



## **CESG CLAIMS TESTED MARK SCHEME**

### **DECISION AUTHORITY GUIDE**

**Issue 3.0.0**

**February 2009**

**© Crown Copyright 2009 – All Rights Reserved**

Reproduction is authorised provided the document is copied in its entirety

IACS Delivery Office, CESG  
Hubble Road, Cheltenham  
Gloucestershire, GL51 0EX  
United Kingdom

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

**FOREWORD**

The CESG Claims Tested Mark (CCTM) 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.

From 7 April 2008, the Scheme is under the new ownership of CESG. This document sets out the process and objectives, applied by the CCTM Scheme Decision Authority (DA) in assessing IA Claims Documents (ICDs) and Test Reports, and in deciding whether to Award the CESG Claims Tested Mark to IS Products and Services.

Scheme Senior Executive  
CCTM Scheme, CESG

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

Address: CCTM Secretariat, 35 Endell Street, London WC2H 9BA

Telephone: 020 7240 7220

Facsimile: 020 7240 7221

E-mail: [secretariat@cctmark.gov.uk](mailto:secretariat@cctmark.gov.uk)

Website: [www.cctmark.gov.uk](http://www.cctmark.gov.uk)

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

**DOCUMENT HISTORY**

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

<b>Issue</b>	<b>Description of Changes</b>	<b>Date Issued</b>
3.0.0	Updated version of CCTM DA Guide document under the ownership of CESG	16/03/2009

**CONTENTS**

<b>I</b>	<b>OVERVIEW OF THE DECISION AUTHORITY (DA) ROLE</b> .....	<b>5</b>
1	Introduction.....	5
2	Document Control .....	5
<b>II</b>	<b>DA REVIEW PROCESSES</b> .....	<b>6</b>
3	Responsibilities of the Decision Authority.....	6
4	DA Review Requirements .....	6
<b>III</b>	<b>DA ASSESSMENT PROCEDURES</b> .....	<b>8</b>
5	First ICD Review .....	8
6	Second ICD Review .....	8
7	ICD Conference Call .....	8
8	Approval of ICD.....	8
9	Customer Questionnaire Review.....	9
10	Test Report Review.....	9
11	Supplementary Test Report Review .....	10
12	Test Report Conference Call .....	10
13	Decision on CCTM Award.....	10
14	Publication Review .....	11
	<b>APPENDIX A - DA REVIEW CHECKLISTS</b> .....	<b>12</b>
	<b>ICD Review Checklist</b> .....	<b>12</b>
	<b>Test Report Checklist</b> .....	<b>16</b>
	<b>APPENDIX B - DA REVIEW FORM</b> .....	<b>18</b>
	<b>APPENDIX C - GLOSSARY AND TERMINOLOGY</b> .....	<b>19</b>
	<b>References</b> .....	<b>22</b>
	<b>Abbreviations</b> .....	<b>22</b>

## **I OVERVIEW OF THE DECISION AUTHORITY (DA) ROLE**

### **1 Introduction**

- 1.1 The CESG Claims Tested 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 For an introduction and overview of the CESG Claims Tested Mark (CCTM) Scheme, including its procedures, management, operation and terminology, see “CCTM Scheme – Description of the Scheme” [\[DES\]](#). This guide should be read in conjunction with [\[DES\]](#).
- 1.3 This document sets out the process and objectives, applied by the CCTM Scheme Decision Authority (DA) in assessing IA Claims Documents (ICDs) and Test Reports, and in deciding whether to Award the CCTM to IS Products and Services.
- 1.4 For details of the assessment criteria and checks applied by the DA, see Appendix F of the “CCTM Scheme – Test Laboratory Guide” [\[TLG\]](#) and [Appendix A](#) of this Guide.
- 1.5 For details about Vendors responsibilities and admission to the Scheme, see the “CCTM Scheme – Vendor Guide” [\[VG\]](#).
- 1.6 For details about Test Laboratory responsibilities and participation in the Scheme, see the [\[TLG\]](#).

