Structure of Part I

1.7.1 This document is divided into the following chapters:

a) Chapter 1 (this chapter) provides an introduction to UKSP 16;

b) Chapter 2 provides an overview of the UK Certificate Maintenance Scheme and its relationship to the UK Scheme;

c) Chapter 3 defines the requirements on the Certificate Maintenance Plan (CMP);

d) Chapter 4 defines requirements on the Developer Security Analyst (DSA);

e) Chapter 5 highlights requirements on the Security Impact Analysis and on how re-evaluations are to be carried out under the UK Certificate Maintenance Scheme;

f) Chapter 6 defines requirements for Certificate Maintenance Audits;

g) Chapter 7 describes the significance and scope of CMS Approval of TOE versions;

h) Chapter 8 defines the requirements for the maintenance of certificates for TOEs that do not have full membership of the CMS.

1.7.2 Additionally, there are two annexes, as follows:

a) Annex A describes how the CMS requirements can be applied to certificate maintenance for secure systems (and in particular, HMG systems) and composite TOEs;

b) Annex B provides guidance to sponsors and accreditors who need to make decisions on the scheduling of re-evaluations under the CMS.

Chapter 2 Certificate Maintenance Scheme Description

2.1 Introduction

2.1.1 This chapter provides a description of the UK Certificate Maintenance Scheme (CMS). The requirements of the CMS are described in greater detail in the remaining chapters of this document:

a) Chapters 3 to 7 describe the CMS requirements where the sponsor has committed to maintain the certificate under the CMS;

b) Chapter 8 deals with the case where no such commitment has been made.

2.2 Why the CMS is Needed

2.2.1 Evaluation results apply to a specific version of a TOE. Any change to that TOE or its environment may invalidate those results, and thus require re-evaluation. Users who have a need for a certified TOE may therefore be forced to decide whether to use:

a) a version of the TOE in which there is no assurance that it is secure; or

b) a certified, but obsolete, version of the TOE, which may indeed no longer be secure (owing to changes within the TOE environment such as new threats or the discovery of previously unknown vulnerabilities).

2.2.2 The CMS addresses this problem by providing a means for establishing confidence that the assurance in a TOE has been maintained without always requiring a formal re-evaluation. This is achieved by requiring the sponsor or developer to appoint a Developer Security Analyst (DSA) who performs an analysis of the security impact of all changes affecting the TOE. The periodic re-evaluations of the TOE required by the CMS make use of this

analysis to guide the re-evaluation, leading to a *significant* reduction in costs and timescales[1].

2.2.3 These benefits are a necessary prerequisite for encouraging more sponsors to commit to ongoing certificate maintenance rather than 'one-off' certification or ad-hoc re-certification.

2.2.4 The CMS nonetheless ensures that the assurance established in a certified TOE *is* maintained in practice by:

a) being founded on a clear underlying technical rationale, closely linked to the evaluation criteria and methodology: Part II explains how this is achieved;

b) requiring periodic audits of the application of the certificate maintenance processes for the TOE to provide confidence that assurance is maintained between re-evaluations (these require broadly the same level of CLEF effort as the Development Environment Assessment (DEA) in a full evaluation).

2.2.5 In summary, the CMS provides benefits to all parties involved in the certificate maintenance process; in particular:

a) sponsors benefit from a significant reduction in the cost and timescales of re-evaluations under the CMS;

b) product vendors benefit from the formal recognition of their commitment to certificate maintenance in UKSP 06 (the UK Certified Products List), and in timely approval of releases of their product produced under the CMS;

c) developers benefit from a higher quality TOE, since the CMS demands an analysis of the security impact of changes affecting the TOE, thereby helping to ensure that potential security problems are discovered and rectified at an earlier stage in the

[1]Estimates indicate a cost saving of 30-50% at E3, as compared with previous re-evaluations under the UK Scheme.

development process;

d) accreditors, and the user community in general, benefit as the risk to the security of their assets is reduced; the needs of users need no longer conflict with the need for a certified TOE.

2.3 CMS and the UK Scheme

2.3.1 The CMS operates as an integral part of the UK Scheme. The sponsor for the evaluation of any TOE which enters the UK Scheme is required to either:

a) make a formal commitment to maintenance of the certificate by applying for full membership of the CMS for the TOE; or

b) formally state that there is no commitment to maintain the certificate (for new tasks this will be at the Task Startup Meeting); in such cases there is no guarantee that the certificate will remain valid indefinitely, e.g. if exploitable vulnerabilities are discovered in the certified TOE at a later date: see Chapter 8.

2.3.2 This decision is not, however, irrevocable: for example, a sponsor may choose to apply for full membership of the CMS at a later stage, or may resign from the CMS.

2.3.3 The UKSP 06 entry for a product will state not only its certification status but also its status under the CMS.

2.3.4 Since the CMS is part of the UK Scheme, CLEFs performing CMS re-evaluations and other activities under the CMS must follow:

a) the UK Scheme requirements as defined in [UKSP01], [UKSP02] and other applicable UK Scheme Publications;

b) the requirements of the appropriate evaluation criteria and methodology, except where UKSP 16 dictates otherwise.

2.3.5 Thus a CLEF providing consultancy to sponsors and developers involved in the CMS must 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. See section 2.6 below.

2.4 Overview of the CMS

2.4.1 The detailed requirements of the CMS are provided in Chapters 3 to 8 of this document. The principal features of the CMS are:

a) the *Certificate Maintenance Plan* (CMP), which represents the sponsor's commitment to certificate maintenance according to an agreed re-evaluation and audit schedule;

b) the *Certificate Maintenance Status Report* (CMSR), by which a sponsor provides the CB with an annual report on the implementation of the CMP;

c) the *Developer Security Analyst* (DSA), who has prime responsibility for ensuring that the assurance in the TOE is maintained whilst the TOE is under the CMS;

d) the *Security Impact Analysis* (for which the DSA is responsible), which documents the analysis of changes affecting the TOE and justifies why the assurance in the TOE has been maintained;

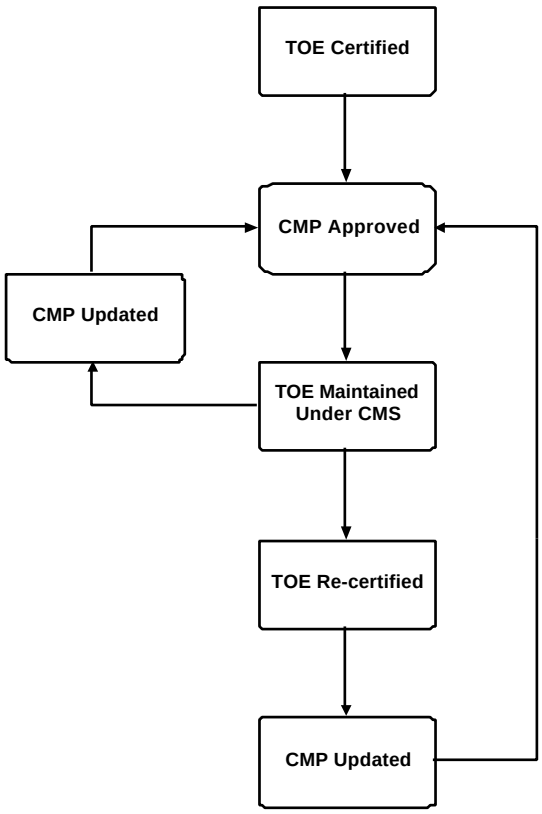
e) the *CMS Re-evaluation Methodology*, to be applied in all re-evaluations under the CMS, in which the level of evaluator effort reflects the risk that changes to the TOE or its environment could introduce vulnerabilities;

f) *Certificate Maintenance Audits*, performed by a CLEF in order to establish confidence that the requirements of the CMS are being met;

g) *CMS Approval*, which is awarded by the CB to versions of the TOE produced under the CMS.

2.4.2 If the sponsor has no intention to maintain the certificate for a TOE, then the CMS merely requires the sponsor to formally state this at the Task Startup Meeting (TSM).

2.4.3 The CMP represents the terms of reference for the development and modification of the TOE during the period between evaluations. It is produced by the sponsor, reviewed by a CLEF and approved by the CB. Approval of the CMP is one of the prerequisites for a TOE being granted full membership of the CMS (see below). The CMP justifies the proposed audit and re-evaluation schedules in terms of the anticipated changes to the TOE over the period and their likely impact on security.



2.4.4 Figure 2.1 below illustrates the TOE lifecycle under the CMS, highlighting the importance of the approval of the CMP and any updates made to it.

Figure 2.1: TOE Life Cycle under the CMS

2.4.5 It should be noted that although Figure 2.1 shows approval of the CMP occurring *after*

certification of the TOE, there is no reason why it cannot be produced prior to certification.

2.4.6 The CMSR is produced annually by the sponsor and is submitted to the CB and the contracted CLEF for review. It 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. The schedule for CMS re-evaluations and Certificate Maintenance Audits will be reassessed in the light of the contents of the CMSR.

2.4.7 CMPs and CMSRs are described in detail in Chapter 3.

2.4.8 The DSA is expected to be familiar with the TOE, the evaluation results, and the requirements of the evaluation criteria and methodology 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 an independent security consultant. If, however, the DSA is contracted from a CLEF, then the Certificate Maintenance Audits must be carried out by a different CLEF, in order to preserve independence (see section 2.6 below).

