



CSIA CLAIMS TESTED MARK SCHEME

TEST LABORATORY GUIDE

Issued v2.3.0

4 May 2007

© Crown Copyright 2007 – All Rights Reserved

Reproduction is authorised provided the document is copied in its entirety

Central Sponsor for Information Assurance

FOREWORD

The CSIA (Central Sponsor for Information Assurance) Claims Tested Mark Scheme has been established to test the validity of claims of security functionality in information system (IS) products and services, in which information assurance (IA) is a major consideration.

This document specifies the requirements on the appointment and conduct of tests by Test Laboratories under the Scheme.

H Mattinson
Senior Executive
CSIA Claims Tested Mark

In the event of any questions concerning this publication, or for further information, please consult the Secretariat of the Scheme:

Address: Central Sponsor for Information Assurance, Cabinet Office. 26 Whitehall, London, SW1A 2WH

Telephone: 020 7276 5029

Facsimile: 020 7276 5096

E-mail: secretariat@cctmark.gov.uk

Website: www.cctmark.gov.uk

DOCUMENT HISTORY

Amendments to this document will be published as and when required during the Pilot phase of the Scheme. All major changes made since the last update of the document will be outlined in the document history record.

Issue	Description of Changes	Date Issued
1.0	First version of CCT Mark Test Laboratory Guide issued	22/02/05
1.1.0	<p>Second version of CCT Mark Test Laboratory Guide issued at the end of Stage 1 of the Pilot, to all Stage 1 Test Laboratories and Stage 2 applicant Test Laboratories.</p> <p>Major changes concern:</p> <ul style="list-style-type: none"> • Full Appointment Requirements (Sections I and III); • Claims Testing Categories for Generalist and Specialist Testing (Section 1 and new Appendix D); • Claims Test Procedure (Section IV); • Claims Test Method (new Appendix B); • CCT Mark Test Report (Appendix C). 	22/08/05
2.0.0	<p>Third version of the CCT Mark Test Laboratory Guide published at the start of Stage 2 of the Pilot.</p> <p>This Guide replaces the guidance issued for Stage 1 in version 1.0, and should be used for all new applications received in Stage 2.</p> <p>See also the revised Vendor Guide (v2.0.0) and Scheme Description (v2.0.0) which have also been updated and replace the versions published for Stage 1.</p>	08/09/05
2.1.0	<p>Fourth version of the CCT Mark Test Laboratory Guide published during Stage 2 of the Pilot.</p> <p>Two new paragraphs were added. 16.2.6.7- 16.2.6.8 relates to requirements when an IA Service is tested.</p>	17/10/05

Issue	Description of Changes	Date Issued
2.2.0	<p>Fifth version of the CCT Mark Test Laboratory Guide published during Stage 2 of the Pilot.</p> <p>Validation of existing assurance certificates specified in the ICD:</p> <ul style="list-style-type: none"> • New paragraph 17.2.5 inserted • Minor change made to first sentence of paragraph 17.7.1 • Appendix C (Test Report Format) - new section 3.4 (Validation of Existing Assurance Certificates) <p>List of specialist testing capabilities (Appendix D) amended and new hardware testing category added.</p> <p>Duplication of the detailed process in the Scheme Description, Test Laboratory Guide and Vendor Guide removed.</p>	05/12/05
2.3.0	<p>Sixth version of the CCT Mark Test Laboratory Guide.</p> <p>Incorporates and formalises the changes and further guidance which have been implemented during 2006 and 2007 for all applications registered and processed by the CCT Mark Scheme.</p> <p>Includes the Statement of Clarification notices SOC2006/01 (Cryptography), SOC2006/02 (Web ICDs) and SOC2006/03 (Test Report Summaries).</p> <p>All paragraphs about the UKAS accreditation and assessment process are now in section 15, rather than in different parts of the Guide.</p> <p>Guidelines on the requirements for testing services have been added to section 18, and Appendices D-E.</p> <p>Updated format and guidance for the Test Report and Test Report Summary in Appendices D-E.</p>	04/05/07

CONTENTS

DOCUMENT HISTORY	3
I OVERVIEW OF TEST LABORATORY APPOINTMENTS	7
1 Introduction.....	7
2 Document Changes	8
3 Test Laboratory Appointment.....	8
4 Specialised Testing Methods and Equipment.....	8
5 Terminology	9
6 Annual Registration Fees.....	9
II SETTING UP A CCT MARK TEST LABORATORY	11
7 Basic Requirements and Criteria	11
8 Quality and Management	11
8.1 Management Objectives.....	11
8.2 The Quality Manual.....	12
9 Staff Qualifications and Training.....	12
9.1 Objectives	12
9.2 Tester Status.....	12
III APPOINTMENT AND ASSESSMENT FOR TEST LABORATORIES ...	13
10 Introduction	13
11 Granting of a Full Appointment	13
12 Granting of a Provisional Appointment.....	14
13 Termination of Appointment	15
14 Disputes	16
15 UKAS Accreditation	16
15.1 UKAS Accreditation Application	16
15.2 Schedule of Accreditation	16

15.3	Maintenance of UKAS Accreditation	17
15.4	UKAS Fees	17
15.5	Conduct of UKAS Assessments	17
15.6	The Trial Test	18
15.7	UKAS Surveillance and Reassessment	18
15.8	UKAS Complaints	19
IV	TEST LABORATORY OPERATION	20
16	Introduction	20
17	Commercial Impartiality	20
18	Claims Test Procedure	20
18.1	Pre-Requisites to initiate Claims Testing	20
18.2	Test Procedures	21
18.3	Test Equipment	22
18.4	Sub-contracting of Testing	22
18.5	Conduct of Testing	23
18.6	Test Environment	24
18.7	Test Reports	25
18.8	Test Suspension or Termination	26
APPENDIX A	TRIAL TEST	28
APPENDIX B	GENERIC CLAIMS TEST METHOD	30
APPENDIX C	CCT MARK TEST REPORT FORMAT	33
APPENDIX D	CCT MARK TEST REPORT SUMMARY FORMAT	40
APPENDIX E	CLAIMS TESTING CATEGORIES	45
APPENDIX F	46
	GLOSSARY AND TERMINOLOGY	46
	REFERENCES	49
	ABBREVIATIONS	50

I OVERVIEW OF TEST LABORATORY APPOINTMENTS

1 Introduction

- 1.1 The CSIA Claims Tested (CCT) Mark scheme (referred to as the “Scheme” in this document) was established in January 2005 by Her Majesty’s Government (HMG) to test the validity of security functionality in information systems (IS) products and services, in which information assurance (IA) is a major consideration.
- 1.2 The objective of the Scheme is to meet the needs of Government and Industry for cost effective and efficient functionality claims testing of IS Products and IS Services. The Scheme provides a basic level of assurance to these products and services, for purchasers and users. This level of assurance is broadly equivalent to Common Criteria EAL2. The Scheme provides the public sector with confidence in the claims made by Vendors about the functionality of their information security products and services.
- 1.3 All references to the Scheme in this document include the Pilot.
- 1.4 Claims testing under the Scheme is independent testing of the security functionality claims of IS Products and Services by a Test Laboratory accredited by the UK Accreditation Service (UKAS), and appointed by the Scheme. This provides the users of such IS Products and Services with confidence that the Vendor’s security functionality claims have been validated.
- 1.5 This document sets out:
 - 1.5.1 the objectives, assessment criteria and requirements for evidence for a company wishing to be appointed as a Test Laboratory under the Scheme;
 - 1.5.2 the procedural requirements for the conduct of testing performed by a Test Laboratory.
- 1.6 A description of the Scheme, the procedures, management, and operation of the Scheme is included in the “CSIA Claims Tested Mark Scheme – Description of the Scheme” document (“Scheme Description”).
- 1.7 Further details about the responsibilities of Vendors and the process for registering and acceptance of applications to the Scheme, and award of the CCT Mark are included in the “CSIA Claims Tested Mark Scheme – Vendor Guide”.

2 Document Changes

- 2.1 All the Scheme documents (including this Guide) will be subject to review and amendment during the Pilot phase of the Scheme. Changes to the Scheme documents will be published on the Scheme website and those participating in the Scheme will be notified at least 20 business days before the changes in the documents take effect.