### **2 Document Control**

- 2.1 All the Scheme documents (including this Guide) will be subject to review and amendment. Changes to the Scheme documents will be published on the Scheme website and those participating in the Scheme will be notified at least 20 working days before substantive or material changes in the documents take effect.

## **II DA REVIEW PROCESSES**

### **3 Responsibilities of the Decision Authority**

- 3.1 The DA role is detailed in the [\[DES\]](#). The responsibilities of the DA role are to:
- a) ensure that the technical and procedural standards of the Scheme are applied to each application to the Scheme, based on the review of the ICD and provision of appropriate advice and guidance;
  - b) ensure the validity and completeness of the ICD claims and Marketing Statement prior to the Claims Test starting and prior to Award of the CCTM;
  - c) ensure that the ICD Test Approach addresses all ICD claims, together with any relevant publicly known vulnerabilities, and that the required combinations of platforms, including any associated witnessing, are adequate;
  - d) for IS Services, ensure that the proposed Customer Questionnaire addresses all ICD Claims;
  - e) make the final decision on the Award of a CCTM certificate based on the review of the Test Report and any associated Supplementary Test Report;
  - f) ensure that standards and procedures are reviewed regularly with development recommendations made to the Scheme Senior Executive.

### **4 DA Review Requirements**

- 4.1 ICDs, Test Reports, Supplementary Test Reports and Test Report Summaries must be reviewed by the DA in accordance with the decision and approval procedures detailed in the [\[VG\]](#) and [\[TLG\]](#). The set of DA processes and procedures described within this guide support the procedures outlined in the [\[VG\]](#) and [\[TLG\]](#).
- 4.2 A record of all DA review decisions related to an ICD, together with the required Vendor actions, must be documented by the DA in an ICD DA Review form (see [Appendix B](#)), which is issued by the Secretariat to the Vendor for action as appropriate.
- 4.3 A record of all DA review decisions related to a Test Report, Supplementary Test Report or Test Report Summary, together with the required Test Laboratory actions, must also be documented by the DA in a Test Report DA Review form (see [Appendix B](#)), which is issued by the Secretariat to the Test Laboratory for action as appropriate.

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

- 4.4 Any DA decision and Vendor and/or Test Laboratory actions agreed in ICD or Test Report Conference Calls should be recorded in the appropriate DA Review form.
- 4.5 Each DA review must be completed, and the DA Review form returned to the Secretariat, within 8 working days of receipt of the document from the Secretariat.
- 4.6 A written response to all DA Reviews must be supplied to the DA by the Vendor or Test Laboratory as appropriate via the Secretariat.

### **III DA ASSESSMENT PROCEDURES**

#### **5 First ICD Review**

- 5.1 The purpose of the ICD review is to ensure that the ICD meets the requirements of the Scheme as set out in the [\[VG\]](#), the Basic Checks listed in the [\[TLG\]](#) and the checks listed in [Appendix A](#).
- 5.2 The ICD must be reviewed in full the first time it is received. This first review must consider all of the ICD requirements. Comments on where the ICD does not meet these requirements must be included in the ICD DA Review.
- 5.3 Any ambiguity in the ICD that could lead to misunderstandings by the customer must be reported on the ICD DA Review form for clarification action by the Vendor. An updated ICD or written response will be required for any actions raised.

#### **6 Second ICD Review**

- 6.1 The DA must review the changes in the ICD, or a written response from the Vendor or Test Laboratory, against the ICD DA Review to ensure that all the points have been addressed.

#### **7 ICD Conference Call**

- 7.1 If outstanding issues remain after the Second ICD Review, a conference call should be arranged between the DA, Test Laboratory and Vendor. This is to resolve the outstanding issues and to agree what changes should be made to the ICD, either before testing starts, or after testing has been completed.