2.4.9 The DSA carries out an analysis of the impact of changes to the TOE and its environment, and documents this in a Security Impact Analysis. The DSA maintains the Security Impact Analysis in step with the changes. The DSA also maintains a list of known vulnerabilities in the construction and operation of the TOE. In particular, the DSA must ensure that:

a) any new exploitable vulnerabilities reported in the TOE are removed or neutralised;

b) the TOE's user community is provided with the means of removing or neutralising any remaining vulnerabilities.

2.4.10 The responsibilities of the DSA are described in detail in Chapter 4.

2.4.11 The Security Impact Analysis 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 provision of the Security Impact Analysis significantly reduces the level of evaluation effort required in a CMS re-evaluation to confirm that the assurance in the TOE has been maintained. This leads to a corresponding reduction in the cost and timescales of CMS re-evaluations as compared with non-CMS re-evaluations. The analysis is also subject to checking during the Certificate Maintenance Audits.

2.4.12 The requirements for a Security Impact Analysis, and how it is used in a CMS re-evaluation, are highlighted in Chapter 5 and specified in detail in Part II.

2.4.13 Confidence that the DSA is following the CMP and the requirements of the CMS is established by regular (by default, annual) Certificate Maintenance Audits (hereinafter abbreviated to 'CM Audits') carried out by a CLEF. The CLEF reports the results of the CM Audit in a CM Audit Report (CMAR). The CLEF carrying out the CM Audit need not be the same CLEF as that contracted for evaluation or CMS re-evaluation of the TOE.

2.4.14 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-compliances with the CMS or CMP.

2.4.15 CM Audits and CMS Approval are described in Chapter 6 and Chapter 7, respectively. The methodology for CM Audits is described in Part II.

2.4.16 Figure 2.2 illustrates a TOE being maintained under the CMS in accordance with its CMP, from the certification of version 1.0 to the CMS re-evaluation of version 2.0. The following should be noted in particular:

a) Versions 1.1 and 1.2 of the TOE are *CMS Approved*, provided the Security Impact

Analysis (SIA) confirms that the changes made since the certified version (1.0) are within the scope of CMS Approval.

b) The latest version of the SIA acts as input to the CM Audits. In the example given in Figure 2.2, a CM Audit has been scheduled shortly after the release of version 1.1 (note that in practice there may be more than one CM Audit between the evaluation and the CMS re-evaluation);

c) The version of the SIA produced for version 2.0 of the TOE acts as input to the CMS re-evaluation.

d) Each version of the SIA must address all changes since the certified version (1.0).

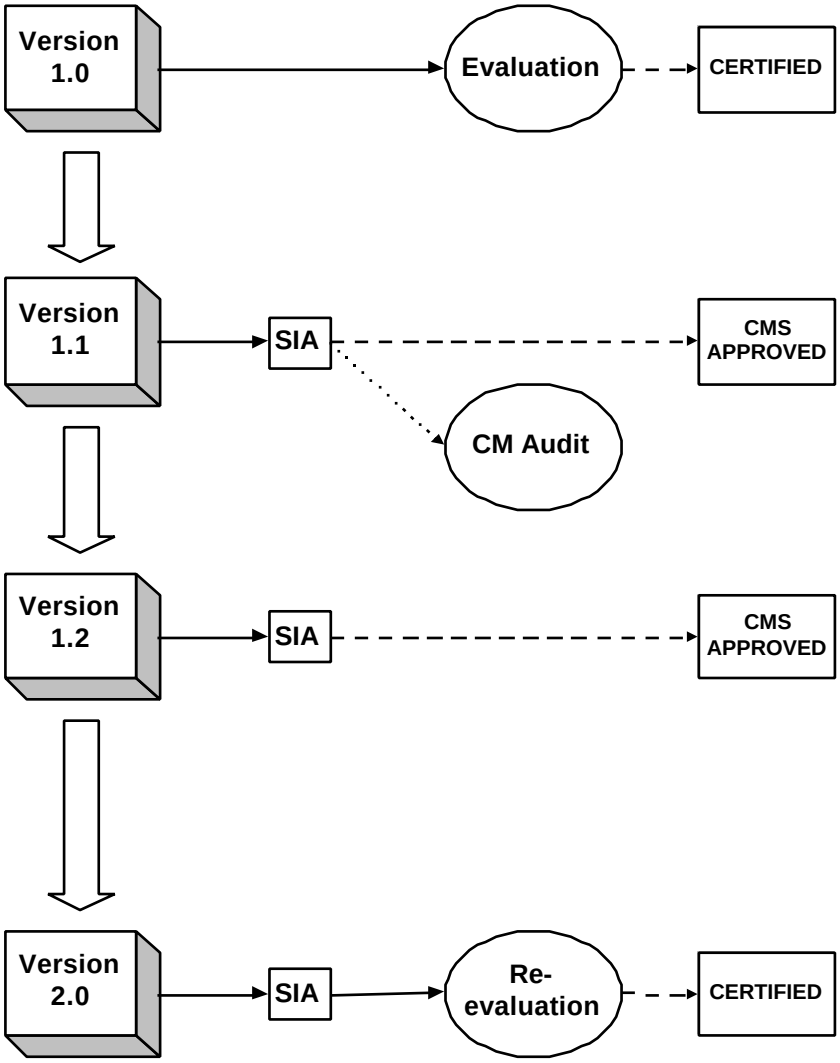


Figure 2.2: Progress of a TOE under the CMS

2.5 Membership of the UK Certificate Maintenance Scheme

2.5.1 The CB assigns a TOE's membership status of the CMS as one, and only one, of the following:

a) None

b) Full

c) Suspended

d) Terminated

e) Resigned.

2.5.2 The CMS membership status of a product will be stated in its UKSP 06 entry, which will also identify versions of the TOE that are *CMS Approved*.

2.5.3 A membership status of *None* signifies that the sponsor has either:

a) applied for the TOE to gain full membership, but this has not yet been achieved; or

b) has not committed to maintain the certificate for the TOE.

2.5.4 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 UK Scheme or under another jurisdiction subject to a mutual recognition agreement; a completed evaluation must, naturally, have led to the award of a certificate stating that the target assurance level has been met. Formal application is signified by submission of a CMP to a CLEF for review (normally the CLEF who evaluated the TOE), copied to the CB.

2.5.5 Full membership of the CMS is granted (where the previous membership status was *None*) 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.

2.5.6 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. Chapter 3 describes the circumstances where such deviation may be allowed.

2.5.7 Figure 2.3 below highlights the different stages in membership that a TOE may go through, beginning with a status of *None*, together with the events that trigger a change in status.

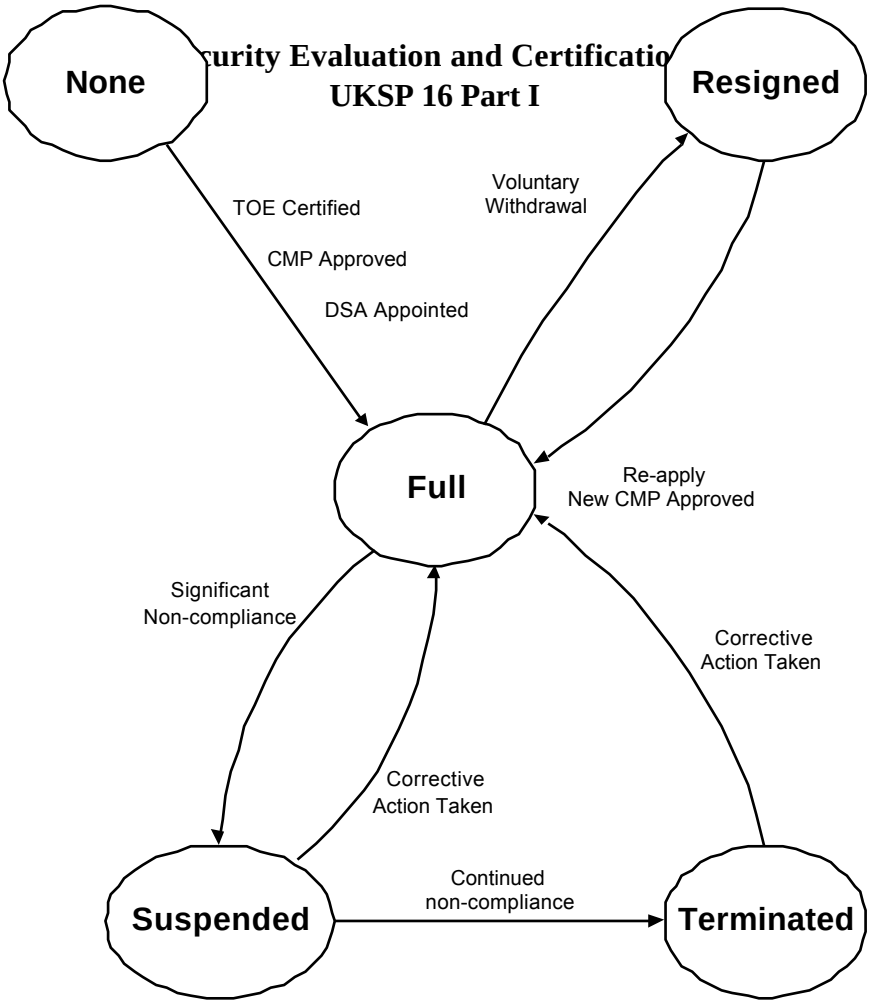

None
Resigned
TOE Certified
CMP Approved
DSA Appointed
Voluntary
Withdrawal
Full
Re-apply
New CMP Approved
Significant
Non-compliance
Corrective
Action Taken
Corrective
Action Taken
Suspended
Continued
non-compliance
Terminated

Figure 2.3: CMS Membership Status for a TOE

2.5.8 If a CLEF reports any non-compliance with the CMS or the agreed CMP then no further releases of the TOE will be granted a status of *CMS Approved* until corrective action has been agreed and applied. Such non-compliance includes failures to:

a) comply with the CM Audit and/or CMS re-evaluation schedule as stated in the CMP;

b) provide adequate DSA cover for the TOE;

c) notify the CB of changes that are outside the scope of CMS Approval;

d) adequately address any new known vulnerabilities affecting the TOE.

