



CSIA CLAIMS TESTED MARK SCHEME

VENDOR 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 of Vendors who participate in 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
1.0.0	First version of CCT Mark Vendor Guide	31/03/05
2.0.0	<p>Second version of the CCT Mark Test Vendor Guide published at the start of Stage 2 of the Pilot.</p> <p>This Guide replaces the guidance issued for Stage 1 in version 1.0.0, and should be used for all new applications received in Stage 2.</p> <p>Major changes concern:</p> <ul style="list-style-type: none"> • Changes in Registration process for payment of Registration Fee and signing of Vendor Agreement (Section II, • Claims Testing Process (Sections II, III) • Production of Test Report (Sections II, III) • Award of the CCT Mark, including publication of final version of ICD accepted by the Scheme, and Test Report Summary (Sections II, III) • Changes in format for IA Claims Document (Appendix A) • Changes in format for Marketing Statement (Section II, III, Appendix A) <p>See also the revised Test Laboratory 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>Third version of the CCT Mark Test Vendor Guide published during Stage 2 of the Pilot.</p> <p>Changes to the content of the IA Claim document for IA services applications as follows:</p> <ul style="list-style-type: none"> • Application for the CCT Mark (Section II) Paragraph 6.6 added which relates to providing 5 existing customers of their service to confirm the Vendor's claim(s). • IA Claim document (Appendix A) two new requirements added to Test Approval (Section 3.2) which relates to IA Services 	17/10/05

Issue	Description of Changes	Date Issued
2.2.0	<p>Fourth version of the CCT Mark Test Vendor Guide published during Stage 2 of the Pilot.</p> <p>Duplication of the detailed process within the Scheme Description, Test Laboratory Guide and Vendor Guide has been removed.</p> <p>Other changes:</p> <ul style="list-style-type: none"> • Submission of the revised final version of the ICD (Section II, Paragraphs 10.4 and 11.6, Section III – Paragraph 14.2) • References to existing assurance certificates in the ICD (Appendix A): Existing Assurance Certificates section has been renumbered 3.2 and is now part of the Security Claims section. • Test Approach (Appendix A) – Requirement added to identify the source of information to validate existing assurance certificates 	05/12/05
2.3.0	<p>Fifth version of the CCT Mark Vendor 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>Guidelines on the requirements for testing services have been added to section 6 and Appendix A.</p> <p>Option for vendor to submit ICD without Test Approach for an initial review included in section 6.</p> <p>Description of process on the preparations for announcing the CCT Mark award added to section 11 (Award of the CCT Mark)</p> <p>Updated format and guidance for the Information Assurance Claims Document in Appendix A.</p>	04/05/07

CONTENTS

FOREWORD	2
DOCUMENT HISTORY	3
I OVERVIEW	7
1 Introduction.....	7
2 Document Changes	7
3 Terminology	7
4 Fees	8
II APPLICATION FOR THE CCT MARK	10
5 Introduction.....	10
6 Information Assurance Claims Document (ICD)	10
7 Registration.....	12
8 Acceptance of the Application	13
9 Claims Testing	13
10 Production of Test Report.....	16
11 Award of the CCT Mark.....	16
III APPLICATION FOR CCT MARK MAINTENANCE	19
12 Introduction	19
13 Preparing the Application for CCT Mark Maintenance.....	19
14 Registration	19
15 Acceptance of the Application.....	20
16 Claims Testing.....	21
17 Production of Test Report.....	21
18 Award of the CCT Mark.....	21
IV DISPUTES PROCEDURES	23
19 Applications under the Scheme.....	23
20 Test Laboratory Conduct.....	23

APPENDIX A - IA CLAIMS DOCUMENT (ICD) FORMAT	24
APPENDIX B	32
GLOSSARY AND TERMINOLOGY	32
REFERENCES.....	35
ABBREVIATIONS.....	35

I OVERVIEW

1 Introduction

- 1.1 The CSIA Claims Tested (CCT) Mark (CCTM) 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 is intended to provide a basic level of assurance which 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 claims of IS Products and IS Services by a Test Laboratory accredited by the UK Accreditation Service (UKAS). This provides the Users of such IS Products and IS Services with confidence that the Vendor’s security claims have been validated.
- 1.5 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”).
- 1.6 Further details about the responsibilities of Test Laboratories and the process for claims testing are included in the “CSIA Claims Tested Mark Scheme – Test Laboratory Guide”.

2 Document Changes

- 2.1 All the Scheme documents (including this guide) will be subject to review and amendment during the Pilot 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 Terminology

- 3.1 The term Vendor is used throughout this document to signify the person or organisation that:
 - 3.1.1 owns and develops the IS Product; or
 - 3.1.2 is the Service Provider who provides the IS Service;

- 3.1.3 prepares and submits the Application and IA Claims Document for the Claims Test of the IS Product or IS Service; and
- 3.1.4 pays the fees associated with registration of the IS Product or IS Service under the Scheme; and
- 3.1.5 pays the costs associated with the Claims Test of the IS Product or IS Service under the Scheme.