#### **8 Approval of ICD**

- 8.1 Any DA required changes to the ICD that impact the Claims Tests must be addressed by the Vendor and the updated ICD resubmitted to the DA for approval prior to commencement of the Claims Tests. Access to the updated ICD will also facilitate any DA advice that may be required during the subsequent Claims Tests.
- 8.2 If there are no outstanding issues from the ICD Reviews and all ICD Review recommendations have been addressed, the DA may confirm in the ICD DA Review that the ICD is approved and that Claims Tests may start. If outstanding issues remain from the Second ICD Review, then the DA may either report a conditional approval, subject to specified conditions, or refer the ICD to the Vendor for potential withdrawal of the Application.
- 8.3 Any conditional approval must be recorded in the ICD DA Review:

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

- a) Any required changes to the ICD which are clearly stated in the ICD DA Review, or in a written response from the Test Laboratory can be included in the revised copy of the ICD submitted with the Test Report after claims testing has been completed.
- b) Comments on the ICD (e.g. clarification on an aspect of the Test Approach) which can be addressed by email or conference call before claims testing starts and resolved within a given time.
- c) Minor changes to the ICD must be included in the revised copy of the ICD submitted with the Test Report after claims testing has been completed.

## **9 Customer Questionnaire Review**

- 9.1 For IS Services, Test Laboratory must submit the Customer Questionnaire (to be used as the basis of the proposed customer interviews) to the DA for review and approval prior to formal distribution to sample customers. This is to ensure that all ICD Claims have been addressed. The DA must also review the list of proposed customers that will be interviewed during the Claims Tests.

## **10 Test Report Review**

- 10.1 The purpose of the review of the Test Report is to review and approve the recommendations and observations of the Test Laboratory, and to ensure that the Test Laboratory has tested all the claims according to the Test Approach outlined in the ICD, and the requirements set out in the [\[TLG\]](#). A set of Test Report checks is also listed in [Appendix A](#).
- 10.2 The Test Report must be reviewed in full the first time it is received.
- 10.3 If the Test Report includes a recommendation to remove an ICD claim, and the claim is insignificant, does not devalue the rest of the claims being made, or is not essential to the effective use of the IS Product or Service, the DA can agree that this claim can be removed. The Marketing Statement may need to be updated to remove any related claims.
- 10.4 If the claim relates to a major piece of functionality which the Vendor is promoting in their marketing material and IS Product or Service documentation, the DA should not agree that the claim can be removed.
- 10.5 If the DA does not agree that the claim can be removed, the Vendor must be asked to assess what needs to be done to fix the identified problem, and how long this will take to fix so that the claim can be re-tested. The DA must agree the timescales for this, and can agree an

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

extension (up to 3 months) for the fix to be implemented and the claims retested.

- 10.6 If the affected claimed functionality is minor, does not devalue the rest of the claims being made or is not essential to the effective use of the IS Product or Service, the DA can exceptionally award the CCTM subject to the fix being implemented and the claim successfully re-tested within 3 months from the date of the CCTM Award.
- 10.7 If functionality does not work on some of the platform combinations (i.e. OS, Browser, Mobile Device, etc) specified for the claims testing, the ICD claims must be amended to mention the platform combinations that were successful. The IS Product or Service documentation must also make this point clear.
- 10.8 All the Test Laboratory recommendations and observations in the Test Report must be implemented, or if not, suitably justified in writing by the Vendor and/or Test Laboratory to the DA's satisfaction.

**11 Supplementary Test Report Review**

- 11.1 All clarifications on the Test Report raised by the DA must be demonstrably addressed by either the Test Laboratory or Vendor, (i.e. in a Supplementary Test Report or written response). This will be reviewed again by the DA in line with the above criteria.
- 11.2 All the Test Laboratory recommendations and observations in the Supplementary Test Report must be implemented, or if not, suitably justified by the Vendor and/or Test Laboratory to the DA's satisfaction.

**12 Test Report Conference Call**

- 12.1 If outstanding issues remain after the Supplementary Test Report Review, a conference call should be arranged between the DA, Test Laboratory and Vendor. This is to resolve the outstanding issues and to agree what is required to satisfactorily complete the ICD, claims testing, and/or its associated Test Reports, prior to the Award of the CCTM.