2.5.9 Membership of the CMS is *suspended* if the CB is not satisfied that appropriate corrective action is being taken to resolve any reported non-compliances within agreed timescales. The CB will normally require corrective action to be taken, and evidence provided, within three months. However, a serious non-compliance with the CMS may lead to *immediate* suspension from the CMS if (as a result) the CB has little confidence in the ability of the

DSA and developer to maintain the assurance in the TOE .

2.5.10 Membership of the CMS is *terminated* if there is continued non-compliance with the requirements of the CMS. This sanction will only be applied as a last resort; once membership has been terminated, the sponsor must re-apply for full membership of the CMS. Again, the CB will normally allow three months before converting a status of *suspended* to *terminated.*

2.5.11 The CB will issue formal warnings to the sponsor prior to any change in status to *suspended* or *terminated*, which will state the required timescales for implementation of appropriate corrective actions. The sponsor has right of appeal against any such change in status, initially to the Certification Body via the Head of the Certification Body or (if the sponsor considers this course of action ineffective) to the Management Board.

2.5.12 A sponsor may also voluntarily change a TOE's status to *resigned* by notifying the CB and the contracted CLEF(s). This might be necessary if, for example:

a) the TOE is no longer available or is no longer required;

b) the developer is no longer able to meet the obligations of the CMP or the CMS;

c) the CMS re-evaluation schedule cannot be met due to financial or other constraints.

2.6 Independence Rules

2.6.1 The following rules apply to ensure the independence of evaluation activities which CLEF staff may carry out under the CMS for a given TOE:

a) An individual who has been involved in the development of a TOE, or has provided consultancy for it, may not be involved in any evaluation activity for that TOE (i.e. the CMS re-evaluation, the CM Audits, and review of the CMP and CMSRs) during

the same maintenance cycle.

b) If a CLEF provides the DSA for a TOE during a maintenance cycle, the same CLEF may not be contracted to perform the CM Audits, the CMS re-evaluation or the reviews of the CMP or CMSR during the same cycle.

2.6.2 Note that a 'maintenance cycle' is defined as the period which begins at the conclusion of an evaluation (or re-evaluation) of the TOE and finishes at the conclusion of the subsequent CMS re-evaluation of the TOE (i.e. it covers the expected lifetime of the CMP).

2.7 CMS Closedown Procedures

2.7.1 CMS closedown procedures must be invoked whenever a TOE is withdrawn from the CMS (voluntarily or forced). The closedown and archiving procedures described in [UKSP05-1] apply. In addition to the documentation listed in [UKSP05-1], the following task material should normally be archived by the CLEF:

a) the CMP and CMSR(s);

b) Security Impact Analysis (all versions since the last evaluation or re-evaluation);

c) CM Audit Reports;

d) Records of reviews of the CMP and CMSR(s).

2.7.2 As described in [UKSP05-1], the CB and CLEF obviously cannot insist that the sponsor and/or developer should archive all relevant material for the period required by the UK Accreditation Service (UKAS), i.e. six years. Nevertheless, sponsors and developers should note that continued availability of relevant material will greatly assist any future evaluation involving the TOE, as well as facilitating a TOE regaining full membership of the CMS at a later date.

2.7.3 In the event of a sponsor deciding to contract a different CLEF to perform the CMS re-evaluation and audit work, the sponsor should arrange for transmission of deliverables to the new CLEF. Any residual information relevant only to the original CLEF must be archived as described in [UKSP05-1].

2.8 Summary of UK Certificate Maintenance Scheme Obligations

2.8.1 Figure 2.4 below summarises the obligations on the sponsor, DSA, developer, CLEF and Certification Body (CB) in relation to the various aspects of the CMS.

Certificate Maintenance Plan	
Sponsor	Produces and maintains the CMP Provides CMP to CB and CLEF Pays CLEF fees for review of CMP
DSA	Provides input to CMP as required Provides or checks the Categorisation Report
Developer	Provides information and support to DSA
CLEF	Provides or checks the Categorisation Report Reviews the CMP for content and presentation Reviews updates to CMP Submits results and recommendations to CB and sponsor
CB	Examines results of CLEF review Approves the CMP Reviews CMS membership status for TOE

Certificate Maintenance Status Report	
Sponsor	Produces the CMSR Provides CMSR to CB and CLEF Pays CLEF fees for review of CMSR
DSA	Provides input to the CMSR
Developer	Provides information and support to the DSA
CLEF	Reviews CMSR to check for divergence from the CMP Submits results and recommendations to CB and sponsor
CB	Examines results of CLEF review Reviews CMS membership status for TOE

Figure 2.4: Certificate Maintenance Scheme Obligations (Page 1 of 3)

CM Audits

Sponsor	Pays CLEF and CB fees for the CM Audits
DSA	Carries out activities as required by the CMP and CMS Provides deliverables for CM Audit Ensures problem reports are resolved
Developer	Provides information and support to DSA Agrees and implements corrective actions Provides support for the CM Audit
CLEF	Performs CM Audit Submits CM Audit Report and any problem reports to CB and sponsor
CB	Where appropriate, witnesses CM Audits Examines CM Audit Report Reviews CMS membership status for TOE

Security Impact Analysis and CMS Approval	
Sponsor	Provides Security Impact Analysis to CLEF Notifies CB of TOE releases submitted for CMS Approval
DSA	Produces and maintains the Security Impact Analysis Checks that changes fall within the scope of CMS Approval
Developer	Provides information and support to DSA
CLEF	Examines Security Impact Analysis during CMS Re-evaluations and CM Audits
CB	Declares product versions as *CMS Approved* in UKSP 06

Figure 2.4: Certificate Maintenance Scheme Obligations (Page 2 of 3)

CMS Re-evaluations	
Sponsor	Pays CLEF and CB fees for performing the CMS re-evaluation
DSA	Provides deliverables required for the CMS re-evaluation Ensures problem reports are resolved
Developer	Provides information and support to DSA
CLEF	Performs CMS re-evaluation Submits ETR and any problem reports to CB and sponsor
CB	Monitors CMS re-evaluation Examines ETR and issues certificate update Reviews CMS membership status for TOE Updates UKSP 06 where relevant

Figure 2.4: Certificate Maintenance Scheme Obligations (Page 3 of 3)

Chapter 3 The Certificate Maintenance Plan and Status Report

3.1 Introduction

3.1.1 This chapter describes requirements for the production and maintenance of the Certificate Maintenance Plan (CMP) for a TOE, and also for the production of the annual Certificate Maintenance Status Report (CMSR).

3.1.2 Responsibility for production of the CMP rests with the sponsor (the intended sponsor of the next CMS re-evaluation, if different from the sponsor of the most recent evaluation). However, much of the input will be provided by the DSA. Input, in the form of categorisation information, may also be provided by a CLEF.

3.2 Required Contents

3.2.1 The CMP shall include or (where appropriate) reference the information identified in Figure 3.1, which is described in more detail below (see also Annex A for guidance on CMPs for systems and composite TOEs).

3.2.2 Some of the information required in a CMP will be commercially sensitive, and hence will be subject to appropriate protective markings (and, potentially, confidentiality agreements).

1 TOE Overview
- 1.1 TOE Description
- 1.2 TOE Evaluation History

2 Maintenance Schedule
- 2.1 Planned Releases of the TOE
- 2.2 CMS Re-evaluation Schedule
- 2.3 CM Audit Schedule

3	Certificate Maintenance Procedures
	3.1 Identification of Key Roles
	3.2 Description of the DSA Role
	3.3 TOE Maintenance Procedures
	3.4 Vulnerability Tracking and Handling Procedures
4	Scheme Interpretations
	4.1 Applicable Interpretations of Evaluation Criteria and Methodology
	4.2 Applicable Interpretations of CMS
A	Categorisation Report
	A.1 Categorisation of TOE Components
	A.2 Criteria for Future Categorisation
	A.3 Security Relevant Development Tools

Figure 3.1: Certificate Maintenance Plan - Contents List

TOE Description

3.2.3 This section shall contain a brief description of the TOE, including the security functionality provided by the TOE. The CMP may reference the security target for this information, provided the security target is made available to all recipients of the CMP.

TOE Evaluation History

3.2.4 This section shall, for each version of the TOE that has undergone, or is undergoing, evaluation under the UK Scheme (including CMS):

a) identify the version evaluated, or currently under evaluation, and the target evaluation level;

b) reference any evaluation results (ETRs and CMARs) and certification reports.