4 Fees

- 4.1 The Scheme requires the Vendor to pay a fee to the Scheme Secretariat to register the Application for an IS Product or IS Service to be tested under the Scheme. This registration fee covers administrative charges for:
 - 4.1.1 Registration of the Application by the Scheme Secretariat;
 - 4.1.2 Review of the Application and supporting documentation, and Test Report by the Technical Review Body (TRB);
 - 4.1.3 Review and Decision by the Decision Authority (DA) to accept the Application for a Claims Test and to award the CCT Mark under the Scheme;
 - 4.1.4 Granting of a licence to the Vendor to use the CCT Mark for:
 - 4.1.4.1 the specified version and platform(s) of the IS Product for a period up to 2 years from the date of the Award; and
 - 4.1.4.2 the specified IS Service for a period up to one year from the date of the Award.
- 4.2 The registration fee will be set by CSIA and will be as notified in the Vendor Agreement and amendments to this which are issued to the Vendor. This will specify the fees payable for new and CCT Mark Maintenance Applications.
- 4.3 The fee will be payable when the Application is registered by the Scheme Secretariat. Details about how the payment should be made are published on the Scheme website.
- 4.4 The Vendor should send the payment for the registration fee to the Scheme Secretariat with the Application. If the Application is not accepted for registration by the Scheme, the Scheme Secretariat will notify the Vendor and the registration fee will not be paid into the Scheme.
- 4.5 There shall be no refund of the registration fee should:
 - 4.5.1 the Application be registered but not formally accepted for claims testing under the Scheme; or

- 4.5.2 the Application is not successful in being awarded the CCT Mark; or
- 4.5.3 the licence to the Vendor to use the CCT Mark is withdrawn by CSIA.

II APPLICATION FOR THE CCT MARK

5 Introduction

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

6 Information Assurance Claims Document (ICD)

- 6.1 Before the Vendor can submit an Application for registration under the Scheme, the Vendor will first need to prepare an Information Assurance Claims Document (ICD) for the IS Product or IS Service. The ICD should be produced in accordance with the format and requirements specified in Appendix A.
- 6.2 The ICD must:
- 6.2.1 provide clear and accurate statements about the security and functionality of the IS Product or IS Service which are to be tested under the Scheme;
 - 6.2.2 include a marketing statement (maximum 150 words) which summarises the functionality claims of the IS Product or IS Service to which the CCT Mark will apply;
 - 6.2.3 specify the name of the IS Product (including exact version and platforms) or IS Service (including the period of assessment), for which the Application to the Scheme is being made. A separate ICD must be produced for each version of the IS Product or IS Service.
- 6.3 The ICD is a key component of the Application to the Scheme, and will be used in the following stages:
- 6.3.1 Registration under the Scheme: The ICD must be submitted with the Application and the required supporting documentation for the Application to be registered under the Scheme;
 - 6.3.2 Acceptance of the Application to the Scheme - The ICD will be reviewed by the TRB and DA to determine whether the ICD for the IS Product or IS Service can be accepted for testing under the Scheme;
 - 6.3.3 Claims Test: The testing for all the claims and platforms for the IS Product or IS Service specified in the ICD, must be performed by an approved Test Laboratory. For specialist testing, the Test Laboratory may sub-contract to an approved Test Laboratory

who has been appointed by the Scheme to undertake such testing.

- 6.3.4 Production of the Test Report: The Test Laboratory must prepare the Test Report and Test Report Summary for all the claims and platforms of the IS Product or IS Service specified in the ICD.
 - 6.3.5 Award of the CCT Mark: It is a requirement of the Scheme that the final version of the ICD accepted by the Scheme will be published on the Scheme website, together with the Test Report Summary, for IS Products and IS Services awarded the CCT Mark.
- 6.4 The Vendor is responsible for producing the ICD, but it is recommended that the Vendor should involve an approved CCT Mark Test Laboratory to provide advice and assistance in preparing the ICD. In particular, to advise that the claims as worded are actually testable and to define the test approach.
 - 6.5 Vendors may submit one version of their ICD for review, where the Vendor has not yet engaged a Test Laboratory to assist in the production of the ICD. In which case, it will be acceptable to exclude the Test Approach from the first version submitted.
 - 6.6 However, the Vendor must register the Application with the Scheme first, before the DA will provide comments on the first version of the ICD to the Vendor. The second and subsequent versions of the ICD submitted to the Scheme should include the Test Approach.
 - 6.7 The Vendor of an IS Service should submit a list of up to 5 Customers to the CCT Mark Secretariat, for the DA to approve before the client questionnaires are carried out. The list should include the name of the company and point of contact. The Scheme Secretariat will not contact any of the Customers provided by the Vendor.
 - 6.8 The Test Laboratory will interview the Customers to confirm their user experience of the service to support validation of specified claims. The period of assessment for the interviews will be for the 12 months prior to the start of claims testing.
 - 6.9 For all IS Products and IS Services the Vendor is advised to:
 - 6.9.1 Give consideration to the timing of the Application, taking into account the Vendor's plans to develop and release future versions of the IS Product or IS Service.
 - 6.9.2 Ensure claims testing is undertaken on the exact version and platforms included in the ICD. New versions or additional platforms implemented after the IS Product or IS Service has been tested under the Scheme will need to be submitted as a new or CCT Mark Maintenance Application;

- 6.9.3 Give consideration to the relationship and inter-dependencies between the testing process and any related assessments (e.g. CAPS or FIPS140 assessment of cryptographic aspects).