3 Test Laboratory Appointment

- 3.1 Testing under the Scheme must be performed by Test Laboratories which are based in the UK and are appointed by CSIA.
- 3.2 Appointments are either Full or Provisional:
 - 3.2.1 a Full Appointment is granted for a period of 1 calendar year, subject to accreditation by UKAS. The Full Appointment can be renewed subject to confirmation that the Test Laboratory's UKAS accreditation has been maintained.
 - 3.2.2 In exceptional circumstances and as agreed by the Decision Authority and Technical Review Body, a Provisional Appointment (see Section III) may be granted by the Scheme to allow a Trial Test (See Appendix A) to be performed and monitored to enable the UK Accreditation Service (UKAS) to accredit against ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B) in this Guide (see section III, Appendices A and B).
- 3.3 Both Full and Provisional Appointments are subject to the terms and conditions in the Test Laboratory Agreement (the TL Agreement) between Cabinet Office (through CSIA) and the Test Laboratory. The appointment will only be confirmed when both the Test Laboratory and CSIA have signed the TL Agreement. Appointments will specify the category of claims testing (see Appendix E) which the Test Laboratory has been appointed to undertake.

4 Specialised Testing Methods and Equipment

- 4.1 Several technologies require specialised testing methods and equipment. The specialist testing categories identified for the CCT Mark Scheme are listed in Appendix E. The Test Methods for the specialist testing categories (See Appendix E) will be approved by CESG during the ISO/IEC 17025 accreditation process. Enquiries about specialist test methods should be directed to iacs@cesg.gsi.gov.uk.
- 4.2 Test Laboratories wishing to test IS Products or Services containing these technologies will need to demonstrate or provide evidence of particular competency in these areas during the UKAS assessment and accreditation process.

- 4.3 Evidence of specialist testing capabilities will also separately be assessed by the Technical Review Body and Decision Authority, when an application is received for specialist testing capabilities. This will be done before the Test Laboratory's appointment to the Scheme for specialist testing capabilities can be confirmed.
- 4.4 The Scheme may appoint a Test Laboratory to undertake specialist testing, subject to the Test Laboratory obtaining UKAS accreditation for claims testing for specific specialist testing categories.
- 4.5 As new technologies are introduced, the Scheme Executive on advice from the Technical Review Body will confirm whether the new technology has been designated as requiring specialist testing. A list of technologies requiring specialist testing will be published on the Scheme website and is also included in Appendix E of this document. A list of Test Laboratories appointed to undertake such testing will also be published on the Scheme website.
- 4.6 Any cryptographic functionality tested under the Scheme is not approved for use to protect UK government information attracting a Protective Marking (ie. classified).
- 4.7 If the Vendor has a requirement to test specific cryptographic algorithms for their product or service, they should apply to the appropriate assurance schemes such as CAPS or FIPS. Further information on CAPS is at: www.cesg.gov.uk and on FIPS at: <http://csrc.nist.gov/cryptval/>.
- 4.8 If the Vendor requires a certificate which is recognised outside the UK, then an evaluation under Common Criteria might be more appropriate. More information about Common Criteria can be found at www.commoncriteriaportal.org/ and www.cesg.gov.uk

5 Terminology

- 5.1 The terminology used in relation to the appointment process follows that of "The Conduct of UKAS Laboratory Assessments" ("UKAS Assessments Conduct"). Where the term 'Vendor' is used to refer to the person or organisation that requests a test, this equates to the 'Customer' in UKAS terms. Further information is at www.ukas.org.

6 Annual Registration Fees

- 6.1 The Scheme requires the Test Laboratory to pay an annual registration fee on the initial granting of either a Full or Provisional Appointment and on the renewal of the Full or Provisional Appointments. This fee will be set and reviewed annually by CSIA.
- 6.2 There shall be no refund of all or part of the annual registration fee should the Appointment as a CCT Mark Test Laboratory be withdrawn,

or the Provisional Appointment not be successful in being confirmed as a Full Appointment.

- 6.3 The registration fee paid for the Provisional Appointment is valid should the Test Laboratory be accepted as a Full Appointment, until the Full Appointment is due for renewal.

II SETTING UP A CCT MARK TEST LABORATORY

7 Basic Requirements and Criteria

- 7.1 A Test Laboratory must be accredited as a testing laboratory against ISO/IEC17025:2005 by UKAS in accordance with the current Standards [D,E] and the appropriate Claims Test Method (see Appendix B) for the generalist and any specialist claims testing categories for which the Test Laboratory has applied.
- 7.2 The CCT Mark Scheme requires Test Laboratories to be accredited against ISO/IEC 17025:2005 to confirm the competence of the test laboratory, and that there is a quality management system in place which meets the requirements of ISO/IEC 17025:2005. The standard specifies the general requirements for the competence to carry out tests and/or calibrations, including sampling. It covers testing and calibration performed using standard methods, non-standard methods, and laboratory-developed methods. The Test Laboratory should develop their management system for quality, administrative and technical operations against this standard as to gain ISO/IEC 17025 accreditation.
- 7.3 In order to obtain UKAS accreditation for claims testing, a Test Laboratory must apply to UKAS who will undertake an assessment as described in section III, and may require the Test Laboratory to complete an appropriate level trial test to demonstrate that:
 - 7.3.1 the testers are technically competent;
 - 7.3.2 the management, administrative and quality management system are adequate and comply with the requirements of the Scheme in accordance with UKAS accreditation.
- 7.4 The Test Laboratory shall also complete a trial test to demonstrate that the Claims Test Methods (see Appendix B), are valid and appropriate to satisfy the requirements for validating the security functionality claims in the IA Claims Document.

8 Quality and Management

8.1 Management Objectives

- 8.1.1 The organisational structure of a Test Laboratory must provide a sufficiently high standard of quality in all aspects of its work. This must be reflected in the Quality Management System, including Quality Manual and Quality procedures, which covers all management and technical aspects related to claims testing.
- 8.1.2 Each Test Laboratory shall appoint an individual with appropriate authority and seniority to act as point of contact with the Scheme Secretariat and CSIA.

8.2 The Quality Manual

- 8.2.1 A Test Laboratory must possess its own Quality Manual that should conform to UKAS requirements and those of ISO/IEC Guide 17025.

9 Staff Qualifications and Training

9.1 Objectives

- 9.1.1 The training of testers has the objective of producing Qualified Testers who:
 - 9.1.1.1. understand the notion and principles of information assurance and security;
 - 9.1.1.2. can conduct tests and otherwise validate claims to assess the compliance of a product or service with a set of claims;
 - 9.1.1.3. can manage a Claims Test team and any associated specialist testing sub-contractors.

9.2 Tester Status

- 9.2.1 In practice, individual testers will have differing levels of expertise. The Scheme recognises two levels of qualification:
 - 9.2.1.1. Trainee Testers, i.e. testers who have successfully completed an initial training programme;
 - 9.2.1.2. Qualified Testers, i.e. Trainee Testers who have successfully completed a Claims Test under the supervision of a Qualified Tester, and are deemed by the Test Laboratory to be capable of undertaking further Claims Tests without supervision.

III APPOINTMENT AND ASSESSMENT FOR TEST LABORATORIES

10 Introduction

- 10.1 Test Laboratories are appointed by CSIA to operate under the Scheme. The approval of a Full Appointment is subject to the Test Laboratory being accredited by UKAS against ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B).
- 10.2 It should be noted that appointment to the Scheme does not imply any guarantee of business.

11 Granting of a Full Appointment

- 11.1 The Test Laboratory should apply to the Scheme Secretariat for a Full Appointment. The Test Laboratory should submit the following to the Scheme Secretariat:
 - 11.1.1 CCT Mark application form for a full appointment;
 - 11.1.2 Registration Fee for CCT Mark Test Laboratory;
 - 11.1.3 Confirmation of accreditation by UKAS against ISO/IEC:2005 and the appropriate Claims Test Method (see Appendix B).
- 11.2 The Scheme Secretariat will register the application, as long as the application form (including confirmation of UKAS accreditation for claims testing) and registration fee have been submitted by the Test Laboratory. Details of how the registration fee can be paid are available from the Scheme Secretariat and are published on the Scheme website.
- 11.3 The Scheme Secretariat will also:
 - 11.3.1 prepare the TL Agreement based on the information provided in the application form, and will arrange for two copies of this to be signed by CSIA on behalf of the Minister for the Cabinet Office; and
 - 11.3.2 send the two signed copies of the TL Agreement to the Test Laboratory. The Test Laboratory should sign both copies and return one of these to the Scheme Secretariat within 10 business days of the date the signed TL Agreements were received from the Scheme Secretariat.
- 11.4 The Test Laboratory's appointment will be confirmed by the Scheme Secretariat when the TL Agreement has been signed by both parties.
- 11.5 If the Test Laboratory has completed the Provisional Appointment and been accepted as a Full Appointment, the registration fee already paid for the Provisional Appointment is valid for the remainder of the registration period until the Full Appointment is due for renewal.