3.2.5 The evaluation history may also refer to any other relevant evaluations of the TOE (for example, non-UK Scheme evaluations), or of closely related TOEs (for example, of underlying platforms or of TOEs based on some common components).

Planned Releases of the TOE

3.2.6 This section shall describe the TOE life-cycle and shall identify the current plans (forecast) for new releases of the TOE. This shall include a brief description of any planned changes to the TOE that are likely to have a significant security impact. The expected timetable for new releases shall be given, where known.

CMS Re-evaluation Schedule

3.2.7 This section shall identify the target date for the start of the next CMS re-evaluation of the TOE (if any). Where possible, the target date should be linked to a planned version of the TOE. It is accepted that this will be subject to change as time progresses; however, any changes must be notified in the CMSR.

3.2.8 The CMP shall justify why the 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 normally shall be no more than three years, shall 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 (see Annex B for further guidance).

CM Audit Schedule

3.2.9 This section shall identify (to the nearest month) the planned dates for the CM Audits. If it is intended that CM Audits occur at intervals of greater than one year, this must be justified.

Identification of Key Roles

3.2.10 This section shall identify the following key roles:

a) the sponsor for the next CMS re-evaluation and CM Audits;

b) the DSA(s) for the TOE, and the date of their appointment to the role (actual or planned);

c) the CLEF assigned for undertaking CM Audits (if known);

d) the CLEF assigned for the next CMS re-evaluation (if known);

e) the CLEF who produced the Categorisation Report (if relevant);

f) Certifier for the certificate maintenance activities (if known).

Description of the DSA Role

3.2.11 This section shall describe how the DSA role will be fulfilled by the identified individuals (for example, as a technical assurance or security authority, or as part of the development team).

TOE Maintenance Procedures

3.2.12 This section shall describe or reference the procedures for:

a) configuration management of the TOE;

b) maintenance of the evaluation deliverables, including a statement of the regression testing policy for the TOE and the use of development tools to support the maintenance process (e.g. configuration control tools, traceability databases and automated test suites);

c) performing the analysis required in order to produce the Security Impact Analysis (as detailed in Chapter 5 and Part II), and how this fits in with the TOE development process.

Vulnerability Tracking and Handling Procedures

3.2.13 This section shall describe or reference procedures for handling new known vulnerabilities in the TOE, which the DSA must ensure are followed. This description shall detail the procedures for:

a) identifying and collating the information (for example, from reports submitted by users of the TOE, or from active threat monitoring); this shall include a statement of the intended frequency of submitting requests to the CB for vulnerability information relevant to the TOE;

b) developing, implementing and testing fixes;

c) distribution, to the TOE's user community, of fixes to be applied to the TOE;

d) notifying users of interim workarounds required to address vulnerabilities.

Applicable Interpretations

3.2.14 The CMP shall describe or reference (e.g. as documented in SORs or SINs) any agreed interpretations (between the sponsor, developer, CLEF and CB) of the evaluation criteria or CMS requirements as they apply to the TOE. Such interpretations shall remain valid for the period of validity of the CMP. New interpretations (as documented in SINs) shall apply as follows:

a) new interpretations of the evaluation criteria shall apply if agreed by the sponsor and developer;

b) new interpretations of CMS requirements shall always apply.

3.2.15 This section shall also (in the *Applicable Interpretations of the CMS* subsection) include a description of any changes to the TOE or its security target that are permitted for the TOE, where these would otherwise fall outside the scope of CMS Approval (see Chapter 7). It shall justify why such changes can be allowed, by reference to the criteria specified in paragraph 7.4.4.

3.2.16 Examples of the types of change that can be allowed include (see Chapter 7):

a) changes to the TOE platform (which constitute a change to the TOE environment);

b) changes to threats, where the threats are changing more frequently than the scheduled CMS re-evaluations.

Categorisation Report

3.2.17 The CMP shall include or reference the Categorisation Report for the TOE. This shall categorise each component of the TOE (defined at the lowest representation available at the target evaluation level) as described in Chapter 5 and in Part II. It shall define the criteria to be used for categorising new components introduced into the TOE, and for deciding whether changes to existing components result in a change of the category to which they are assigned.

3.2.18 The Categorisation Report shall also identify any tools used in the development environment that are categorised by the evaluators as security relevant.

3.2.19 The initial Categorisation Report may be produced by a CLEF, possibly as part of the final ETR. Much of the categorisation information is, however, likely to be based on evidence that was provided by the developer for the initial evaluation and validated by the evaluators. As such, it is permissible for the Categorisation Report to be produced by the DSA, and checked by the CLEF. The Categorisation Report will be maintained by the DSA, and will be subject to validation by the evaluators in subsequent CMS re-evaluations of the TOE (and, to some extent, the CM Audits).

3.3 Delayed Applications for Full Membership

3.3.1 The granting of full membership of the CMS to a TOE will not always coincide with or closely follow an evaluation of the TOE under the UK Scheme. This may be because:

a) the TOE was evaluated prior to the CMS;

b) the sponsor decides to apply for full membership of the CMS at a later date.

3.3.2 In such cases, the CMP must take into account the possible impact of changes made to the certified TOE during the period between the release of the certified version and the appointment of a DSA. If significant changes have been made to the TOE during this period, the CB may require the next CMS re-evaluation to be brought forward. Alternatively, the CB may rule that the CMP can only be approved once:

a) the outcome of the first CM Audit is known; or

b) a Security Impact Analysis is provided covering the changes made in the absence of DSA cover, and has been checked by a CLEF (by a sampling approach, as for a CM Audit: see Chapter 6).

3.4 Conditions for Re-application to the CMS

3.4.1 As described in Chapter 2, a sponsor for a TOE whose CMS status is either *Resigned* or *Terminated* may subsequently re-apply for full membership of the CMS. In such cases, a new CMP must be submitted for approval. The following conditions must also be satisfied:

a) the CMP must take into account the possible impact of changes made to the TOE since it had full membership of the CMS, as described in paragraph 3.3.2 above.

b) if the TOE membership was terminated, evidence is required that the problem which led to termination has been resolved, and this must be confirmed by a CLEF during a CM Audit.

3.5 Approval of the Certificate Maintenance Plan

3.5.1 The CMP shall be reviewed for content and presentation by a CLEF. A record of the review of the CMP shall be sent to the sponsor and copied to the CB. If the Categorisation Report has been produced by the DSA, this shall be included in the CMP review.

3.5.2 Following successful review, the CB will approve the plan. The CB may, however, choose to withhold approval if they are not satisfied with any aspect of the CMP (for example, the planned schedule for CMS re-evaluations or CM Audits, or the validity of the approaches taken by the developer or the CLEF).

3.5.3 Following approval of the CMP and appointment of a DSA, the CB will confirm that the TOE has full membership of the CMS. For products, a statement to this effect will be made in their UKSP 06 entry, where relevant.

3.6 Certificate Maintenance Plan Validity

3.6.1 The CMP remains valid until the completion of the next CMS re-evaluation of the TOE, provided that:

a) no significant problems are found during the CM Audits carried out during this period;

b) assurance in the TOE is not adversely impacted by the discovery of new vulnerabilities or attack techniques;

c) the CB is satisfied with the annual CMSRs submitted by the sponsor.

3.6.2 The CB and CLEF must be informed, without delay, of any event which affects the validity of the CMP, including:

a) intended changes to the schedule for CMS re-evaluation or CM Audits;

b) changes being made to the TOE that are outside the scope of CMS Approval;

c) changes to DSA personnel.

3.6.3 Deviation from the CMP will not be permitted if, in the CB's judgement, it will result in a loss of confidence in versions of the TOE submitted for CMS Approval. The CB may rule that the CMP is updated and re-submitted to a CLEF for review within specified timescales (see next section).

3.6.4 The CMP may also be rendered invalid in the event of the identification of an entirely new threat to the TOE[2], or the discovery of an exploitable vulnerability that can only be

[2]As opposed to a 'new' threat which is simply a further instantiation of a threat already included in the security target.

addressed by a change that is outside the scope of CMS Approval (see Chapter 7). In such cases the CB and CLEF must be informed of the event without delay, following which the CB will, in consultation with the sponsor, decide on the level of CLEF effort appropriate. This may involve any of the following:

a) an additional CM Audit;

b) examination of the list of known vulnerabilities to assess the proposed countermeasures;

c) a CMS re-evaluation which includes penetration testing by the evaluators.

3.7 Updating the Certificate Maintenance Plan

3.7.1 The CMP must be kept under configuration control. The sponsor must review the CMP at regular intervals (at minimum, during production of the annual CMSR) and update it when necessary. An update will usually be necessary following (or during) the next CMS re-evaluation of the TOE, to cover the period to the next CMS re-evaluation. The CB may also require that the CMP is updated following a CM Audit or review of the CMSR.

3.7.2 The procedures for approval of an updated CMP are as follows:

a) the updated CMP shall be submitted to the CLEF and CB, with changes clearly identified;

b) the updated CMP shall be reviewed by the CLEF as described for the initial issue of the CMP.