7 Registration

- 7.1 The Vendor is responsible for submitting the Application for the IS Product or IS Service to be tested under the Scheme. The Vendor should submit a separate Application and ICD for each version of the IS Product or IS Service for which the Vendor applies for the CCT Mark to be awarded.
- 7.2 The Scheme requires the Vendor Agreement to be signed by the Cabinet Office, acting through CSIA, and the Vendor. A separate Vendor Agreement must be signed by both parties for each application registered under the Scheme. The Vendor Agreement sets out the terms and conditions for the Vendor to participate in the Scheme, and the role of CSIA in the Cabinet Office. The Vendor Agreement is available from the Scheme Secretariat.
- 7.3 The Vendor must submit the following to the Scheme Secretariat to register the Application:
 - 7.3.1 CCT Mark Application form to register the IS Product or IS Service;
 - 7.3.2 ICD for the exact version and platforms of the IS Product or IS Service to be tested;
 - 7.3.3 User or Administration Guides (or equivalent) for the exact version and platforms of the IS Product or IS Service to be tested;
 - 7.3.4 Marketing literature (including the URLs of website pages) for the exact version and platforms of the IS Product or IS Service to be tested;
 - 7.3.5 Vendor Registration fee.
- 7.4 The Scheme Secretariat will register the Application, as long as the Application meets the conditions of the Scheme. Once the Application for the IS Product or IS Service has been registered the Vendor will be issued an application number. This should be quoted on all correspondence with the Scheme Secretariat
- 7.5 The Scheme Secretariat will also:
 - 7.5.1 prepare the Vendor 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

- 7.5.2 send the 2 signed copies of the Vendor Agreement to the Vendor. The Vendor should sign both copies and return one of these to the Scheme Secretariat within 10 business days of the date the signed Vendor Agreements were received from the Scheme Secretariat.

8 Acceptance of the Application

- 8.1 The Scheme Secretariat will arrange for the Application and supporting documentation to be reviewed by the TRB and approved by the DA.
- 8.2 Review of the Application and supporting documentation by the TRB and approval by the DA should normally take 5-10 business days following registration of the Application by the Scheme Secretariat, unless the Vendor is notified that the TRB or DA require additional time, to consider the Application. It should be noted that some large software products, such as operating systems, may be unsuitable for testing under the Scheme.
- 8.3 The TRB will send its recommendations on whether or not to accept the Application to the DA.
- 8.4 The DA will review the recommendations of the TRB and send the DA's decision on the acceptance or rejection of the Application to the Scheme Secretariat.
- 8.5 The Scheme Secretariat will notify the Vendor of the decision of the DA. A written explanation will be issued to the Vendor in the case of Applications which have not been accepted under the Scheme.
- 8.6 Should the decision of the DA be to accept the Application, the Scheme Secretariat will check that the Vendor Agreement has been signed by both parties, and write to the Vendor to confirm acceptance of the Application to be claims tested under the Scheme. Applications will only be formally accepted if they meet the conditions for acceptance as defined under the Scheme.

9 Claims Testing

- 9.1 The Vendor is responsible for agreeing a contract with an approved Test Laboratory to undertake testing against the ICD accepted under the Scheme, and in accordance with the Scheme documents.
- 9.2 Testing under the Scheme must be performed by Test Laboratories accredited by UKAS and appointed by the Scheme. Any specialist sub-contractors should also be accredited by UKAS, and appointed by the Scheme. The testing must be carried out in accordance with the process described in the Test Laboratory Guide.
- 9.3 A list of approved Test Laboratories appointed to undertake Claims Tests under the Scheme is published on the Scheme website, including whether the appointment is for a specialist testing capability.

- 9.4 The Vendor should only authorise the Test Laboratory to start testing after the Scheme Secretariat has confirmed to the Vendor that the ICD has been approved by the Scheme to be used in the claims testing.
- 9.5 Any testing work undertaken before formal acceptance of the ICD is received by the Vendor, will be at the risk and cost of the Vendor or Test Laboratory.
- 9.6 The Vendor should notify the Scheme Secretariat of the Test Laboratory who will be undertaking the Claims Test, the planned start and planned end dates.
- 9.7 The Claims Test by the Test Laboratory should not exceed 20 days effort and should be completed within 6-8 weeks of the start of testing. Some flexibility in these targets may be acceptable. For example, in the case of particularly complex products or for concurrent testing of product families, but the Vendor will need to consult the Scheme Secretariat on this.
- 9.8 Should the IS Product or IS 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:
- 9.8.1 Terminate the testing:
- 9.8.1.1. The Vendor will notify the Scheme Secretariat that it has been agreed with the Test Laboratory to terminate the testing. The Scheme Secretariat will mark the Application as closed and will confirm this action has been taken with the DA, Vendor and Test Laboratory.
- 9.8.1.2. The Vendor retains the option of re-submitting the IS Product or IS Service for testing at a future date, but this will be registered as a new Application under the Scheme.
- 9.8.2 Correct the offending functionality:
- 9.8.2.1. 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. However, the Vendor must inform the Scheme Secretariat by email if this action is taken, and advise the new version number of the corrected IS Product.
- 9.8.3 Suspend the testing whilst the offending functionality is corrected.
- 9.8.3.1. This action can only be taken with prior approval by the DA, via the Scheme Secretariat. Suspension of testing is