**13 Decision on CCTM Award**

- 13.1 If all outstanding issues have been resolved and all conditions stated in the DA Reviews have been met, then the DA may confirm the Award of the CCTM in the Test Report DA Review, subject to approval of the Final ICD and Test Report Summary during the Publication Review that occurs prior to formal announcement.

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

- 13.2 If there are minor changes to be made to the Final ICD or Test Report Summary following a review of the Test Report or associated Supplementary Test Reports, the DA may still Award the CCTM, subject to conditions. These conditions are changes being made to the Final ICD and Test Report Summary before the Award is publicly announced on the CCTM website.
- 13.3 If any outstanding issue remains unresolved following the Test Report Conference Call, then the DA will confirm that the Award of the CCTM cannot be made.

**14 Publication Review**

- 14.1 The Publication Review addresses the Test Report Summary and Final ICD, which must be reviewed and approved by the DA. This is normally after the Test Report has been reviewed, all outstanding actions on the Test Report or Supplementary Test Report have been approved by the DA and a decision has been made to Award the CCTM.
- 14.2 The DA will check the changes in the Final ICD and the Test Report Summary against all DA Reviews to ensure that all points have been addressed.
- 14.3 The DA will also check the Final ICD and Test Report Summary for consistency with the Marketing Statement. (See [Appendix A](#) - ICD Review Checklist.)
- 14.4 Any ambiguity in the Final ICD and Test Report Summary that could lead to misunderstandings by the customer should be reported on the DA Review form for clarification action by the Vendor or Test Laboratory as appropriate. An updated document or written response will be required for any actions raised.

## **APPENDIX A - DA REVIEW CHECKLISTS**

### **ICD Review Checklist**

#### Suitability

- 1 The ICD should not be for a complex solution which will take longer than 20 days to test, as this may not be suitable to be tested under the CCTM Scheme. A written rationale for the suitability of complex solutions must be submitted by the Vendor and Test Laboratory.

#### Format and Content

- 2 The ICD wherever possible should avoid the use of subjective terminology (e.g. "should counter threats").

#### Claims Statements

- 3 The Claims must be S.M.A.R.T (S = Specific, M = Measurable, A = Attainable, R = Realistic, T = Timely). Claims to work on any PC or all versions of an OS are not acceptable.
- 4 Claims must cover all the information security functionality in Section 2 of the ICD, the marketing material and user and administration guides.
- 5 Any platforms supported by the IS Product or Service functionality but which are not the platforms to be used in the Claims Tests, these must be documented as exclusions in section 2.2.4 (Out of Scope) of the ICD.
- 6 If some of the functionality for the IS Product or Service does not have a claim to be validated in the Claims Test, there must be a written justification for this and it must be documented as an exclusion in section 2.2.4 (Out of Scope) of the ICD. Any exclusion must not compromise normal use of the IS Product or Service. For example, including a claim about an audit trail but excluding audit trail management and analysis.
- 7 Where there are external processes needed to support a claim, these must be verified, e.g. If an IS Product tests that a client's patch levels and anti virus are up to date, there must be a claim to verify that there is a corresponding process for doing this.
  - 7.1 CCTM is a Government quality mark assured by independent testing. Purchasers of IS Products and Services that have been awarded the CCTM can be confident that any security-enforcing claims have been fully tested. All IS Products and Services must undergo the appropriate rigor to attain the CCTM. This may include the re-use of previous tests, conducted within the previous 4 months, as long as the results show that it was conducted in accordance with the processes laid down in the [\[TLG\]](#) and this fact is verifiable to the DA.

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

For any re-use of test results, it must be the same version without amendments or patches for the same, specified platforms.