3.7.3 Any proposal by the sponsor to defer the planned CMS re-evaluation is subject to approval of the CB, who will require a justification for the delay (e.g. slippage in the development schedule). Any proposal to re-evaluate a later version of the TOE than that stated in the

CMP must be justified by reference to the changes made to, and the number of vulnerabilities found in, the TOE since the most recent evaluation or re-evaluation.

3.8 Certificate Maintenance Status Report

3.8.1 The CMSR is a report of progress against the CMP which the sponsor must submit annually to the contracted CLEF(s) and the CB, unless there is already a CMS re-evaluation of the TOE ongoing. The first CMSR must be issued no later than 12 months after certification or approval of the CMP, whichever is the later.

3.8.2 Figure 3.2 below defines the required content of a CMSR, which is discussed in more detail in the rest of this section.

Figure 3.2: Certificate Maintenance Status Report - Contents List

Introduction

3.8.3 This section of the CMSR shall identify the TOE, reference the CMP, and state the reporting period.

Significant Events During Reporting Period

3.8.4 This section shall give dates for all milestones reached during the reporting period, including releases of the TOE and CLEF activities.

3.8.5 For each release of the TOE during the reporting period shall indicate their status, i.e. one of certified, CMS Approved or uncertified (the latter indicating that it has been subject to changes that are outside the scope of CMS Approval). A brief summary of the current Security Impact Analysis shall also be provided, highlighting any significant changes to the TOE and their impact on security.

3.8.6 Any divergence from the CMP shall be described, together with a justification as to why the CMP need not be updated. This includes any changes to DSA personnel or their status, with appropriate dates.

Status of Problems

3.8.7 This section shall identify the status of each outstanding problem report raised during previous evaluations or CM Audits.

3.8.8 It shall also reference the current version of the list of known vulnerabilities in the TOE, and shall provide statistics which identify the numbers of vulnerabilities discovered during the reporting period that:

a) have been fixed;

b) have had procedural workarounds identified;

c) are currently under investigation;

d) have been subject to evaluation.

Milestones for Next Reporting Period

3.8.9 This section shall give dates for any milestones forecast for the next reporting period, i.e. releases of the TOE and CLEF activities.

Review of the CMSR

3.8.10 The CMSR shall be reviewed by a CLEF, who shall submit recommendations to the CB as to whether the CMS re-evaluation and CM Audit schedules are still valid in light of the content of the CMSR. The CB will consider the CMSR and the CLEF's recommendations, and will discuss with the sponsor and CLEF any changes that are required to the schedule defined in the CMP.

Chapter 4 Developer Security Analyst

4.1 Introduction

4.1.1 This chapter defines the role of the Developer Security Analyst (DSA), and the responsibilities on such an individual (or individuals).

4.1.2 The TOE will only be granted full membership of the CMS once at least one DSA has been appointed for the TOE, and the identity of the DSA has been notified to the CB in the CMP. The sponsor must ensure that:

a) the appointed DSA has the appropriate skills and experience for the role (training should be sought where appropriate);

b) there is adequate cover in the event of a DSA not being available for an extended period of time;

c) the CB is notified without delay of any changes to DSA personnel.

4.1.3 If the sponsor fails to ensure the above requirements are met, resulting to a failed CM Audit, this could constitute grounds for immediate suspension of the TOE from the CMS (see Chapter 2).

4.1.4 The CB must be consulted before a DSA may be assigned to another TOE, or assume the role for more than one TOE.

4.1.5 Throughout this document, the DSA is referred to in the singular. However, it is acceptable for the DSA role to be filled by more than one person, provided there is a single point of contact assuming responsibility for the certificate maintenance process. For most TOEs, a single DSA will be sufficient to satisfy the obligations of the CMS; however, for large and complex TOEs, it is possible that more than one DSA will be required to provide adequate cover for the TOE.

4.2 Developer Security Analyst Role

4.2.1 The CMS does not mandate any particular way in which the DSA role must be fulfilled for a TOE: that is a matter for the sponsor to decide, in consultation with the developer. The DSA must, however, be familiar with:

a) the TOE security target and architecture;

b) the evaluation results for the TOE (i.e. the ETR);

c) the evaluation criteria and methodology;

d) the requirements of the CMS.

4.2.2 The CMS does not preclude the DSA being involved in the development of the TOE.

4.2.3 Figure 4.1 illustrates a reporting structure in which the DSA delegates aspects of the analysis work to members of a small development team (of which the DSA could be a member).

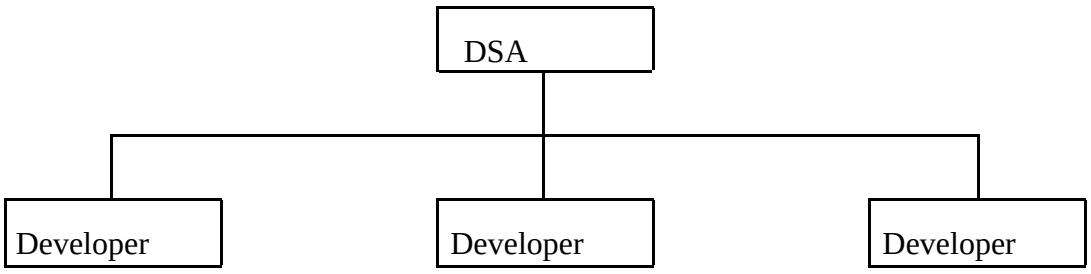


Figure 4.1: Example DSA Role for a Small TOE Development

4.2.4 For large TOE developments, it is possible that several DSAs will be required. For example, if there are several development teams, it may be appropriate to appoint a DSA for each team, each of whom reports to a single DSA who assumes DSA responsibilities for the TOE as a whole. A possible structure is illustrated in Figure 4.2 below.

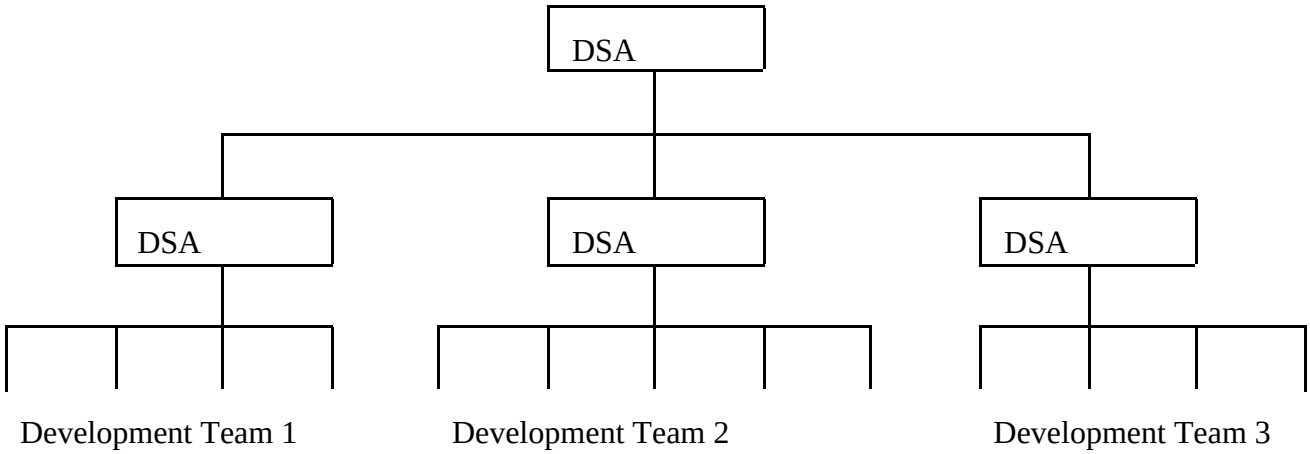


Figure 4.2: Example DSA Role for a Large TOE Development

4.2.5 The role of the system DSA, particularly those following [MEMO7] and [MEMO11], is discussed in Annex A. For example, the DSA may be provided by the project office for the system. The model illustrated in Figure 4.2 could be adopted for a large system, in which the 'subordinate' DSAs are appointed within different subcontractors or developers.

4.3 DSA Responsibilities

4.3.1 In order to adequately carry out the responsibilities required by the CMS, the DSA must have access to the criteria and methodology and all relevant UK Scheme Publications (in particular, UKSP 05, UKSP 16 and UKSP 11). The DSA is responsible for dissemination of appropriate documentation to the development team, and for ensuring that these documents are followed where relevant.

Deliverables

4.3.2 The DSA is responsible for ensuring that the deliverables required to support a CMS re-evaluation of the TOE or CM Audit are produced, and acts as the main point of contact for the CLEF and CB. The DSA has particular responsibility for provision of the Security Impact Analysis required as described in Chapter 5 and in Part II, and also for maintaining the Categorisation Report. The DSA must ensure that both documents are kept under configuration control.

4.3.3 The DSA must take ultimate responsibility for the Security Impact Analysis, and for the other deliverables required to support a CMS re-evaluation. However, the CMS does not preclude a DSA:

a) delegating analysis work to members of the development team or (in the case of TOEs under the US RAMP scheme) Vendor Security Analysts (VSAs);

b) seeking assistance in the form of consultancy to help in the preparation of any of the deliverables.

4.3.4 The DSA must have sufficient technical authority to be able to ensure that the evaluation deliverables are updated when necessary. The DSA must have a reporting line up to senior management, to ensure that the developers follow the procedures required by the CMP (as is normal for QA managers). Part II defines the criteria for deciding whether or not particular deliverables should be updated. The DSA's decision should be made on the basis of the assessment of the changes provided in the Security Impact Analysis; the DSA may seek advice from the CLEF or from the CB if in doubt.