allowed for a maximum period not exceeding 3 calendar months from the date that testing was suspended.

- 9.8.3.2. The Test Laboratory must resume testing of resolved problems within the approved period of suspension, and the Vendor must advise the Scheme Secretariat of the date on which the testing was resumed.
- 9.8.3.3. The Scheme Secretariat will advise the Vendor and Test Laboratory 10 business days before the approved period of suspension is due to be exceeded.
- 9.8.3.4. The Vendor should advise the Test Laboratory when the approved period of suspension has been exceeded and terminate the testing.
- 9.8.3.5. The Vendor should notify the Scheme Secretariat that the testing has not been resumed within the approved period of suspension. In which case, the Scheme Secretariat will mark the Application as closed and will confirm this action has been taken with the DA, Vendor and Test Laboratory.
- 9.8.3.6. If the approved period of suspension is exceeded, and neither the Vendor nor Test Laboratory has contacted the Scheme Secretariat about the current position on this, the DA will, via the Scheme Secretariat, advise the Vendor and the Test Laboratory that the Application will be closed, unless either party clarifies the position within 5 business days of the receipt of the letter from the DA.

9.8.4 Recommend a change to the ICD

- 9.8.4.1. 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. The DA reserves the right to reject the recommended change if it is felt that the offending claim is critical to the effective use of the IS Product.
- 9.9 It will not be acceptable to remove any items from the ICD, the testing or the Test Report, but recommendations made by the Test Laboratory in the Test Report to delete items in the ICD, will be considered by the TRB and DA.
- 9.10 If an IS Product or IS Service which has previously failed is subsequently corrected and re-submitted for testing under the Scheme, a new Application should be submitted and the full testing process shall

apply. It will not be acceptable to re-use the results from the earlier tests.

10 Production of Test Report

- 10.1 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 Test Laboratory Guide.
- 10.2 On completion of all the tests against the ICD, the Test Laboratory shall issue the final version of the Test Report to the Vendor to enable them to see all the observations and recommendations of the report. At the same time the Test Laboratory should submit the Test Report to the Scheme Secretariat along with a properly formatted Test Report Summary.
- 10.3 The Vendor may submit comments on the observations and recommendations contained in the Test Report and the Test Report Summary to the Scheme Secretariat to inform the subsequent review process. This must be submitted by the Vendor to the Scheme Secretariat separately from the Test Report and Test Report Summary.
- 10.4 The Vendor is responsible for producing the final version of the ICD which incorporates the changes to the ICD as recommended by the Test Laboratory in the Test Report. This should be submitted by the Vendor to the Scheme Secretariat at the same time as the Test Laboratory submits the final version of the Test Report to the Scheme Secretariat. The final version of the ICD should exclude the Test Approach and be formatted according to the requirements in Appendix A of this Guide.
- 10.5 The Test Report and the Test Report Summary should be submitted to the Scheme Secretariat within 3 months of the date that the Vendor was notified by the Scheme Secretariat that the ICD had been accepted to go forward to claims testing. If the Test Report is not received within the period specified, the Scheme Secretariat will mark the Application as closed and will confirm this action with the DA, Vendor and Test Laboratory.

11 Award of the CCT Mark

- 11.1 The Scheme Secretariat will arrange for the Test Report, Test Report Summary and the final version of the ICD to be reviewed by the TRB, and a decision on the award to be made by the DA.
- 11.2 The TRB reviews the Test Report to:
 - 11.2.1 confirm that tests have been undertaken on all the claims in the ICD, in accordance with the test process outlined in the Test Laboratory Guide;