- 11.6 A Full Appointment lasts for 1 calendar year and will be renewed by the Scheme Secretariat on receipt of confirmation that accreditation by UKAS for claims testing has been maintained, and payment of the registration fee.
- 11.7 If the Test Laboratory is appointed as a Provisional Appointment and subsequently as a Full Appointment before the end of the Provisional Appointment period, the Test Laboratory will need to renew their Full Appointment at the end of this period.
- 11.8 Details of the Test Laboratories who have been granted a Full Appointment will be published on the Scheme website.

12 Granting of a Provisional Appointment

- 12.1 Test Laboratories that are not already accredited against ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B) should make a formal application to UKAS. Further information on the UKAS accreditation and assessment process is outlined later in this section.
- 12.2 The Test Laboratory may apply to the Scheme Secretariat for a Provisional Appointment, subject to the following:
 - 12.2.1 CCT Mark Test Laboratory must have registered with UKAS for assessment and accreditation by UKAS against ISO/IEC17025: 2005 and the appropriate Claims Test Method (Appendix B); and
 - 12.2.2 UKAS must have completed the Initial Assessment visit to the Test Laboratory and issued a report on improvement actions to be taken to the Test Laboratory.
- 12.3 To register for a Provisional Appointment, the Test Laboratory should submit the following to the Scheme Secretariat:
 - 12.3.1 CCT Mark Test Laboratory application form for a provisional appointment;
 - 12.3.2 UKAS Summary Report from the Initial Assessment Visit;
 - 12.3.3 Registration fee.
- 12.4 The Scheme Secretariat will register the application, as long as the application form, registration fee and UKAS Summary Report have been submitted by the Test Laboratory. Details of how the registration fee can be paid are available from the Scheme Secretariat and are published on the Scheme website.
- 12.5 The Scheme Secretariat will prepare and send two copies (signed by CSIA on behalf of the Minister for the Cabinet Office) of the TL

Agreement to the Test Laboratory for them to sign and return one signed copy to the Scheme Secretariat.

- 12.6 If the application is accepted, then the applicant company (Test Laboratory) is granted a Provisional Appointment by the Scheme to undertake a trial test. The Test Laboratory's Provisional Appointment will be confirmed by the Scheme Secretariat when the TL Agreement has been signed by both parties.
- 12.7 The applicant company should only undertake a trial test for one product or service during the Provisional Appointment period.
- 12.8 The Test Report produced from a trial test will be recognised by the Scheme and processed in the same way as a Test Report from a fully accredited Test Laboratory, provided that the Test Laboratory carries out claims testing according to the requirements for the Scheme and UKAS accreditation.
- 12.9 The Test Laboratory must gain accreditation by UKAS against ISO 17025:2005 and the appropriate Claims Test Method (see Appendix B) within twelve months of being granted a Provisional Appointment to the CCT Mark Scheme.

13 Termination of Appointment

- 13.1 CSIA may terminate the Test Laboratory's appointment immediately or with notice in accordance with the terms of the TL Agreement with CSIA. CSIA will terminate the Test Laboratory appointment if the UKAS accreditation against ISO/IEC 17025:2005 and the appropriate Claims Test Method (see Appendix B) for the Test Laboratory is withdrawn or is not achieved within 12 months of the Provisional Appointment to the Scheme.
- 13.2 Exceptionally, CSIA, via the Scheme Secretariat, will give notice of intention to withdraw the appointment following receipt of evidence indicating that Claims Tests have not been performed thoroughly, resulting in IS Products or Services failing to meet stated claims.
- 13.3 At the termination of a Test Laboratory appointment, CSIA will determine whether any ongoing test work under the Scheme will be allowed to continue in order for the Test Laboratory to fulfil its contractual obligations to its Customers. Tests will not be allowed to continue if to do so would bring the Scheme into disrepute or would be against the interests of the Customer. The Test Laboratory and the relevant Vendors will be notified by the Scheme of CSIA's decision on the continuation of tests, should the appointment of the Test Laboratory be terminated.

14 Disputes

- 14.1 In the event of a dispute concerning the appointment of the Test Laboratory, the matter should be raised in writing as soon as practicable with the Scheme Senior Executive for resolution.
- 14.2 If the dispute remains unresolved within 10 business days of the matter being received in writing by the Scheme Senior Executive, the dispute can be escalated in writing to the Director of CSIA.
- 14.3 The decision of the Director of CSIA will be given in writing to the Vendor within 20 business days of the matter being received in writing by the Director of CSIA.
- 14.4 The decision of the Director of CSIA on disputes concerning the appointment of the Test Laboratory is final.

15 UKAS Accreditation

15.1 UKAS Accreditation Application

- 15.1.1 Test Laboratories which are already accredited against ISO/IEC17025:2005 will need to apply to UKAS in advance of their next visit for an Extension of Scope to their Schedule of Accreditation for the appropriate Claims Test Method (see Appendix B). In which case, the Test Laboratory must gain an Extension of Scope to their Schedule of Accreditation within twelve months of being granted a Provisional Appointment to the CCT Mark Scheme.
- 15.1.2 Test Laboratories that are not already accredited against ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B) should make a formal application to UKAS for accreditation. The Test Laboratory should complete the UKAS application form concerning the company and scope of accreditation sought (available from their website www.ukas.com) and forward this, together with a copy of the Quality Manual and the application fee, to UKAS.
- 15.1.3 UKAS will undertake an initial assessment of the quality processes and technical capability of the Testers to be used which leads to a UKAS Summary Report on what further measures are needed to meet the requirements for ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B).

15.2 Schedule of Accreditation

- 15.2.1 A Schedule of Accreditation describes the category of tests performed by a Test Laboratory. The Test Reports they produce

must meet the standards of technical competence and quality which fall within the area of UKAS accreditation.

- 15.2.2 The Schedule of Accreditation will also specify any specialist testing which the Test Laboratory has demonstrated competence in performing, and is published on the UKAS website at www.ukas.org.

15.3 Maintenance of UKAS Accreditation

- 15.3.1 Throughout its lifetime, a Test Laboratory will deal directly with UKAS on matters concerning its own accreditation. The Scheme Secretariat might be able to advise on this aspect during the early stages, but will take no formal part in UKAS assessment leading to the award of accreditation. The Scheme Secretariat will, however, keep the results of UKAS accreditation under review for appointment purposes.

15.4 UKAS Fees

- 15.4.1 UKAS charges for its accreditation services including the initial assessment, the main inspection visit, any further work undertaken as a result of the inspection and then ongoing surveillance visits to retain the ISO/IEC 17025:2005 accreditation. Further details of these fees are available from the UKAS Executive and published on the UKAS website: www.ukas.com.

15.5 Conduct of UKAS Assessments

- 15.5.1 The UKAS assessment and accreditation process is conducted as an independent activity in accordance with its standard procedures. These are described in detail in the UKAS Assessments Conduct document which should be consulted for further information. The process is concerned with the Test Laboratory procedures which have been implemented as part of the Test Laboratory's quality system and the test procedures documented in this Guide.
- 15.5.2 UKAS assessments of Test Laboratories will be conducted by fully trained UKAS assessors, who will be tasked by UKAS specifically for the purpose. One Technical Assessor from the Technical Review Body (TRB) will be selected to assess the competence of the Test Laboratory specifically to undertake testing under the Scheme.
- 15.5.3 Test Laboratory accreditation is necessary for a Full Appointment and must therefore be completed before CSIA can make its final decision on whether to grant the Full Appointment, and additionally whether the Test Laboratory has been appointed with specialist testing capabilities. In practice, the appointment

activities continue in parallel with the UKAS assessment, with the object of reducing duplication of effort as far as possible.

- 15.5.4 Formal UKAS assessment is expected to take place during the latter stages of the trial test and should be completed in one or two days.