Testing

4.3.5 The DSA must ensure that sufficient security testing (as required by the evaluation criteria) is performed on all releases of the TOE to be submitted for CMS Approval. This must include the execution of tests (when appropriate) to demonstrate that previously corrected flaws in the implementation of the TOE, that were raised as problem reports during previous evaluations of the TOE, have not been re-introduced following changes to the TOE.

Vulnerabilities

4.3.6 The DSA shall ensure that there is effective tracking and management of vulnerabilities affecting the TOE; this includes active monitoring of changes to the TOE threat environment as described in the CMP. The DSA must, on a regular basis (as stated in the CMP) request from the CB details of any generic vulnerabilities the CB are aware of that may apply to the TOE. The DSA is responsible for maintaining a list of known vulnerabilities affecting the TOE.

4.3.7 The DSA shall ensure that appropriate corrective action is taken to resolve all known vulnerabilities. The DSA shall also ensure that the TOE user community is provided with the means of removing or neutralising any such vulnerabilities (e.g. patches or TOE upgrades, or procedural countermeasures). This shall be accompanied by information which enables users to decide whether or not the vulnerability is relevant to their system.

4.3.8 Figure 4.3 summarises the obligations on the DSA.

Obtain training if necessary.
Provide input to the CMP and CMSRs as required by the sponsor.
Follow the requirements of the CMP and the CMS and ensure any necessary corrective actions are taken.
Maintain the Categorisation Report.
Produce and maintain the Security Impact Analysis.
Act as main point of contact for CMS re-evaluations and CM Audits
Ensure evaluation deliverables are updated when appropriate
Ensure adequate security testing is performed on all CMS Approved TOE releases.
Maintain the list of known vulnerabilities in the TOE by: a) ensuring that reported vulnerabilities are being adequately tracked;

b) ensuring that any changes to the threat environment are being adequately tracked;
c) making periodic requests to the CB for a list of known generic vulnerabilities;
d) ensuring appropriate corrective action is taken in each case.

Figure 4.3: Obligations on the DSA

Chapter 5 Impact Analysis and CMS Re-evaluations

5.1 Introduction

5.1.1 This chapter highlights the requirements on CMS re-evaluations and also the Security Impact Analysis, which is a key input to a CMS re-evaluation as well as a CM Audit (see Chapter 6).

5.1.2 A CMS re-evaluation addresses the changes to the TOE and/or its security target since the most recent evaluation of the TOE. It is guided by the Security Impact Analysis which, in turn, is dependent on the components affected, and their categorisation as defined in the Categorisation Report.

5.2 Categorisation of TOE Components

5.2.1 The CMS requires the DSA to maintain, and optionally produce, a Categorisation Report. The Categorisation Report shall assign each TOE component (including data files where relevant) to one, and only one, of the following categories identified below:

a) Security Enforcing (SE): any component which contains at least one function that *directly* contributes to the fulfilment of the security objectives, or which implements any security mechanism that is essential to the protection of a security enforcing mechanism from bypassing or tampering attacks.

b) Security Relevant (SR): any component which implements at least one security relevant function and no security enforcing functions, or for which it cannot be shown that, whatever the behaviour of the component, the security objectives will be upheld.

c) Security Irrelevant (SI): any component for which it is not necessary to make any assumptions regarding its behaviour in order to have confidence that the security objectives will be upheld.

5.2.2 The granularity of TOE component is dependent on the target evaluation level. Note that SI

components may be identified implicitly (e.g. all TOE components not explicitly identified as SE or SR).

5.2.3 If the TOE security target identifies dependencies on hardware, software and/or firmware that is external to the TOE, such components must also be categorised, by default as SR. If there are requirements for any external security enforcing functionality (e.g. an operating system providing identification and authentication of users), then the external component must either have been certified, or its functionality must have been evaluated as part of the TOE. In this case the component must be categorised as SE. (Note that the boundary of the TOE is defined by its security target.)

5.2.4 The Categorisation Report must also apply the general criteria defined above in the context of the TOE (for example, taking into account architectural boundaries between trusted and untrusted code) to enable a DSA to decide:

a) to which category any new component should be assigned;

b) whether a change to an existing component causes it to be placed in a different category.

5.3 Security Impact Analysis

5.3.1 The DSA is responsible for production and maintenance of the Security Impact Analysis, which provides an analysis of changes which may have an impact on the assurance that the TOE satisfies its security target. The Security Impact Analysis is presented to the evaluators as a key input to a CMS re-evaluation, and is also provided for sampling purposes in the CM Audits (see Chapter 6). An executive summary of the analysis is presented in each CMSR (see Chapter 3).

5.3.2 The main part of the Security Impact Analysis deals with changes to the construction of the TOE. Changes affecting the TOE development environment and operation are, however, also addressed by the analysis. For all changes, the Security Impact Analysis must describe the change and justify why the assurance in the TOE has been maintained. The justifications in respect of changes to the TOE implementation must always be supported by test

evidence.

5.3.3 Part II defines the detailed requirements for the content of a Security Impact Analysis.

5.4 Approach to CMS Re-evaluations

5.4.1 A CMS re-evaluation addresses changes to the construction of the TOE as well as those affecting the TOE development environment or the operation of the TOE.

5.4.2 For changes affecting the construction of the TOE, the level of evaluator effort required is critically dependent on the target evaluation level, the highest (most abstract) representation of the TOE affected, and the categorisation of the new or modified components. The following general principles apply (the CMS re-evaluation always being guided by the Security Impact Analysis):

a) changes with a major security impact require a detailed examination;

b) intermediate (significant) changes require sampling of changed evaluation deliverables in support of penetration testing;

c) changes with a minor security impact require only a review of the relevant part of the Security Impact Analysis, together with (where applicable) the supporting test evidence.

5.4.3 Part II defines the detailed requirements for CMS re-evaluations.

Chapter 6 Certificate Maintenance Audits

6.1 Introduction

6.1.1 This chapter describes the requirements on Certificate Maintenance Audits (CM Audits),

the purpose of which is to establish confidence that the DSA is ensuring that the necessary actions are carried out in order to maintain the assurance established in the previously certified TOE. The methodology for CM Audits is described in Part II.

6.2 Audit Schedule

6.2.1 The first CM Audit for a TOE shall take place no more than six months after approval of the CMP or certification of the TOE, whichever is the later. Thereafter, CM Audits shall occur annually (unless the CMP states otherwise) until the next CMS re-evaluation of the TOE.

6.2.2 The CB may require that the frequency of CM Audits is increased if:

a) a CM Audit or review of the CMSR reveals a significant divergence from the CMP in terms of the number of changes with an impact on the security of the TOE; or

b) a CM Audit results in a significant number of problem reports being raised.

6.2.3 Conversely, the CB may allow CM Audits to occur at intervals of greater than one year if there have been a small number of changes relevant to security, or if the CM Audits reveal no significant problems. Any changes to the audit schedule will be agreed with the sponsor.

6.2.4 Although it is a distinct activity from those required in a CMS re-evaluation, it is acceptable for the CM Audit to be combined with the DEA for the next CMS re-evaluation (assuming one is required). Such an arrangement may be appropriate in order to reduce travel costs.

6.3 Required Deliverables

6.3.1 The evaluators must be provided with copies of the following documents in advance of each CM Audit, if they do not already have them:

a) all issues of the CMP produced since the previous evaluation;

b) details of any certificate maintenance procedures referenced by the CMP;

c) any CMSRs produced since the previous evaluation;

d) records of the review of the CMP and CMSRs;

e) latest version of the Security Impact Analysis;

f) previous CM Audit Reports and any problem reports raised;

g) the ETR, ESR and Certification Report from the previous evaluation.

6.4 Evaluator Actions

6.4.1 The evaluator actions for a CM Audit consist of a series of checks on the following:

a) evidence of application of the certificate maintenance procedures described in the CMP;

b) clearance of previously reported problems;

c) evidence that evaluation deliverables are being maintained and that appropriate security testing is being performed on new releases of the TOE (this includes witnessing a sample of such tests where feasible);

d) sampling of the Security Impact Analysis;

e) evidence of vulnerability and threat tracking activities, neutralisation of vulnerabilities, and dissemination of appropriate information to the TOE's user community.

6.4.2 The methodology for CM Audits is described in Part II.

6.4.3 The CLEF shall document the results of the audit in a CM Audit Report, and shall raise problem reports where appropriate (any problems the CLEF intends to raise as a result of the CM Audit shall be identified to the DSA at the conclusion of the visit to the development site). The CB shall review CMARs to ensure consistency between CLEFs.

6.5 Corrective Action

6.5.1 Acceptable corrective action must be taken by the appropriate party, and evidence supplied, within timescales that are agreed between the CB, sponsor, DSA and developer. The form the evidence should take, and how it should be checked, will be stipulated by the CLEF (in agreement with the CB) on a case-by-case basis.

Chapter 7 CMS Approval of TOE Versions

7.1 Introduction

7.1.1 This chapter describes the significance of, and requirements for, CMS Approval of versions of the TOE produced between the scheduled CMS re-evaluations.