- 11.2.2 review the test results and observations made by the Test Laboratory, and make recommendations to the DA on whether the CCT Mark should be awarded.
- 11.3 Review of the Test Report by the TRB and approval by the DA should normally take 5-10 business days following receipt of the Test Report by the Scheme Secretariat, unless the Vendor is notified that the TRB or DA require additional time to consider the Test Report. For example, to clarify issues arising from the Test Report with the Test Laboratory or Vendor.
- 11.4 The TRB will send its recommendations on whether or not to award the CCT Mark to the DA.
- 11.5 The DA will review the Test Report and the recommendations of the TRB and will make a decision on whether or not to approve the award of the CCT Mark to the IS Product or IS Service.
- 11.6 The DA also reviews the Test Report Summary and final version of the ICD to:
 - 11.6.1 confirm that only the changes to the ICD recommended by the Test Laboratory and approved by the DA have been incorporated;
 - 11.6.2 confirm that the Test Report Summary meets the requirements specified in the Test Laboratory Guide;
 - 11.6.3 approve the Test Report Summary and final version of the ICD to be published on the Scheme website, when the award is formally announced.
- 11.7 The DA will confirm whether or not the CCT Mark has been awarded to the IS Product or IS Service, and the Test Report Summary and final version of the ICD has been approved for publication on the Scheme website.
- 11.8 The Scheme Secretariat will advise the Vendor of the decision of the DA, and the Application will be closed.
- 11.9 Once the award of the CCT Mark has been approved by the DA, the Scheme Secretariat will arrange for the award to be publicly announced on the Scheme website. This should take up to 10 working days to complete and includes the following:
 - 11.9.1 publishing the final version of the ICD approved by the Scheme and the Test Report Summary on the Scheme website;
 - 11.9.2 the IS Product or IS Service and its associated marketing statement to be added to the list of CCT Mark Awards on the Scheme website;

- 11.9.3 the CCT Mark logo with certificate number to be issued to the Vendor;
 - 11.9.4 confirmation to be sent to the Vendor to authorise them to use the CCT Mark logo on the exact version and platforms of the IS Product or IS Service tested according to the conditions for the award of the CCT Mark and licence set out in the Vendor Agreement. This will include the CCT Mark logo with the certificate number and branding guidelines on the use of the CCT Mark logo;
 - 11.9.5 the CCT Mark certificate for the IS Product or IS Service signed by the Scheme Senior Executive to be issued to the Vendor.
- 11.10 Copyright of the certificate remains the property of the Scheme Senior Executive.
 - 11.11 The Vendor must wait until the award is formally announced on the Scheme website, before issuing any communication about this to customers or other interested parties.
 - 11.12 The Vendor should use the CCT mark according to the conditions for the award of the CCT Mark and licence set out in the Vendor Agreement.
 - 11.13 The award of the CCT Mark is valid for a maximum of 2 years from the date of the Award for IS Products, and for IS Services for 1 year from the date of the Award. The Award for the IS Service can be maintained for a second year, subject to the IS service being tested under the CCT Mark Maintenance. The CCT Mark should not be used on any other version or platforms other than those for which the Award was granted, or for any other product or service.
 - 11.14 In the case where the award of the CCT Mark ceases to be valid or authority to use the CCT Mark is withdrawn, the Scheme Secretariat will publish the name of the IS Product or IS Service, exact version and platforms of the IS Product or IS Service for which the CCT Mark has been withdrawn, or ceased to be valid on the Scheme website. This will be published for a period of 2 years.
 - 11.15 Where the IS Product or IS Service is not awarded the CCT Mark, the final version of the ICD and Test Report Summary are not published on the Scheme website.
 - 11.16 In all cases the ICD and Test Report remain the property of the Vendor who submitted the Application to the Scheme. The Vendor will grant a non-exclusive license to copy, use, publish and distribute the final versions of the ICD and Test Report in accordance with the requirements of the Scheme. This includes publication on the CCT Mark website of the final version of the ICD and Test Report Summary for the IS Product or IS Service which is awarded the CCT Mark.

III APPLICATION FOR CCT MARK MAINTENANCE

12 Introduction

- 12.1 This section describes the process for maintenance of the CCT Mark for the IS Product or IS Service.
- 12.2 This section only specifies the differences in the process for CCT Mark maintenance applications.
- 12.3 The process for registering and acceptance of applications to the Scheme, and award of the CCT Mark is described in more detail in Section II.

13 Preparing the Application for CCT Mark Maintenance

- 13.1 When there are changes to the specified version of the IS Product or IS Service, such as additional or updated functionality, patches, new releases or versions, additional platforms, change in procedures or location of the IS service, the Vendor should:
 - 13.1.1 first update all sections of the ICD to reflect the changes to the IS Product or IS Service since the IS Product or IS Service was last tested.
 - 13.1.2 submit a CCT Mark Maintenance Application to the Scheme Secretariat for :
 - 13.1.2.1. the CCT Mark to be awarded to the new version and additional platforms for the remainder of the period of the Certificate already awarded to the IS Product; or
 - 13.1.2.2. the CCT Mark to be awarded to the new version of the IS service during the first year of the Award, or maintain the Award for a second year.
- 13.2 The Vendor is responsible for updating the ICD, but it is recommended as with a new application that an approved Test Laboratory should be used to provide consultancy advice and assistance in updating the ICD.