15.6 The Trial Test

- 15.6.1 The purpose of the trial test is to provide evidence to UKAS that the Test Laboratory complies with ISO/IEC17025:2005 and the appropriate Claims Test Method (see Appendix B) in this Guide. Further details of the trial test can be found at Appendix A.
- 15.6.2 The Test Laboratory shall carry out the trial test in accordance with Appendix A, using the test method in Appendix B or an alternative documented approach. It may be expected to last about 1 calendar month and should end with submission of a test report to the Vendor and the Scheme Secretariat. The Test Report must also be submitted to UKAS to enable completion of the UKAS assessment.
- 15.6.3 UKAS will use the trial test as the basis for its assessment for Accreditation for claims testing and therefore needs to be consulted at an early stage so that its formal assessment can be scheduled to take place at suitable points in the trial test
- 15.6.4 An established test laboratory will be expected to use existing work packages to demonstrate to UKAS compliance with ISO/IEC 17025:2005 and the appropriate Claims Test Method (see Appendix B) in this Guide; this is the preferred process.

15.7 UKAS Surveillance and Reassessment

- 15.7.1 UKAS assessors will carry out surveillance visits to the Test Laboratory as specified in the UKAS Assessments Conduct document [E]. The first surveillance visit is normally carried out six months after the date of initial accreditation. Subsequent surveillance visits are carried out at yearly intervals. A full reassessment will take place three and a half years after the date of accreditation, and thereafter at four yearly intervals. Reassessments are similar to initial assessments except that the Test Laboratory's current tests replace the need for a trial test.
- 15.7.2 Surveillance visits will normally be undertaken by one or two assessors and will be completed within one or two days. Surveillance and reassessment assesses the Test Laboratory in its conduct of "real life" tests rather than a trial test and may involve the assessors accompanying the testers on a site visit.

Normally assessors will not be expected to check all the tests which are in progress at the time.

- 15.7.3 A reassessment visit will provide the opportunity for a more comprehensive re-examination of a Test Laboratory's compliance with ISO/IEC 17025:2005, and the appropriate Claims Test Method (see Appendix B).

15.8 **UKAS Complaints**

- 15.9 Complaints which concern the scope of the UKAS accreditation of the Test Laboratory for ISO/IEC 17025:2005 and the appropriate Claims Test Method (see Appendix B) can be referred to the UK Accreditation Service for consideration under the UKAS accreditation procedures. This might include, for example, customers not being satisfied with aspects of testing performed or the level of competence of the assigned evaluators. The Customer should in the first instance raise their complaint with the Test Laboratory. If the Customer does not receive a response or an unsatisfactory response, the Customer should raise the matter with UKAS and notify the Scheme Secretariat.
- 15.10 UKAS will audit the Test Laboratory's complaints procedures on each annual visit to the Test Laboratory to check compliance with ISO 17025:2005 and the appropriate Claims Test Method (see Appendix B).

IV TEST LABORATORY OPERATION

16 Introduction

- 16.1 This section outlines the responsibilities of the Test Laboratory relating to the conduct of tests under the Scheme.
- 16.2 The responsibilities of the Vendor relating to the registration and acceptance of applications to the Scheme, and the award of the CCT Mark are outlined in the Vendor Guide.

17 Commercial Impartiality

- 17.1 The Test Laboratory must demonstrate to the Scheme Secretariat and UKAS that neither the Test Laboratory, nor individual Test Laboratory staff concerned with a particular test, has a vested interest in the outcome of a test.
- 17.2 A Test Laboratory may not test the IS Product or Service of any group or division in the parent company to which it belongs.

18 Claims Test Procedure

18.1 Pre-Requisites to initiate Claims Testing

- 18.1.1 Testing under the Scheme must be performed by Test Laboratories accredited by UKAS and appointed by the Scheme (see section III for appointment of Test Laboratories).
- 18.1.2 The Test Laboratory may be asked by the Vendor to provide advice and assistance in preparing the ICD, before this is submitted to the Scheme to be accepted for claims testing. In particular, to define the test approach and to advise that the claims as worded are actually testable.
- 18.1.3 The Vendor is responsible for agreeing a contract with the Test Laboratory to undertake testing against the ICD accepted under the Scheme.
- 18.1.4 Before commencing any testing work, the Test Laboratory should await or request confirmation from the Scheme Secretariat that an Application from the Vendor for the IS Product or Service to be tested has been accepted under the Scheme, including the ICD. The Scheme Secretariat will also send to the Test Laboratory, approved by the Decision Authority, a copy of the ICD accepted for claims testing under the Scheme. Any testing work undertaken by the Test Laboratory without such confirmation is at the risk and cost of the Test Laboratory or Vendor.
- 18.1.5 For Applications to maintain the CCT Mark and which are accepted under the Scheme, the Scheme Secretariat will issue

confirmation to the Vendor and Test Laboratory whether full or partial testing should be undertaken.

- 18.1.6 Where full testing is approved by the DA, the Test Laboratory should undertake testing of all the claims in the approved ICD;
- 18.1.7 Where partial re-testing under the CCT Mark Maintenance is approved by the DA, the DA will issue confirmation to the Test Laboratory on the claims to be re-tested and tested for the first time, and the test approach for this partial re-testing as specified in the approved ICD.
- 18.1.8 The test procedures for Applications accepted as CCT Mark Maintenance Applications, for both full and partial re-testing, are the same as for new Applications accepted by the Scheme. The Vendor's Guide (Sections II and III) describe the process for registering and accepting new and CCT Mark Maintenance Applications.

18.2 Test Procedures

- 18.2.1 The Claims Testing should not exceed 20 days effort and should be completed within 6-8 weeks of the start of testing. The Executive Panel will monitor the performance of Test Laboratories in respect of all obligations.

18.2.2 IS Products

- 18.2.2.1. The Test Laboratory shall install the IS Product on all of the platforms identified in the ICD and test all functionality on all the platforms for which a claim has been made in the ICD.
- 18.2.2.2. The Test Laboratory may carry out witness testing for all of the claims on each of the platforms specified in the ICD, provided that the Test Laboratory has installed the IS Product and fully tested all the claims on at least one (set) of platforms identified in the ICD.
- 18.2.2.3. Installation and testing must be performed by either a Qualified Tester or by a Trainee Tester under the direct and constant supervision by a Qualified Tester or approved subcontractor, using the appropriate Claims Test Method and procedures approved by UKAS.

18.2.3 IS Services

- 18.2.3.1. The Test Laboratory shall test the functionality of the IS Service through running the process, witnessing service provision and verifying evidence of previous service provision to validate the outcome of the process and to validate the claims made in the ICD.

- 18.2.3.2. The Test Laboratory shall validate the claims concerning procedures, through interviewing the Vendor's staff responsible for running the IS Service and reviewing the Vendor's documented procedures to ensure that these fully support the claims made. The staff interviewed should be from the site(s) from which the IS Service is run.
- 18.2.3.3. The Test Laboratory shall also interview up to 5 Customers to validate the customer experience of using the IS Service in the previous 12 months.
- 18.2.3.4. The Test Laboratory shall produce questionnaires setting out the claims and questions to be asked, in advance of the interviews with the Vendor's staff and Customers.
- 18.2.4 If an IS Product or Service which has previously failed is subsequently corrected and re-submitted for testing under the Scheme, the full testing process shall apply. It will not be acceptable to re-use the results from the earlier tests.
- 18.2.5 The Test Laboratory shall maintain an effective quality management system (QMS) to ensure that tests against all claimed functionality are undertaken or witnessed on all platforms identified in the ICD. The QMS shall also ensure that problems, difficulties, concerns and issues are captured, recorded and reported.
- 18.2.6 The Test Laboratory shall validate the assurance certificates specified in the ICD to ensure that they relate to the exact version of the product or service being claims tested, and the certificates are still valid. The exact reference to the certificates (including a link to an Internet website) should be included in the Test Report.
- 18.2.7 The Test Laboratory should ensure that all test methods and procedures for handling test items should comply with the requirements of ISO/IEC 17025:2005, and the appropriate Claims Test Method (see Appendix B).

18.3 Test Equipment

- 18.3.1 In cases where the Test Laboratory does not have access to equipment needed to conduct all the tests, it will be acceptable for the Laboratory to use equipment on loan from the Vendor, provided that this is detailed in the report together with the location of the tests.

18.4 Sub-contracting of Testing

- 18.4.1 If the claims testing requires specialist testing, and the Test Laboratory selected by the Vendor does not have the capability to

undertake such testing, then the Test Laboratory must sub contract to one that has in order to test those aspects.