7.2 Significance of CMS Approval

7.2.1 CMS Approval of a version of a TOE is not equivalent to saying that the TOE is *certified* to the target level of assurance. It *does* mean, however, that there is an appropriate level of confidence that the assurance in the TOE has been maintained.

7.2.2 What this means in practice is that a re-evaluation of that version of the TOE *might* reveal problems that indicate that the TOE does not satisfy its security target. The risk that such problems have been introduced is, however, reduced to an acceptable level, because of the activities performed by the DSA and the CM Audits by the CLEF which provide confirmation that these activities are being performed.

7.2.3 To all intents and purposes, therefore, a CMS Approved version of a TOE should be considered to have the same level of assurance as the certified version.

7.3 Requirements for CMS Approval

7.3.1 CMS Approval can only be granted once the TOE has full membership of the CMS, which implies:

a) a version of the TOE has already been certified;

b) the CMP has been approved by the CB;

c) a DSA has been appointed for the TOE;

d) no major non-compliances with the CMP or CMS have been reported.

7.3.2 Any version of the TOE that is produced whilst the TOE has full membership of the CMS qualifies as *CMS Approved*, providing the changes to the TOE are not outside the scope of such approval (see below). The sponsor is responsible for notifying the CB of the versions of the TOE which qualify as *CMS Approved*. In the case of products, the UKSP 06 entry will state which versions of the TOE are *CMS Approved*.

7.3.3 The CB may choose to withhold approval of new versions of the TOE in the event of any significant non-compliance with the CMP or the CMS requirements, or the discovery of an exploitable vulnerability in the TOE, until appropriate corrective action is taken. In such an event the TOE is (in effect) temporarily suspended from the CMS. However, formal suspension will only occur if there is continued non-compliance with the CMP or CMS requirements.

7.3.4 Only in exceptional circumstances (e.g. discovery of an exploitable vulnerability that cannot be countered by procedural or other means) will there be retrospective removal of CMS Approved status from a particular version of a TOE.

7.4 Scope of CMS Approval

7.4.1 CMS Approval only provides assurance that the new version of the TOE continues to meet the security target against which it was previously evaluated. Thus, for example, a product vendor could not claim that CMS Approval extended to security features introduced since the previous evaluation (or re-evaluation). Similarly, CMS Approval cannot be granted in the event of a major change to the TOE architecture affecting the way the security enforcing components provide the security target SEFs.

7.4.2 The DSA must use the results of the Security Impact Analysis to determine whether changes to the TOE fall within the scope of CMS Approval (see Part II). If a change to the

TOE falls outside the scope of CMS Approval, then the new version must either undergo a CMS re-evaluation or be designated as uncertified.

7.4.3 The detailed rules governing what type of changes fall within the scope of CMS Approval are on the evaluation criteria. However, at all evaluation levels, significant changes to the security target or architectural design-level security enforcing components by default fall outside the scope of CMS Approval.

7.4.4 Changes that would otherwise be outside the scope of CMS Approval *can* nonetheless be considered to be within scope if the following criteria are met:

a) implementation of the change is covered by a well-defined procedure, such that the evaluators can check its application during each CM Audit;

b) application of the procedure has been validated at least once by a CLEF (whether in the original evaluation, a CMS re-evaluation, or a CM Audit);

c) the change type is detailed in the CMP (see paragraph 3.2.15).

7.4.5 For example, it is permissible (subject to the rules stated in paragraph 7.4.9 below) for the security target to change in order to ensure that the TOE remains effective in its environment, e.g. introducing new environmental assumptions to counter a newly discovered vulnerability. Such changes will be covered by the examination of the list of known vulnerabilities during the CM Audits and CMS re-evaluations.

7.4.6 Where the threat itself is changing, such that the security target is required to change more frequently than the scheduled CMS re-evaluations, the changes can only be covered by CMS Approval if the evaluators have assessed the ability of the developer to track the threat and implement appropriate countermeasures.

7.4.7 A similar example is that of changes to the TOE platform, which constitute a change to the TOE environment and hence to the security target. CMS Approval *can* be extended to

include different platforms in the following circumstances:

a) the developer's testing on a one platform (sometimes referred to as the *primary* platform) has been subject to an evaluation or a re-evaluation.

b) changes to the platform do not, following the CMS re-evaluation methodology described in Part II, require penetration testing (these other platforms are sometimes referred to as *secondary* platforms).

7.4.8 (*Primary* and *secondary* platforms normally share the same processor architecture.)

7.4.9 The following types of change to the security target cannot, under any circumstances, be covered by CMS Approval:

a) changes to security objectives;

b) new (high-level) threats[3];

c) significant changes in the TOE environment;[4]

d) increases in the evaluation level;

e) additional or significantly modified security features[5].

---

[3]If a new threat is included, a decision must be made as to whether it is simply a further instantiation of an existing threat (which would be within the scope of CMS Approval), or whether it is an entirely new threat (which would be outside the scope of CMS Approval).

[4]This does not preclude a system accreditor choosing to accept changes to the system environment whilst waiving the requirement for certification of such changes.

[5]This rule applies mainly to products. In the case of systems, limited changes to the system security requirements may be accepted as within scope, provided the resultant changes to the TOE design do not fall

7.4.10 Such changes must therefore be subject to a CMS re-evaluation.

outside the scope of CMS Approval. The CB will advise sponsors and accreditors on a case-by-case basis.

Chapter 8 TOEs Without Full Membership Of The CMS

8.1 Introduction

8.1.1 This chapter defines the requirements imposed by the CMS on TOEs which do not have full membership of the CMS, and in particular where there is no formal commitment on the part of the sponsor to maintaining the certificate.

8.2 Statement of Commitment to Certificate Maintenance

8.2.1 For TOEs entering the UK Scheme following the introduction of the CMS, the sponsor is required to formally state, at the Task Startup Meeting (TSM) whether or not the TOE is to be maintained under the CMS.

8.2.2 This statement does not preclude a sponsor:

a) committing to re-evaluate the TOE at some future date according to a re-evaluation method acceptable under the UK Scheme;

b) applying for the TOE to gain full membership of the CMS at a later date.

8.2.3 A sponsor choosing the first option may still elect to document the commitment to future re-evaluation of the TOE in a CMP, and submit this for approval by the CB. This may be appropriate if the sponsor wishes to gain approval of the re-evaluation policy, and recognition of the commitment. However, in such a case the TOE would not have full membership of the CMS since there would be no DSA appointed: hence there will be no periodic CM Audits, and no CMS Approval of versions of the TOE produced between the evaluations.

8.3 Certificate Validity

8.3.1 The CMS requires that a TOE continues to be effective in its intended environment. This

may mean that a TOE has to change in response to changes within its environment, such as the discovery of previously unknown vulnerabilities in the TOE.

8.3.2 Sponsors should therefore be aware that if they do not commit to maintaining the TOE under the CMS (whether or not it was certified before introduction of the CMS), there is a risk of the certificate being invalidated (and hence withdrawn) should the CB become aware of new vulnerabilities which affect the certified version of the TOE. In such cases, the sponsor will normally be required to provide evidence, submitted for evaluation by a CLEF, that the vulnerability is either irrelevant to the TOE, or has been removed or neutralised in a subsequent version of the TOE.

Annex B Applying the CMS to Systems and Composite TOEs

B.1 Introduction

B.1.1 This annex provides an interpretation of how the CMS should be applied to systems, particularly HMG systems following standards such as [MEMO7] and [MEMO11], and composite TOEs. Some of the guidance presented in Annex B (guidance to sponsors) is also likely to be relevant.

B.2 Certificate Maintenance Plans for Systems

B.2.1 Under the CMS, the sponsor is responsible for the CMP. In the case of a system, the accreditor and the project office responsible for procurement are likely to have a major say in the certificate maintenance policy, and in the appointment of key roles such as the DSA.

B.2.2 For systems following [MEMO7], it is expected that the Configuration Management Board (CMB) will play a significant role in providing input to, and monitoring the implementation of, the CMP. (The Accreditation authority designates the CMB as the formal authority for approval of all proposed modifications and enhancements to the system.)

B.2.3 Some of the information required in the system CMP could be referenced out to the Configuration Management Plan for the system, particularly the procedural aspects relevant to certificate maintenance. The system CMP should detail or reference the procedures for reviewing change requests and how this fits in with the process of producing the Security Impact Analysis. This information should be included in the *TOE Maintenance Procedures* section of the CMP.

B.2.4 Where Commercial Off The Shelf (COTS) products are used, the system CMP must (in the *TOE Maintenance Procedures* section) define the policy for accepting or rejecting upgrades to those products. It must also define the policy for the inclusion of additional COTS products in the system, and for the exchange of one COTS product for another.

B.3 DSA Role for Systems

B.3.1 As stated in [MEMO7] (section 3.5), the developers of the TOE may not be available in the maintenance phase. For simple systems, it is possible that system maintenance is carried out by the user community. However, [MEMO7] does require the *availability of adequate technical resources (especially relating to security)* for the maintenance phase. For a system under the CMS, the DSA will have a key role to play in advising the CMB on the impact of changes on security.

B.3.2 [MEMO11] introduces the concept of a Security Assurance Coordinator (SAC). The SAC chairs the Security Working Group (SWG), which is responsible for monitoring the security in the development of the system, dealing with security issues and reporting them to the SAC. Therefore, the SAC may be the ideal person to appoint as DSA, particularly if it is the same individual as was involved in the initial evaluation. A SAC must, of course, have the required familiarity with the TOE security target and its architecture in order to be acceptable as a DSA.