14 Registration

- 14.1 The Vendor is responsible for submitting the Application for CCT Mark maintenance of the IS Product or IS Service under the Scheme. The Vendor must submit the following to the Scheme Secretariat:
 - 14.1.1 CCT Mark Application form to register the maintenance of the CCT Mark for the IS Product or IS Service;
 - 14.1.2 Revised IA Claims Document for the exact version and platforms of the IS Product or IS Service;

- 14.1.3 A separate document with a reasoned argument justifying the case for CCT Mark maintenance. This should include details of what has changed since the CCT Mark was awarded, what the impact is on the original claims and whether new claims have been added;
 - 14.1.4 The new User or Administration guides (or equivalent) for the exact version and platforms of the IS Product or IS Service;
 - 14.1.5 Current marketing literature (including the URLs of website pages) for the exact version and platforms of the IS Product or IS Service;
 - 14.1.6 Vendor Registration fee for CCT Mark maintenance.
- 14.2 Additional information is needed in the IA Claims document about, the changes which have been made to the IS Product or IS Service since it was last tested under the Scheme. This might include for example:
- 14.2.1 The IS Product or IS Service operates on an additional platform;
 - 14.2.2 The security functionality, procedures or location of the IS Service have changed;
 - 14.2.3 Improved performance of the IS Product or IS Service;
 - 14.2.4 Observations raised during the previous Claims Tests have been addressed;
 - 14.2.5 Significant changes have been implemented such as a new version, or the IS Product or IS Service has been re-engineered;
 - 14.2.6 The Test Approach in the ICD should make clear which claims are to be re-tested or tested for the first time under the CCT Mark Maintenance and how this will be carried out ;
 - 14.2.7 In addition, for IS Services, the Vendor should submit to the CCT Mark Secretariat contact details (name and organisation) of up to 5 customers who have used the service in the previous 12 months. These customers will be interviewed by the Test Laboratory, to confirm that the IS Service is still providing the same service according to the claims stated in the ICD.
- 14.3 The Scheme Secretariat will register the Application, as long as the Application meets the conditions of the Scheme.

15 Acceptance of the Application

- 15.1 The Scheme Secretariat will notify the Vendor of the decision of the DA:

- 15.1.1 Whether the DA has confirmed partial re-testing under the CCT Mark Maintenance, and agreed the claims to be tested and the test approach as specified in the ICD.
- 15.1.2 Whether the DA has not accepted the Application for CCT Mark Maintenance, in which case a written explanation from the DA will be issued to the Vendor, including whether full testing is required to achieve the CCT Mark.

16 Claims Testing

- 16.1 All testing for CCT Mark maintenance should be undertaken in accordance with the process described in Section II of this document, and described in more detail in the Test Laboratory Guide.

17 Production of Test Report

- 17.1 The production of the Test Report, and the resulting changes made to the Test Report Summary and ICD, should be undertaken in accordance with Section II of this document and, described in more detail in the Test Laboratory Guide.

18 Award of the CCT Mark

- 18.1 The TRB reviews the new Test Report to:
 - 18.1.1 confirm that tests have been undertaken on those claims in the revised ICD where testing is required under CCT Mark Maintenance, in accordance with the test process outlined in the Test Laboratory document;
 - 18.1.2 confirm that tests have been undertaken on the additional functionality or new platform specified in the revised ICD where a partial re-test has been approved by the DA;
 - 18.1.3 review the test results and observations made by the Test Laboratory, and make recommendations to the DA on whether the CCT Mark should be awarded to the new version of the IS Product or IS Service.
- 18.2 If the DA approves the award of the CCT Mark for the CCT Mark maintenance application, the Scheme Secretariat will arrange for:
 - 18.2.1 a new Certificate to be awarded to the Vendor;
 - 18.2.2 the CCT Mark logo with the new certificate number to be issued to the Vendor;
 - 18.2.3 the new final version of the ICD (excluding the test approach) and the Test Report Summary to be published on the CCT Mark website.

- 18.3 The new Certificate will be valid for the remainder of the period of the existing Certificate for the IS Product or IS Service, or for a further year for the IS Service where the CCT Mark Maintenance is undertaken to retain the CCT Mark for a second year.

IV DISPUTES PROCEDURES

19 Applications under the Scheme

- 19.1 In the event of a dispute concerning Applications submitted to the Scheme, the Vendor should raise the matter in writing as soon as practical with the Scheme Senior Executive for resolution.
- 19.2 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.
- 19.3 The decision of the Director of CSIA will be given in writing to the Vendor within 20 working days of the matter being received in writing by the Director of CSIA.
- 19.4 The decision of the Director of CSIA on disputes concerning the acceptance of Applications by the Scheme or the award of the CCT Mark is final.

20 Test Laboratory Conduct

- 20.1 The Vendor should raise any complaint in respect of the conduct of testing or the preparation of the Test Report by a Test Laboratory undertaking Claims Tests, with the Test Laboratory itself.
- 20.2 If the complaint is not resolved to the satisfaction of the Vendor, the Vendor may raise the matter, if appropriate, with UKAS and the Scheme Senior Executive for consideration under the UKAS accreditation procedures, or appointment of Test Laboratories under the Scheme.
- 20.3 Complaints which concern the UKAS accreditation (ISO/IEC 17025:2005) for claims testing should be directed to the United Kingdom Accreditation Service in the first instance. See www.ukas.com for further information.
- 20.4 Complaints which concern the appointment of the Test Laboratory, should be raised with the Scheme Senior Executive.
- 20.5 Further details about the Complaints Procedure are included in the "CSIA Claims Tested Mark Scheme – Description of Scheme".