- 18.4.2 Any sub-contracted Test Laboratory must also be UKAS accredited against ISO/IEC 17025:2005 and the appropriate Claims Test Method (see Appendix B) to undertake claims testing under the Scheme. If the Test Laboratory is not UKAS accredited against ISO/IEC 17025:2005, approval for the sub-contracted test laboratory to undertake the tests must first be gained from the Scheme. Any independent contractors working at the Test Laboratory must have demonstrated competence in the relevant techniques and have a suitable level of expertise in accordance with this Guide and use the procedures documented in the Test Laboratory Quality Manual and this Guide.
- 18.4.3 The Test Laboratory should issue the full ICD approved by the DA to the sub-contractor and specify which claims should be tested by the sub contractor. The sub contractor must produce a Test Report in the format specified in this Guide for the claims for which sub-contractor is responsible for claims testing. The Sub contractor must carry out the claims testing in accordance with this Guide.

18.5 Conduct of Testing

- 18.5.1 IS Products and Services are tested against the Information Assurance Claims Document (ICD). All claims in the version of the ICD accepted under the Scheme must be tested. In some cases where the IS Product or Service contains functionality which require specialist testing as listed in Appendix E, testing of these aspects needs to be carried out by the Test Laboratory or it's sub-contractor which is accredited by UKAS against ISO/IEC 17025:2005 and the relevant specialist Claims Test Method (see Appendix B).
- 18.5.2 The Test Laboratory shall install the IS Product on at least one platform, and shall test all the claims functionality stated in the ICD on that same platform. The testing should include checking for publicly known vulnerabilities, and that the assurance certificates are for the exact versions and platforms of the IS product or IS service being tested.
- 18.5.3 Where the Test Laboratory does not have specialist equipment to complete testing of all the claims functionality on the chosen platform at their own premises, it will be acceptable for the Test Laboratory to go to the Vendor's premises to use specialist equipment provided that:
- the product is installed or the configuration verified by the Test Laboratory; and

- the test scripts and test requirements are determined by the Test Laboratory and used by the Vendor.
- 18.5.4 It will be acceptable under the Scheme for the Test Laboratory to witness Vendor testing of all of the claims in the ICD on additional platforms specified in the ICD, provided that the Test Laboratory has tested all of the claims on at least one of the platforms specified in the ICD.
- 18.5.5 Witnessing will usually involve visiting the Vendor's premises or an appropriate site to observe the tests, but in exceptional circumstances, and with the prior approval of the Scheme Secretariat, automated tests could be observed remotely via a network connection at a known location, ideally using a secure link (eg. VPN).
- 18.5.6 The required combinations of platforms for each of the claims to be used in the claims testing, including any witnessing, will be specified in the ICD and will have been previously agreed by the TRB and the rationale for this documented in the ICD. Otherwise any test deviations shall be recorded in the Test Report. An IS service must not be delivered on a different platform unknown to the tester.
- 18.5.7 Where an IS Service is to be tested, the functionality of the IS Service, as well as evidence on the provision of the service during the last 12 months must be validated against the claims. An appropriate test environment is needed which the IS Service is to protect. The process of engaging the Service Provider needs to be followed through – this is analogous to setting up a product. The purpose is to see how easy it is to get the service up and running correctly in a known state.
- 18.5.8 Some of the claims for an IS Service can be tested in the same way as for products but other claims are not so easy to test objectively. In this case it will be necessary to interview up to 5 existing customers of the IS Service about these aspects in order to form a view of the accuracy of the claim. An example may help. Suppose the claim is that a service is available for 99.999% of the time. This means that the total downtime in a year is just over 5 minutes. This can only be confirmed by examining logs kept by the Service Provider and talking to customers.

18.6 Test Environment

- 18.6.1 The test architecture and environment must be detailed in the Test Report. Wherever feasible, tests must simulate as accurately as possible the 'real world' use of the IS Product or Service , eg a networked product must be tested in a networked environment,

network traffic must be a reasonable representation of 'live' data, etc and include representative invalid traffic data.

18.7 Test Reports

- 18.7.1 The Test Laboratory should document the results of the functionality testing, validation of existing assurance certificates (as specified in the ICD) and, for IS Services, the results of validation inspections, audits and interviews, in a Test Report according to the format and procedure described in the Appendix C. The Test Laboratory shall note any problems, difficulties, concerns or issues experienced or identified in installing, configuring and using the IS Product or Service. These shall be reported in the Test Report. The Test Report should meet the ISO/IEC 17025:2005 requirements for reporting test results.
- 18.7.2 The Test Laboratory should also produce a summary of the main findings of the Test Report (including the Test Report of the subcontractor) in a single Test Report Summary. The Test Report Summary will be viewed by prospective customers and so it should be written with their interests in mind, rather than for the benefit of the TRB and the DA. It should not include any detailed references to the claims testing process. Further guidance about the content of the Test Report Summary, and which sections of the Test Report should be consulted, are in Appendix D of this Guide.
- 18.7.3 For new ICDs which have been accepted under the CCT Mark Maintenance Scheme and where partial testing has been agreed by the DA, the Test Laboratory should produce a Supplement to the existing Test Report documenting the results of the tests carried out against the revised ICD, and update the Test Report Summary.
- 18.7.4 It will not be acceptable to remove or re-word any claims from the ICD, the testing or the Test Report, but the Test Laboratory may make recommendations in the Test Report to delete or re-word claims in the ICD. Such recommendations will be considered and approved by the DA.
- 18.7.5 On completion of all tests against the ICD, the Test Laboratory shall issue the final version of the Test Report and Test Report Summary to the Vendor to enable them to see the observations and recommendations at the same time as the Test Laboratory submits the Test Report and Test Report Summary to the Scheme Secretariat. The Vendor can comment on the observations in the Test Report, but this must be submitted by the Vendor to the Scheme Secretariat, separately from the Test Report.

- 18.7.6 The Test Laboratory must verify and confirm whether the observations and recommendations in the Test Report have been addressed by the Vendor. The Test Laboratory should report on this in the Test Report before it is submitted to the Scheme Secretariat, or provide a Supplement to the Test Report to the Scheme Secretariat.
- 18.7.7 The Scheme Secretariat will arrange for the Test Report, Supplement to the Test Report and Test Report Summary to be reviewed and approved by the TRB and DA, and a decision on the award to be made by the DA. The Scheme Secretariat will arrange for questions or clarifications on the Test Report raised by the TRB or DA to be issued to the Test Laboratory for consideration.
- 18.7.8 The Test Report Summary with the main findings in the Test Report, will be published on the Scheme website, if the IS Product or Service has been awarded the CCT Mark.

18.8 Test Suspension or Termination

- 18.8.1 Should the IS Product or Service fail to perform one or more claims satisfactorily on any or all of the platforms specified in the ICD, the Test Laboratory shall consult and agree with the Vendor one of the following actions (see Vendor Guide for further information):
- 18.8.1.1. Terminate the testing:
 - 18.8.1.2. Correct the offending functionality - Provided that the correction can be made and a corrected version of the IS Product delivered to the Test Laboratory within 5 business days, testing may continue without unnecessary interruption. The Test Laboratory must also include details of the corrected version and which claims this relates to in the Test Report.
 - 18.8.1.3. Suspend the testing whilst the offending functionality or test procedures are corrected.
 - 18.8.1.4. Suspend the testing whilst the IS Product or Service documentation is updated to correct inaccurate or incomplete information.
 - 18.8.1.5. Recommend a change to the ICD - The Test Laboratory may recommend in the Test Report that the offending claim be modified or, exceptionally, deleted from the ICD. The Scheme Secretariat must be informed as soon as such a change to the ICD is identified during the testing, in addition to the recommended change being included in the Test

Report submitted to the Scheme Secretariat at the end of testing.

APPENDIX A TRIAL TEST

Purpose

- 1 The purpose of the trial test is to provide evidence to UKAS that the Test Laboratory complies with ISO/IEC17025:2005 and the Generic Claims Test Method (see Appendix B). It is also used as the basis for Appointment by the Scheme.

Objectives

- 2 The Trial Test is designed to demonstrate that:
 - 2.1 the individual testers are technically competent;
 - 2.2 the management and administration of the Test Laboratory is competent to fulfil its role in supporting tests under the Scheme;
 - 2.3 the test methods are valid;
 - 2.4 the test reports meet the standards.