- 8 If the IS Service to be tested is part of a group of services, it must be clear which other parts are not being tested. These should be stated in the ICD in the 'Out of Scope' Section.
- 9 The wording of the claim must be verifiable in practice. This is an area where technical advice may be required and discussions between the technical expert(s) and the Test laboratory may be required before testing could start, particularly for specialist testing. For example:
  - 9.1 a claim to block all unknown viruses is not verifiable, as "unknown" cannot be defined or tested.
  - 9.2 a claim to block all known viruses may be verifiable if there is a clear definition of what constitutes a known virus (e.g. the Wild List).
  - 9.3 for biometric products, a claim for false positive or false negative rates needs to be no more than 1 in 10,000. Claims for 1 in 100,000 or better cannot be verified under CCTM within 20 days testing.
  - 9.4 claims with an excessive scalability parameter (e.g. will support 1 – 10000 clients) cannot be tested in practice.
  - 9.5 tamper proof evidence claims require CESG advice.

#### Platforms

- 10 Section 2.1 must specify the exact version numbers (including service packs or models of the IS Products and IS Services to be tested, and the operating system(s), browser(s), mobile devices and any other software/hardware to be used to validate the claims. Details for both the client and server should be included. This information should be in a table format.
- 11 It is the Vendor's decision to propose which platforms should be used to test the ICD claims, based on their current marketing of the IS Product or Service. The version of the platform should be the most relevant to current user profiles. The platforms chosen by the Vendor are subject to approval by the DA during the DA Review.

#### Test Approach

- 12 The Test Approach should confirm how long the testing of the claims is likely to take. This should be no more than 20 working days. If longer, an explanation should be given for this.
- 13 The Test Approach must cover each claim specifically.

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

- 14 There must be a clearly defined link between the ICD Claims (ICD Claims Section 3.1) and the Test Approach (ICD Test Approach Section 3.3), with unique reference to claims in the Test Approach.
- 15 It must be clear which claims will be tested by the Test Laboratory, witness tested and the location(s) of the testing.
- 16 Testing should be carried out at the premises of the test laboratory. If this is not the case, then the ICD should supply adequate explanation for this.
- 17 The Test Lab's decision to use Witness testing must be clearly stated in the Test Approach (ICD Section 3.3). The Vendor should provide a justification for using witness testing and an explanation of how this will be conducted.
- 18 If the installation procedure of the IS Product or Service requires specialised assistance which is only available at the Vendors' premises, this should be noted in the ICD.

#### IS Services

- 19 The Test Approach must state which claims will be validated through functional testing, and how.
- 20 The Test Approach must state which claims will be validated by Customer questionnaires and inspections.
- 21 It must be clearly stated which claims will be supported by interviews with customers, and which customers will be interviewed.
- 22 The customers to be interviewed must be referred to the DA for approval. Customer details must include the name of the point of contact, their job title and the company's name. If a new IS Service is being assessed customer interviews can be deferred for up to 6 months after Award.

#### Marketing Statement

- 23 The Marketing Statement must only refer to the IS Product or Service which has been claims tested, and should not refer to any functionality, platforms or certificates which have not been claims tested.

#### Cryptographic Functionality

- 24 Where there is a reference to FIPS or CAPS certificates in Section 3.2, the Test Approach must include the Test Laboratory checking that these certificates are still current and relate to the exact version of the IS Product or Service being claims tested.
- 25 For IS Products or Services validated through the CCTM Scheme, there will be no verification that the cryptographic algorithm has been correctly implemented or assessment of the strength of the algorithm. In which

**CESG CLAIMS TESTED MARK SCHEME**  
**Decision Authority Guide**

case, the Test Approach must be restricted to testing that there is cryptographic functionality which is correctly invoked and that any patches have been applied.

- 26 Unless FIPS or CAPS certificates have been included in Section 3.2 (Existing Assurance Certificates) and subsequently validated through the CCTM Scheme, the ICD (including Marketing Statement in Annex B) should not include claims for specific algorithms.