APPENDIX A - IA CLAIMS DOCUMENT (ICD) FORMAT

Insert Vendor logo here

(jpeg or eps format)

CCT MARK IA CLAIMS DOCUMENT (ICD)

[Vendor Name]

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

VENDOR DETAILS
<Insert Vendor Name.>
<Insert Vendor Address>
Telephone Number: <insert here – this is for customer enquiries>
Vendor Website: <insert here – this is for further information about the product or service>
Vendor Contact Email: <insert here – this is for customer enquiries>

APPLICATION DETAILS	
<i>The table will be deleted from the final version of the ICD to be published on the CCT Mark Website</i>	
CCT Mark Application Reference Number	
CCT Mark Maintenance Applications only	<insert CCT Mark Certificate Number>
ICD Reference Number	<insert here>
ICD Version Number	<insert here>
Author	<insert here>
Date	<insert here>
CONTACT POINT FOR TECHNICAL QUERIES ON THE ICD	
Contact Name	<insert here>

Contact Email Address	<insert here>
Telephone Number	<insert here>

CERTIFICATE DETAILS

The table will be on the front cover of the final version of the ICD when this is published on the CCT Mark Website

CCT Mark Certificate Number	<i>[To be completed by CCT Mark Secretariat]</i>
CCT Mark Award Expires on	<i>[To be completed by CCT Mark Secretariat]</i>
ICD Issue Date	<i>[To be completed by CCT Mark Secretariat]</i>

Note:

- *The headers and footers of all the pages in the ICD should be marked “Commercial in Confidence”, CCT Mark Test IA Claims Document”, followed by the Product Name and Version Number, or Service Name and Period of Assessment.*
- *The final version of the ICD published on the CCT Mark website should not include “Commercial in Confidence” in the headers or footers.*
- *The preferred usage for the Vendor’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 tables and for headers and footers should be Arial 10.*
- *The Test Approach (section 3.4) should be removed from the final version which the Vendor should submit after claims testing has finished. The final version will need to be approved by the Scheme for publication on the CCT Mark website, when the Award of the CCT Mark is confirmed.*
- *The ICD should be submitted as a Word document. This will be published (without the Test Approach) 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.*

Table of Contents

1 Introduction

1.1 Background

This document outlines the IA claims made by [Vendor Name] in regard to the suitability of [Product or Service Name] for use by the UK Public Sector for [describe the purpose of the IS Product].....

1.2 Objectives

1.2.1 The objectives of this ICD are to provide:

1.3 Purpose of Document

1.3.1 This document is the ICD for [Product or Service Name]

1.3.2 This ICD is the baseline document for the CCT Mark Claims Test of [Product or Service Name].

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material.
- Section 2 contains the description of functionality of [Product or Service Name] and all the information related to the security of [Product or Service Name].
- Section 3 details the security functionality claims that are being made.

2 **Product/Service Description**

Plain English and diagrams where appropriate will reduce the number of iterations of the ICD. Terminology should be consistent throughout and cross-references to the claim numbers in Section 3.1 should be highlighted.

2.1 Product/Service Identification

This should only specify the IS Product or IS Service Name, Version Number and Platforms which are to be used to validate the security functionality claims in Section 3.

Product or 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 in table format similar to the one below)

Operating System	Version	Browser	Version

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

The period of assessment is one year prior to the start of claims testing.

2.2 Product/Service Overview

The following sections should only include the security functionality which is being tested in the security claims in Section 3. Do not include references to functionality or platforms which are not included in the claims statements in Section 3.

2.2.1 Security architecture

This should include diagrams that are properly linked into the text, security protocols and where there are dependencies on external services, these should be referenced with web addresses if possible.

2.2.2 Hardware requirements

This should include models and versions.

2.2.3 Software requirements

This should include the versions, including service packs.

2.2.4 Out of Scope

This should only exceptionally include details of aspects of the IS Product or IS Service which are not being tested under the CCT Mark Scheme (eg. functionality, platforms, cryptographic algorithms or other editions of the IS Product or IS Service).

The testing of specific cryptographic algorithms will not be tested under the CCT Mark Scheme. If the Vendor has a requirement to test specific cryptographic algorithms, the Vendor should apply to the appropriate assurance schemes such as CAPS or FIPS to have the cryptographic algorithms validated. Further information on CAPS is at www.cesg.gov.uk and on FIPS at www.csrc.nist.gov/cryptval .

2.3 Usage assumptions

2.3.1 Assets

This should define the assets which are to be protected

2.3.2 Threat scenario

Threats to assets which are countered are:

-

This should identify the threats to assets which are countered by the product or service

2.3.2.1 Expected operational environment

This should include business benefits and scale of use.

2.3.2.2 Organisational security policies

This should identify what should be included in the organisation's security policy that has to be in place to successfully run the product or use the service.

2.3.2.3 Security requirements on the environment

The assumptions for security requirements which need to be implemented on the expected operational environment should be specified. This includes physical, personnel and procedural.