Conduct

- 3 The precise details and subject of the Trial Test will be determined in accordance with the above mentioned objectives and the assessment criteria given below.
- 4 The candidate Test Laboratory is free to select any product or system which will demonstrate the required capability for UKAS accreditation for claims testing, but the Trial Test will not be automatically recognized under the Scheme (see paragraphs 6-7 below).

Assessment

- 5 The UKAS assessment takes place during the latter stages of the Trial Test but normally before the testing has been completed. The assessors will accompany testers during a site visit so that they can observe that aspect of the work.

Completion

- 6 Where the Test Laboratory has been granted a Provisional Appointment and a Trial Test has been authorised under the CCT Mark Scheme, the test team is required to complete the Trial Test and produce a Test Report and Test Report Summary for submission to the Vendor and Scheme Secretariat. The Test Report must also be submitted to UKAS to enable completion of the UKAS assessment.
- 7 The Test Report produced from an authorised trial test will be recognized by the Scheme and processed in the same way as a Test Report and Test

Report Summary from a fully accredited Test Laboratory (see the Test Laboratory Operation, section IV) provided UKAS accreditation for claims testing is achieved as a result of that Trial Test.

APPENDIX B GENERIC CLAIMS TEST METHOD

- 1 The test methods used by the Test Laboratory for claims testing under this Scheme must comply with ISO/IEC 17025:2005, the Generic Claims Test Method in this section or other published documents, including any applicable Specialist Test Methods corresponding to the Specialist Testing categories listed in Appendix E.
- 2 Additional or specific requirements for specialist testing under the Scheme will be approved by CESG in consultation with UKAS and the Scheme during the accreditation process. This may include the Test Laboratory's own specialist test method documents, and equipment in addition to any Specialist Test Methods approved by the Scheme.
- 3 Set up a test environment, architecture, harnesses and processes which represent a reasonable approximation to the real world use of the IS Product or Service, especially in the context of network connectivity, network configuration and data volumes.
- 4 Prepare the test environment comprising all platform and test components (hardware, firmware and software) specified in the ICD. Ensure that where applicable the product is delivered to the Test Laboratory using the published delivery procedure. Install and configure all platform and test components using only the installation and configuration procedures specified in the user, administration or functionality documentation provided by the Vendor for the IS Product or Service.
- 5 If the Vendor's test environment is to be used by the Test Laboratory for some of the tests, the installation and configuration of the Vendor's test environment should be witnessed by the Test Laboratory, or examined to ensure that it conforms to the configuration specified by the Test Laboratory.
- 6 Ensure that the test environment is operational and in a known state using only the procedures in the user, administration or functionality documentation provided by the Vendor for the IS Product or Service
- 7 Ensure that any test lab equipment has a valid calibration certificate, where applicable to the tests.
- 8 Prepare or acquire all test material that may be required to undertake testing against the ICD. Test material should address both positive and negative tests (eg. Invalid mail messages).
- 9 For each security claim specified in the ICD, devise one or more tests to fully meet the requirements of the security claims and the test approach in the ICD. Provide a method for recording in a traceable and auditable manner the test results achieved.

- 10 Specify for each test the prerequisite test conditions, ensuring that any test material (e.g. test pattern or test message) is also specified.
- 11 Using only procedures specified in the user, administration or functionality documentation, prepare a set of test steps in a test record that together clearly specify each test. Ensure that the following Claims Test Step Requirements are met:
 - 11.1 Each test step shall state the work to be performed by the Tester and should reference the relevant procedure(s) in the user, administration or functionality documentation. The test step should not unnecessarily repeat text from that documentation;
 - 11.2 Each test step shall state the expected behaviour of the test item and the expected result.
- 12 Develop the test steps using the available Vendor documentation or documentation supplied for the IS Product or Service, ensuring that the Claims Test Step Requirements are met.
- 13 Ensure that the test steps check the correct operation of the test item, including invalid data, at all boundary conditions specified in the user, administration or functionality documentation.
- 14 Where the user, administration or functionality documentation relies on user selected input, ensure that the test steps specify the input to be used by the Tester.
- 15 Ensure that the test steps include instructions for the conclusion of the test and the expected final post-test state.
- 16 Ensure that each test is repeatable and could be followed by a Vendor during any subsequent witnessing activity, or by another Tester. Ensure each test is validated by peer review and is fit for purpose.
- 17 If during preparation of the test steps the procedures in the user , administration or functionality documentation are unclear such that the Tester cannot guarantee that a valid test can be documented using only the user, administration or functionality documentation, terminate or suspend the Claims Test in accordance with the Claims Test Procedure in section IV.
- 18 Conduct each test using only the test steps specified in the test record.
- 19 For each test step, check that the actual test results are consistent with the expected test results.
- 20 Document any inconsistencies between the expected and actual test results on the test record, and any ease of use observations.

- 21 Summarise the test results in the Test Report, as specified in Appendix C of this Guide.
- 22 Authorise, store and retain all test records as required by the Test Laboratory Quality Manual.

APPENDIX C CCT MARK TEST REPORT FORMAT

[Insert Test Laboratory logo here]
(jpeg or eps format)

[Insert Vendor logo here]
(jpeg or eps format)

CCT MARK TEST REPORT

[Vendor Name]

[Insert Product or Service Name]
[Insert Product Version Number or Service Version Number and Period of Assessment]

VENDOR DETAILS	TEST LABORATORY DETAILS
[Insert Vendor Name here]	[Insert Test Laboratory Name here]
[Insert Vendor Address here]	[Insert Test Laboratory Address here]
Telephone Number: [Insert here]	Telephone Number: [Insert here]
Authorisation Details: This should include the name(s), function(s) and signatures or equivalent, of the report Authoriser.	

CCT Mark Application Reference Number	<insert here>
CCT Mark Maintenance Application	<insert CCT Mark Certificate Number>
Test Report Reference Number	<insert here>
Test Report Version Number	<insert here>
Author	<insert here>
Date	<insert here>
<u>CONTACT POINT FOR TECHNICAL QUERIES ON THE TEST REPORT:</u>	
<i>Contact Name:</i> <insert here>	
<i>Contact Email Address:</i> <insert here>	

Table of Contents

Note:

- *The Test Report should ensure that the requirements of ISO/IEC17025:2005 have been met.*
- *The footers of all the pages in the Test Report should be marked “Commercial in Confidence”, “CCT Mark Test Report”, followed by the Product Name and Version Number, or Service Name, Version and Period of Assessment.*
- *The preferred usage for the Test Laboratory’s logo on the cover sheet should be a minimum of 30mm wide and 20mm high. The reason is for legibility of the logo. The preferred size of the logo should also not exceed 55mm in width or 30mm in height. This stops the logo dominating documents.*
- *The font used for the body text must be Arial 12 and the language must be UK English. The font for the headers and footers should be Arial 10.*

1 Executive Summary

1.1 Summary of overall test result

This should state whether all the security claims specified in the IA Claims Document were tested successfully, and, if not, this section should summarise which claims failed and why.

The results in this Test Report only relate to the security claims specified in the IA Claims Document, and also only relate to the items tested.

1.2 Summary of Scope of Product or Service tested

Brief description of the scope of the IS Product or Service to be claims tested.

1.3 Observations and Recommendations

The Test Laboratory should also include all recommendations, observations or important information for customers/administrators to be aware of when installing and using the IS Product or Service.

2 Test Overview

2.1 Introduction

Include the actual start and end dates of testing.

2.2 References

This should include references to the actual version of the ICD used to conduct the tests reported in this Test Report, and other documents used in the tests, eg guides and manuals

- [ICD] IA Claims Document, version number, date published
- [AG] IS Product/Service Administration Guide, version number, date published
- [UG] IS Product/Service User Guide, version number, date published
- [TLG] Test Lab Guide, version number, date published
- [TM] Test Method (ie. generic, or one of the specialist test methods listed in Appendix E) version number, date published
- [TR] Test Reports of sub-contractors

(Add other acronyms and full names of documentation where appropriate)

This should include references to the actual version of the ICD (and the build number of the product where applicable) used to conduct the tests reported in the Test Report. It should also contain references to documentation which customers procuring the product would receive, such as administration guides, installation guides, user guides and release notes, etc.

2.3 Description of Product or Service

This should specify the IS Product or Service Name, Version Number, Platforms for IS Products and Period of Assessment for IS Services which are to be the subject of the Claims Test. Further details about the platforms should be included in the Software Requirements section.