#### Degaussing and Overwriting Services and Equipment

- 27 The degaussing equipment or overwriting application should be assessed by a Test Laboratory confirmed by CESG as having the Specialist Testing capability to test against the CESG degaussing or overwriting standard and approved by CESG.
- 28 Section 3.2 (Existing Assurance Certificates) of the ICD should include this information if the assessment has been completed and CESG approval achieved. Section 3.3 (Test Approach) should include details of when and where the assessment is to be carried out, and by which Test Laboratory, if this assessment is to be undertaken during the period of the Claims Test.
- 29 The ICD must include claims for the procedures and service provision of the degaussing or overwriting service.
- 30 The IS Service claims should, where relevant, include the requirements set out in the relevant HMG standard such as MPS, IS5, CESG Manual S for degaussing and overwriting (lower and higher levels).

#### Specialist Testing

- 31 Testing of certain technologies (see Appendix G of the [TLG](#)) can only be carried out by a Test Laboratory which has been confirmed by CESG as having the Specialist Testing capability for the technology. The Test Laboratory's schedule for UKAS accreditation must include a reference to the relevant Specialist Testing categories. If not, CESG must approve the Test Laboratory to undertake testing of any functionality which requires Specialist Testing.

## **Test Report Checklist**

- 32 The criteria which the DA will apply in the review of the Test Report is as follows:
- 32.1 The claims must have been tested as set out in the Test Approach in the ICD approved by the DA.
  - 32.2 If testing had to be suspended, clarification about which claims were tested, when testing was suspended and resumed and why only those tests were done should be included in the Test Report. Note that if any product or system modifications were applied during suspension, then complete re-testing (in the form of complete retests) must be performed.
  - 32.3 All requirements made in the last ICD DA Review for claims testing or changes to the ICD or inclusion in the Test Report have been addressed.
  - 32.4 The recommendations and observations in the Test Report for changes to ICD or the documentation for the IS Product or Service have been implemented by the Vendor and verified by the Test Laboratory. This has been confirmed in the Test Report.
  - 32.5 The Vendor has updated the ICD with changes recommended in the Test Report (e.g. wording of the claims changed to reflect what was actually validated through testing) and this new version has been submitted to the Scheme for review.
  - 32.6 The Vendor has updated the Documentation for the IS Product or Service including the User/Administration Guides, Help Files, Release Notes, Marketing Statement/ Material and Website. References to the updated Documentation are included in the Test Report.

## **Ease of Use**

- 33 This must state whether any difficulties or problems were experienced in following the procedures to install, configure or operate the IS Product or subscribe to the IS Service. These aspects should bear in mind the intended audience and their technical competence (e.g. whether trained administrators or normal users).
- 34 If the installation or configuration of the IS Product or Service requires specialist or consultancy help (at additional cost or included in the purchase price), this should be mentioned in this section.
- 35 This must comment on aspects of the IS Product which a system administrator should be aware of when implementing or maintaining the product.

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

- 36 This must comment on any specific connectivity requirements for the customer in using the IS Service.
- 37 This must include information that a purchaser of the IS Product or Service would need to use the IS Product or Service securely.

Quality of Documentation

- 38 The purpose of the IS Product or Service documentation must be included for all documentation included in Section 2 (References).
- 39 This must comment on how the IS Product or Service documentation was used by the Test Laboratory in claims testing.

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

**APPENDIX B - DA REVIEW FORM**

<b>CCTM DA REVIEW</b>	
<b>Product/Service:</b>	Name of Company, IS Product/IS Service and Version number
<b>DA Review Type:</b>	ICD or Test Report
<b>ICD/Test Report Version Number:</b>	Document Version number
<b>ICD/Test Report Date:</b>	Issue Date (use date on cover page of document)
<b>ICD/Test Report Reference:</b>	Company's reference number from front of ICD or Test Report
<b>Recommendation:</b>	Accept/Refer ICD/Test Report and/or Approve/Refer Application/Award of CCTM
<b>Reason for Recommendation</b>	
<b>Observations/Constraints/Timescales</b>	
<b>Reviewer:</b>	Name and Organisation
<b>Date:</b>	Date DA Review was issued

## **APPENDIX C - 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 Service specified in the ICD to be registered with the Scheme. This includes new and CCTM 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 ICD, and legitimate use of the CCTM on the specific version of the IS Product or Service tested.