3 Security Claims for the IS Product or IS Service

3.1 Claims Statements

This should give clear statements of what the IS Product or IS Service shall provide to meet the IA requirement of the User. This should be written in plain English.

Each of these statements should be given a unique reference to enable the Test Laboratory to cross reference each of the claims statements with the results in the Test Report.

Unique Reference	Claims Statements

3.2 Existing assurance certificates

This should only include reference to existing assurance certificates which have been awarded to the exact version or component of the product or service to which this IA Claims Document refers.

References to applications which are in evaluation or plans to put the product or service through another evaluation or certification scheme will be not be accepted under the Scheme.

Examples of the evaluation or certification schemes are CCT Mark, FIPS140-2, FIPS 197, CAPS, Common Criteria.

Include the full web addresses for existing assurance certificates as well as the certificate number and name of the evaluation or certification scheme.

Where encryption is involved, only state the names of the algorithms which have been validated through the evaluation or certification scheme and been awarded a certificate.

If the product encrypts data but does not have an existing assurance certificate, there must be a claim in section 3.1 that covers the functionality of the product to encrypt data, pass the data as cipher text and finally read as plain text.

3.3 Test Approach

It is recommended that this section is produced in co-operation with a Test Laboratory.

This section should be clearly linked to the claims in Section 3.1, by including the claims statement reference and:

- *describe the test approach/strategy and reference the applicable Test Method;*
- *should clearly state where witness testing is to be used and why, including which platforms and claims;*
- *For maintenance applications, this should clearly state which claims are to be re-tested and which new claims are to be tested for the first time and how the testing will be done;*
- *describe the test environment, identify any claims which might require any specific equipment and/or technical expertise to test;*
- *provide assurance that the stated claims are capable of being tested objectively;*
- *identify the test location for each of the claims (eg. Test Laboratory, Vendor's site, Customer's site, sub-contractor's site);*
- *identify the client and host platform combinations which will need to be tested. This is best produced in a table specifying the claims references, and the platform combination which will be tested on each of the platform combinations. It should be noted that all the claims should be fully tested on all the platforms specified. If witness testing is used, all the claims should be fully tested on the other platforms specified in the ICD, provided that the Test Laboratory tests all of the claims on at least one platform first. (see the Scope of Testing section in the Test Laboratory Guide for the allowed conditions and variations for testing);*

- *Identify the source of information to verify the existing assurance certificates specified in the ICD.*

Where an IS Service is being tested, this section should:

- *Identify those claims where the functionality of the service will be tested by running the process, witnessing and verifying the outcome of the process;*
- *Identify the claims which test the service's procedures, and how this will be validated through interviews with the Vendor and review of the Vendor's documented procedures;*
- *Identify the claims which validate the user experience of using the service during the previous 12 months;*
- *Identify 5 existing customers of the service who are willing to validate the user experience claims. Where possible one of these customers should be an HMG Department, Local Government Authority, Police Authority or National Health Service Authority.*

Annex A Glossary of Terms

The glossary must be relevant to terms used in the ICD.

Annex B Marketing Statement to be used (if the claim is successful)

This should be statement of no more than 150 words which is directly relevant to the security functionality claims in section 3.1. This statement will be published on the CCT Mark website as the short description for the IS Product or IS Service. It will also be the wording which will have to be approved by the Scheme to be placed next to the CCT Mark logo.

Where aspects of the service are specified as out of scope (section 2.2.4) for claims testing, this should be stated in this marketing statement. For example, the exclusion of specific cryptographic algorithms, which do not have existing assurance certification. .

APPENDIX B

GLOSSARY AND TERMINOLOGY

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

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 in CSIA 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 in CSIA 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 IS 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 the 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 the Service Provider.

ISO/IEC Guide 17025:2005

The document, “General requirements for the Competence of Testing and Calibration Laboratories”.

Managed Service

The operation of the Scheme by an outsourced 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 this document and the References.

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

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

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 IS Service written by a 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 IS Service.

Vendor Agreement

The Vendor Agreement will define the terms and conditions for Vendors related to the registration of Applications and award of the CCT Mark under the Scheme. The Vendor Agreement is between Cabinet Office and the Vendor.

User

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

REFERENCES

- (A) CSIA Claims Tested Mark Scheme - Description of the Scheme [See website www.cctmark.gov.uk]
- (B) CSIA Claims Tested Mark Scheme – Vendor Guide [See website www.cctmark.gov.uk]
- (C) CSIA Claims Tested Mark Scheme - Test Laboratory Guide [See website www.cctmark.gov.uk]
- (D) CCT Mark Brand Guidelines for Vendors [Available from CCT Mark Secretariat]
- (E) CCT Mark Brand Guidelines for Test Laboratories [Available from CCT Mark Secretariat]

ABBREVIATIONS

CAPS	CESG Assisted Products Scheme
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
Scheme	CSIA Claims Tested Mark Scheme
TRB	Technical Review Body
UK	United Kingdom
UKAS	United Kingdom Accreditation Service