Product/Service Name:

Version:

Platforms (for Products):

[Enter details of the operating system(s), browser(s) and any other software/hardware used to validate the claims, for the client and

server. Include the version numbers/service packs]

(Please list all product/platform combinations for each claim tested in table format similar to the one below)

Claim Reference	Operating System	Version	Browser	Version

Period of Assessment (for Services): [Enter start and end dates for the assessment]

The period of assessment is one year prior to the start of claims testing and is the period for which vendor questionnaires were carried out.

2.4 Scope of Product or Service

Reference the section of the ICD which describes the scope of the IS Product/Service to be claims tested, and confirm that this is accurate for the IS Product/Service to be tested.

This should summarise the security features, environmental assumptions, expected operational environment, operational security issues and threats, and platforms.

If the product consists of more than one component or edition, those used in claims testing should be listed, including the version number.

The following features of [product/service name and version number] were not tested under the CCT Mark Scheme:

(list features where appropriate)

2.5 Scope of testing

This should clearly identify Claims Tests which were to be performed or witnessed by the Test Laboratory and if applicable, those which were to be performed or witnessed by a sub-contractor or those performed by the Vendor and witnessed by the Test Laboratory.

This section should document the test environment, architecture and processes used, which will inform the TRB and DA on the real world relevance of the test approach. It also should include test material (eg A-V collection)

For services, this should include the period of the assessment for the service, for which the claims are being validated. This should be for a 12 month period prior to the start of claims testing. It is not the same as when the Test Laboratory actually performs the claims testing. This should also describe how the procedures, performance and user aspects of the IS Service were tested.

2.6 Location of Tests

This should clearly state where the Test Laboratory carried out testing and where witness testing was undertaken.

This section should include details, including postal address of all the locations, including location of remote services or installations, witness testing, interviewing of customers of IS Services, which relate to the Claims Tests being conducted or witnessed. If a sub-contractor conducted part of the tests, the location of the tests conducted by the sub-contractor should also be included.

2.7 Platform Configuration

Models and versions (including any service packs or patches) of each platform component (hardware, firmware, software) and third party components (hardware, firmware, software).

2.8 Test Configuration

Models and versions of each test item component (hardware, firmware, software).

2.9 Conduct of testing

This should clearly identify the Test Method for the Claims Tests carried out by the Test Laboratory and, if applicable, those Claims Tests carried out by a sub-contractor.

2.10 Test Method Deviations

The rationale for any deviation shall be recorded.

2.11 Opinions and Interpretations

Include any general points or opinions which arose or were identified during claims testing.

3 **Product or Service Testing and Results**

3.1 Ease of Use

A statement on ease or difficulty encountered in installing and using the IS Product or Service should be recorded here.

For IS services the Test Laboratory should detail how any vendor and client questionnaires were used as part of the testing process.

The Test Laboratory should include any observations or important information for customers/administrators to be aware of when installing and using the IS Product or Service.

3.2 Quality of Guidance Documentation

Comments on the quality and accuracy of the IS Product or IS Service documentation, including the installation, configuration and use of the claimed security functionality.

Include a short description about what the purpose of each piece of documentation is from a customer perspective.

Comments about the quality and accuracy of the supporting documentation and how easy it was to follow from a customer perspective should also be included here.

Comment whether the Guidance Documentation fully described the installation, configuration and use of the claimed security functionality, as appropriate to those using the IS Product or Service.

3.3 Functional Testing Results

This should include the results for each individual claim tested, including an outline of the test objectives. The results of each of the claims tested must be cross referenced with the relevant claims statements in the ICD.

3.4 Resistance to Publicly Known Vulnerabilities

Statement as to whether there are any publicly known vulnerabilities in the platform(s) being tested for the IS Product or Service and how these have addressed (eg. patches, fixes).

3.5 Validation of Existing Assurance Certificates

This should include a statement to confirm that the existing assurance certificates specified in the ICD have been validated for the exact version of the IS Product or Service which has been claims tested. The exact reference to the certificates (including a link to an Internet website) should be included in the References section.

3.6 Disclaimer

CSIA Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product or IS Service, or the Information System environment supporting the IS Product or IS Service. The issue of a Test Report is not an endorsement of a product or service.

This Test Report serves solely to summarise the results of testing carried out for the CCT Mark Scheme and should not be taken as an endorsement or otherwise of the IS Product or Service.

4 Abbreviations

List abbreviations used in this report and spell out the abbreviation in full.

APPENDIX D CCT MARK TEST REPORT SUMMARY FORMAT

*Insert Test Laboratory logo here
(jpeg or eps format)*

*Insert Vendor logo here
(jpeg or eps format)*

CCT Mark Test Report Summary

[Vendor Name]

[Insert Product or Service Name]
[Insert Product Version Number or Service Version Number and Period of Assessment]

VENDOR DETAILS	TEST LABORATORY DETAILS
[Insert Vendor Name here]	[Insert Test Laboratory Name here]
[Insert Vendor Address here]	[Insert Test Laboratory Address here]
Telephone Number: [Insert here]	Telephone Number: [Insert here]

Test Report Summary Issue Date: [to be completed by CCT Mark Secretariat - *date Test Report Summary published on CCT Mark website*]

Further details about the claims tested are included in the Information Assurance Claims Document (CCT Mark Certificate Number ____/____/____) published on the CCT Mark website (www.cctmark.gov.uk)

Note:

- *The Test Report Summary should be consistent with the Test Report, summarising the test results and whether the claims in the ICD have been validated. The suggested source of information in the Test Report to be used in the production of the Test Report Summary is given in each section.*
- *The footers of all the pages in the Test Report Summary should be marked “CCT Mark Test Report Summary”, followed by the Product Name and Version Number, or Service Name, Version and Period of Assessment.*
- *The preferred usage for the Test Laboratory’s and Vendor’s logos on the cover sheet should be a minimum of 30mm wide and 20mm high. The reason is for legibility of the logo. The preferred size of the logo should also not exceed 55mm in width or 30mm in height. This stops the logo dominating documents.*
- *The font used for the body text must be Arial 12 and the language must be UK English. The font for the headers and footers should be Arial 10.*
- *The Test Report Summary should be submitted as a Word document. This will be published as a PDF document on the CCT Mark website, when the document has been approved and the CCT Mark award has been confirmed by the Scheme.*

1 Test Result

- 1.1 The CSIA claims testing of the [IS Product and version number, or IS Service and period of assessment] by [Test Laboratory name and sub-contractor name] concluded that the security functionality claims made within the IA Claims Document [ICD] are valid for this IS Product or Service.”

This should state whether all the security/functionality claims specified in the IA Claims Document (ICD) for the (exact version of the) relevant IS Product or Service were tested successfully.

The Test Laboratory should also include any additional observations or important information for customers/administrators to be aware of when installing and using the IS Product or Service.

Suggested Test Report source:

- *Section 1.1 Summary of Overall Test Result*

2 References

[ICD] IA Claims Document, version number, date published

[AG] Administration Guide, version number, date published

[UG] User Guide, version number, date published

[Certs] Existing assurance certificates, version number, date published

(Add other acronyms and full names of documentation where appropriate)

This should include references to the actual version of the ICD (and the build number of the product where applicable) used to conduct the tests reported in the Test Report. It should also contain references to documentation which customers procuring the product would receive, such as administration guides, installation guides, user guides and release notes, etc.

Suggested Test Report source:

- Section 2.2 References

3 Scope of Testing

3.1 The [product/service name and version/build number] was tested using the Test Method [TLG and/or TM] against the claims made in the [ICD].

3.2 The following features of [product/service name and version number] were not tested under the CCT Mark Scheme:

(List features where appropriate)

3.3 The [product/service name and version number] consists of:

(List the individual components where appropriate. List models/versions of software, firmware and hardware)

3.4 The Claims Tests were conducted at [locations of all tests carried out by the Test Laboratory, Sub-contractor, at the Vendor and Customers' premises]

Each location used for the tests should be identified separately for test Laboratory testing, witnessing or interviewing.

3.5 The following product/platform combinations (including version numbers and service packs) were used:

(Please list all product/platform combinations in table format similar to the one below)

Operating System	Version	Browser	Version

- 3.6 IS Service Claims concerning procedures, performance and user aspects over the [period of assessment] were validated as follows:

This section should clearly identify the Claims Tests which were to be performed or witnessed by the Test Laboratory and if applicable, those which were to be performed or witnessed by a sub-contractor.