### **Basic Checks**

A series of checks to be undertaken by Test Laboratories on ICDs, Final ICDs, Test Reports, Test Report Summaries and Supplementary Test Reports before submission to the Scheme Secretariat. Basic Checks are documented in [\[TLG\]](#).

### **Claims Test**

The process carried out by a Test Laboratory appointed under the CCTM Scheme for the independent testing of the security functionality of IS Products or 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 the [\[TLG\]](#).

### **Decision Authority (DA)**

The organisation appointed by the Scheme Senior Executive to review ICDs, to formally accept Applications made to the Scheme, to review Test Reports, Supplementary Test Reports and Test Report summaries and to decide the Award of the CCTM.

### **DA Review**

The process undertaken by the DA in assessing ICDs, Test Reports, Test Report Summaries and Supplementary Test Reports, and in deciding whether to Award the CCTM to IS Products and Services. The results of the assessment are recorded in a DA Review Form.

## **Final ICD**

The final version of the ICD approved by the Scheme and published with the Test Report Summary on the Scheme website only, when the Award of the CCTM is publicly announced.

## **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.

## **IA 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 CCTM IA Claims Test comprising of software, firmware and/or hardware and its associated administration, user guidance documentation and marketing material supplied by the Vendor.

## **IS Service**

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

## **ISO/IEC 17025**

The standards set out in the document entitled “ISO/IEC Guide 17025:2005: General requirements for the Competence of Testing and Calibration Laboratories” [\[ISO 17025\]](#).

## **Scheme**

The CCTM Scheme that is described in this document and the References.

## **Scheme Management Panel**

The organisation appointed by the Scheme Senior Executive to manage the day to day activities and operation of the Scheme.

### **Scheme Senior Executive**

The role that sets the objectives, policy and standards for the operation of the Scheme, and who appoints those who operate the Scheme on behalf of CESG.

### **Secretariat**

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

### **Supplementary Test Report**

An additional CCTM Test Report produced by a Test Laboratory and submitted to the Scheme which details additional Claims Test findings or clarification on issues raised in a previous Test Report of the same IS Product or Service, which will be used by the DA to assess whether the CCTM can be awarded.

### **Test Laboratory**

An organisation accredited by UKAS in accordance with the agreed standard ISO/IEC 17025 and the Generic Claims Test Method (see [\[TLG\]](#)) and appointed by the Scheme Senior Executive to undertake Claims 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 DA to assess whether the CCTM 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 approved by the Scheme and published with the Final ICD on the Scheme website, following the Award of the CCTM.

### **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.

### **User**

A person or organisation that purchases the IS Product or Service with IA features.

**CESG CLAIMS TESTED MARK SCHEME  
Decision Authority Guide**

**References**

[DES] CCTM Scheme - Description of the Scheme [See website [www.cctmark.gov.uk](http://www.cctmark.gov.uk)]

[VG] CCTM Scheme – Vendor Guide [See website [www.cctmark.gov.uk](http://www.cctmark.gov.uk)]

[TLG] CCTM Scheme – Test Laboratory Guide [See website [www.cctmark.gov.uk](http://www.cctmark.gov.uk)]

[ISO 17025] ISO/IEC Guide 17025:2005: General Requirements for the Competence of Testing and Calibration Laboratories

**Abbreviations**

CAPS	CESG Assisted Products Service
CCTM	CESG Claims Tested Mark
CESG	The National Technical Authority for Information Assurance
CSIA	Central Sponsor for Information Assurance
DA	Decision Authority
FIPS	Federal Information Processing Standard
HMG	Her Majesty's Government
IA	Information Assurance
ICD	Information Assurance Claims Document
IS	Information Systems
Scheme	CCTM Scheme
UK	United Kingdom
UKAS	United Kingdom Accreditation Service