B.3.3 [MEMO11] states that one of the responsibilities of an accreditor is to ensure that the SAC is monitoring the security aspects of the project in accordance with the Accreditor(s) mandate. The accreditor is responsible for appointing the members of the SWG, and hence is likely to have a major say in appointing the DSA for a system.

B.4 Composite TOEs

B.4.1 A *composite TOE* is a TOE which contains a number of components, at least one of which is a certified component (that is, a product or system that has previously been certified, but which is being used as a component of a larger TOE) (see [UKSP05-3] Chapter 11). Typically, this may be a system which comprises one or more certified COTS products with (possibly) bespoke applications.

B.4.2 In order for such a TOE to have full membership of the CMS, all components must also have full membership of the CMS. However, in the case of a system it is possible that an accreditor could accept the risk of the system having 'partial' membership of the CMS,

whereby some, but not all, of the components requiring certification have full membership of the CMS. The other components could be COTS products that were:

a) certified under the UK Scheme, but where there is no commitment on the part of the product vendor to certificate maintenance under the CMS;

b) certified by another jurisdiction, but subject to a mutual recognition agreement;

c) evaluated in the US, and subject to the US RAMP process;

d) only evaluated as part of the system evaluation.

B.4.3 Any changes to a TOE component that does not have full membership of the CMS must be re-evaluated according to a non-CMS re-evaluation methodology approved by the CB.

B.4.4 The CB will advise on the acceptability of the CMP for composite TOEs on a case-by-case basis.

Annex C Guidance to Sponsors and Accreditors

C.1 Introduction

C.1.1 This annex provides guidance to sponsors of CMS re-evaluations who have a responsibility for producing the Certificate Maintenance Plan, which defines, *inter alia*, the CMS re-evaluation schedule for the TOE. Some of this guidance is also of relevance to accreditors, who need to decide when to demand a CMS re-evaluation of a system for which they are responsible, in order to reduce the risk to security to an acceptable level.

C.1.2 Guidance is also given on commercial aspects, i.e. arrangements with a CLEF.

C.2 Scheduling CMS Re-evaluations

C.2.1 The CMS requirements recognise that it is not feasible to re-evaluate every release of a TOE. One of the important decisions a sponsor or accreditor must make is how frequently a TOE should be submitted for CMS re-evaluation by a CLEF. This depends on the frequency that changes will be made to the TOE.

C.2.2 The CMS defines a minimum period of 1 year between evaluations (assuming there are no problems triggering an earlier re-evaluation). The maximum period that may be defined in a CMP is 3 years, although this may be extended at a later date if the TOE has been subject to minimal change over the period. Broadly speaking, there are three categories of TOE:

a) TOEs for which there are several releases per year (for example, virus scanners): CMS re-evaluations should be planned annually;

b) TOEs for which there is a release every year (on average): CMS re-evaluations should be planned every 1_ to 2_ years;

c) TOEs that will be subject to, at most, minor security relevant changes over the 3 year period: CMS re-evaluations should be planned every 2_ to 3 years.

C.2.3 It should be stressed that the above are only guidelines. The decision of the sponsor or accreditor is likely to be influenced by the nature of the changes to the TOE. For example, if there are plans to include significant new security enforcing or security relevant functionality (indicating significant changes to the security target or TOE architecture), then it would be appropriate to target that version for CMS re-evaluation rather than an earlier (or later) version.

C.2.4 A sponsor or accreditor should seek advice from the CB if in doubt as to the frequency appropriate for the TOE.

C.3 Certificate Maintenance Plans

C.3.1 Although the sponsor is responsible for production of the CMP (because it represents a commitment to maintenance of the certificate which, ultimately, must be paid for), much of the input is provided by other parties, namely the DSA and the CLEF responsible for the most recent evaluation of the TOE:

a) the DSA will (with support from the developer) need to provide the plans for TOE releases, and describe the procedures that apply to maintenance of the certificate;

b) either the CLEF or the DSA will be required to produce the Categorisation Report.

C.3.2 Other aspects of the plan should be self-explanatory, requiring a presentation of known facts such as the TOE evaluation history. Other documents may be referenced for the required information, if desired.

C.3.3 The level of detail expected in the TOE description is equivalent to that which is given in the Certification Report. It may be useful to provide further information if the sponsor intends to use the CMP as the basis for obtaining quotes from other CLEFs for a CMS re-evaluation. As a general rule of thumb, a description of up to a page, incorporating an overview of the TOE architecture as well as its functionality, may be appropriate in these

cases.

C.3.4 It is expected that, in most cases, the CMP will be subject to change over the period to the next CMS re-evaluation. This is particularly true of the plans for new releases of the TOE, since the sponsor will often not be able to predict (or, at least, predict *accurately*) the type and extent of changes that will be made to the TOE. The CMS therefore allows the sponsor to modify the CMP, provided the proposed changes to the CMP are submitted to the CLEF and CB for review and approval.

C.3.5 Guidance on the CMS re-evaluation schedule is given in the previous section. The sponsor should always consult the CB before proposing a CM Audit schedule that differs from the default (i.e. annual) schedule.

C.4 Commercial Arrangements With CLEFs

Maintenance Costs and Timescales

C.4.1 The following activities will incur maintenance costs (excluding additional development costs that may be borne by the sponsor: see Part II):

a) production or review of the Categorisation Report;

b) contribution to and review of the CMP;

c) review of the CMSR;

d) CM Audits;

e) CMS re-evaluation.

C.4.2 The first three are each likely to require of the order of a few man-days of CLEF effort. The CM Audit will typically be of 1-2 days duration, to which must be added time for preparation and reporting.

C.4.3 CMS re-evaluations will vary significantly in terms of costs and timescales, depending on the size and complexity of the TOE, the target evaluation level, and the type and extent of changes made. Some CMS re-evaluations may only require a CLEF to examine the Security Impact Analysis and associated test evidence, and will therefore not require a significant amount of CLEF effort. Where the TOE has been subject to significant changes (e.g. to the security target or the design), it is estimated that the cost of CMS re-evaluations will be significantly lower than re-evaluations previously carried out under the UK Scheme (in some cases by up to 50%).

C.4.4 Note that where the development environment is outside the UK, it may be useful to explore the possibility of the CLEF performing CM Audits via other means such as fax, letter, email, telephone or video conference. Such an approach must, however, be acceptable to the CB, and must ensure that the evaluators would be able to gain sufficient information to provide the required level of assurance. The development site must have been visited in a previous evaluation.

C.4.5 The sponsor should carefully consider the possibility of the CMS re-evaluation being performed concurrently with the development, as this should greatly reduce the delay between the release of a new version of a TOE and the issue of the updated certificate. As with concurrent evaluations, there is of course a risk of changes to the TOE or its deliverables requiring re-work by the evaluators.

C.4.6 Sponsors should also be aware of the impact of the TOE lifecycle on costs; these are covered in Part II.

C.4.7 Sponsors need to consider when budgeting whether planned or requested changes are likely to be outside the scope of CMS Approval, thus requiring the next CMS re-evaluation to be brought forward if the version of the TOE concerned is not to have an uncertified status. It should be quite possible to accommodate additional CM Audits within the sponsor's budget (which should allow for such events as contingency). However, a CMS re-evaluation could

result in costs which cannot be readily accommodated. Therefore, sponsors need to strike an appropriate balance, noting that the longer the next CMS re-evaluation is delayed, the greater the risk of changes being made or required that are outside the scope of CMS Approval. Advice should be sought from the CB or a CLEF, if required.

Guidance on Arrangements with CLEFs

C.4.8 Production (or review) of the Categorisation Report and review of the CMP can be handled as an extension of the evaluation that forms the baseline for certificate maintenance and, as such, can be covered by the contract for that evaluation. Such an arrangement may help to bring forward the date by which a TOE may be granted full membership of the CMS.

C.4.9 CM Audits will be carried out with a frequency determined by the CMP. These will often be carried out by the CLEF that performs the next CMS re-evaluation, although the CMS does not preclude a sponsor from contracting a different CLEF to do the work. If different CLEFs are involved, however, sponsors should note that both CLEFs must have access to the reports of the results of any previous CLEF's work, including any relevant previous ETRs and CMARs.

C.4.10 It may be appropriate to maintain an open arrangement with a CLEF (subject to an appropriate limit of mandays of consultancy) in order to be able to discuss issues concerning potential re-evaluation and the impact of changes with a CLEF that has experience of evaluating (or re-evaluating) the TOE.

Requesting Tenders for CMS Re-evaluations

C.4.11 Although it is likely that the CLEF that performed the original evaluation will have a technical advantage over other CLEFs, it is the intent of the CMS that a sponsor be able to change CLEFs if they so desire. CLEFs wishing to bid for a CMS re-evaluation are likely to require the following information as a minimum:

a) the CMP, including the Categorisation Report;

b) the Security Impact Analysis, or a summary of its content which includes a description of major changes to the TOE since the last evaluation, the numbers of components changed in each category, and the representational level of such changes.

C.4.12 A CLEF may also require access to any previous ETRs, CMARs and CMSRs, as well as the Certification Report.

INDEX