This section should also document the test environment, architecture and processes used during the claims testing.

For IS services the Test Laboratory should reference how any vendor and client questionnaires were used as part of the testing process.

Suggested Test Report sources:

- Section 2.3 Description of Product or Service
- Section 2.4 Scope of Product or Service
- Section 2.5 Scope of Testing
- Section 2.6 Location of Tests

4 **Ease of Use**

4.1 Installation of the product.....

4.2 The administrator should note that...

A statement about the ease or difficulty encountered in installing and using the IS Product or Service, including any key material where appropriate, should be highlighted here.

The Test Laboratory should also include any additional observations or important information for customers/administrators to be aware of when installing and using the IS Product or Service.

For IS Services, evidence from customer questionnaires should also be used.

Suggested Test Report sources:

- Section 1.3 Observations and Recommendations
- Section 3.1 Ease of Use

5 **Quality of User and Administration Documentation**

Include a short description about what the purpose of each piece of documentation is from a customer perspective.

Comments about the quality of the supporting documentation and how easy it was to follow from a customer perspective should also be included here.

Suggested Test Report source:

- *Section 3.2 Quality of Guidance Documentation*

6 Resistance to Publicly Known Vulnerabilities

This should include a statement about if there are any known vulnerabilities in the platform(s) being tested for the IS Product or Service, and how these have been addressed (eg. fixes, patches).

Suggested Test Report source:

- *Section 3.5 Resistance to Publicly Known Vulnerabilities*

7 Validation of Existing Assurance Certificates

This should include a statement to confirm that any existing assurance certificates specified in the ICD have been validated for the exact version of the IS Product or Service which has been claims tested. The exact reference to the certificates (including a link to an Internet website on which the certificate has been published) should be included in the references section.

Suggested Test Report source:

- *Section 3.4 Validation of Existing Assurance Certificates*

8 Disclaimer

CSIA Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product, IS Service or the Information Systems environment supporting the IS Product or IS Service. The issue of a Test Report Summary is not an endorsement of a product or service.

This Test Report Summary serves solely to summarise the results of the testing carried out for the CCT Mark Scheme and should not be taken as an endorsement or otherwise of the IS product or IS Service.

9 Abbreviations

Where appropriate, list any other abbreviations that have been used in the report and their full descriptions.

APPENDIX E CLAIMS TESTING CATEGORIES

This list is up to date at the time of publication of this document but is subject to change. Changes to this list will be published on the Scheme website.

Specialist Test Methods for the Specialist Testing categories will be approved for use in Claims Testing during the ISO/IEC 17025 accreditation process. Enquiries about specialist test methods can be obtained iacs@cesg.gsi.gov.uk.

Generalist Testing:

All other testing that has not been specified as one of the following specialist testing categories in this Guide or subsequently notified on the Scheme website.

Specialist Testing:

Anti-malware (including anti-virus, anti-spam, Trojan detection, etc)

Biometrics

Intrusion Detection and Prevention (systems and services)

Smartcards

Hardware testing

Data Erasure (overwriting and degaussing)

APPENDIX F

GLOSSARY AND TERMINOLOGY

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

Applicant Company

The company applying to become a Test Laboratory under the Scheme.

Application

The formal request submitted by the Vendor to the Scheme for the IS Product or IS Service specified in the IA Claims Document to be registered with the scheme. This includes new and CCT Mark maintenance applications.

Award

The issue of a formal statement by the Scheme confirming the Vendor's security claims for an IS Product or Service have been independently tested by an appointed Test Laboratory and validated against the IA Claims Document, and legitimate use of the CCT Mark on the specific version of the IS Product or Service tested.

Claims Test

The process carried out by a Test Laboratory appointed under the CCT Mark Scheme for the independent testing of the security functionality claims of IS Products or IS Services stated in the ICD, and in accordance with the Test Laboratory's UKAS accreditation.

Claims Test Method

The test methods used by the Test Laboratory for claims testing under this Scheme must comply with Appendix B of this Guide.

Common Criteria

The Common Criteria represents the outcome of efforts to develop criteria for evaluation of IT security that are widely recognised within the international community.

Decision Authority (DA)

The organisation appointed by the Scheme Senior Executive to formally accept Applications made to the Scheme and to award the CCT Mark.

EAL1 and EAL2

Evaluation Assurance Levels (EAL) recognised under Common Criteria.

Executive Panel (EP)

The organisation appointed by the Scheme Senior Executive to manage the launch and operation of the Scheme during the Pilot phase.

Information Assurance (IA)

The confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Information Assurance Claims Document (ICD)

The document which identifies the security functionality claims to be tested and the test approach for the defined IS Product or Service.

IS Product

The subject of a Claims Test comprising software, firmware and/or hardware and its associated administration, user guidance documentation and marketing materials supplied by a Vendor

IS Service

The subject of a Claims Test comprising software, firmware and/or hardware and its associated administration, user guidance documentation and marketing materials supplied by a Service Provider.

ISO/IEC Guide 17025

The document, "General requirements for the Competence of Testing and Calibration Laboratories" (Reference D).

Managed Service

The operation of the Scheme by an organisation, on behalf of CSIA (Cabinet Office).

Pilot

The operation of the Scheme to fully define the processes required to run the Scheme as a managed service.

Scheme

The CSIA Claims Tested Mark Scheme that is described in the Scheme documentation listed in the References section of this document.

Scheme Description

The document which describes the Scheme including the procedures, management and operation of the Scheme (Reference A).

Secretariat

The organisation responsible for supporting the day to day activity of the Scheme and those involved in the Scheme.

Senior Scheme Executive

The person in CSIA who sets objectives and policy for the operation of the Scheme, and who appoints those who operate the Scheme on behalf of CSIA.

Technical Review Body (TRB)

The organisation appointed by CESG to make recommendations to the DA on accepting Applications made to the Scheme and the award of the CCT Mark.

Test Laboratory (TL)

An organisation accredited by UKAS in accordance with the agreed standard ISO/IEC 17025:2005 and appropriate Claims Test Method (see Appendix B) and appointed by the Scheme Senior Executive to undertake tests under the Scheme.

Test Laboratory (TL) Agreement

The Test Laboratory Agreement (known as TL Agreement) will define the terms and conditions for the appointment of the Test Laboratory under the Scheme. The TL Agreement is between Cabinet Office and the Test Laboratory.

Test Report

A report produced by a Test Laboratory and submitted to the Scheme detailing the findings of the Claims Tests, and which will be used by the TRB and DA to assess whether the CCT Mark can be awarded.

Test Report Summary

The summary of the main findings from the Test Report for the IS Product or Service written by the Test Laboratory and submitted by the Test Laboratory to the Scheme. This is published on the Scheme website, following the Award of the CCT Mark.

Vendor

A person or organisation that owns and develops the IS Product, or the Service Provider that provides the IS Service, and requests the Claims Testing of an IS Product or Service.

UKAS Assessment Conduct

The UKAS document “The Conduct of UKAS Laboratory Assessments” (Reference E)

User

A person or organisation which purchases the IS Product or Service.

REFERENCES

- (A) CSIA Claims Tested Mark Scheme - Description of the Scheme [See website www.cctmark.gov.uk]
- (B) CSIA Claims Tested Mark Scheme – Test Laboratory Guide [See website www.cctmark.gov.uk]
- (C) CSIA Claims Tested Mark Scheme – Vendor Guide [See website www.cctmark.gov.uk]
- (D) ISO/IEC Guide 17025:2005: General Requirements for the Competence of Testing and Calibration Laboratories
- (E) The Conduct of UKAS Laboratory Assessments [UKAS Publication Ref: LAB3 see website www.ukas.com].
- (F) CCT Mark Brand Guidelines for Test Laboratories [Available from CCT Mark Secretariat]
- (G) CCT Mark Brand Guidelines for Vendors [Available from CCT Mark Secretariat]

ABBREVIATIONS

CCT	CSIA Claims Tested
CESG	The National Technical Authority for Information Assurance
CSIA	Central Sponsor for Information Assurance
DA	Decision Authority
EP	Executive Panel
FIPS	Federal Information Processing Standard
HMG	Her Majesty's Government
IA	Information Assurance
ICD	Information Assurance Claims Document
IS	Information Systems
QMS	Quality Management System
Scheme	CSIA Claims Tested Mark Scheme
TL	Test Laboratory
TRB	Technical Review Body
UK	United Kingdom
UKAS	United Kingdom Accreditation Service