CESG

Common Criteria Certification in the UK

UK IT security evaluation & certification scheme

Contents

Information Security The Key to Success 3

Basic Security Measures 4

Common Criteria - The Family Tree 5

An International Standard 6

IT Evaluation Services in the UK 7

Evaluation and Commercial Evaluation Facilities 8

Step by Step Guide to Evaluation 10

– Preparation 10

– Evaluation 11

– Certification and the Certification Body 13

– Re-evaluation 14

– Certification Maintenance 14

Evaluation Assurance Levels 15

For Further Information 18

Contacts 19

Information Security - The Key to Success

Now, more than ever, information is a key element in the success of any business. Information security is as important as the more traditional doors and locks for safeguarding the assets of a company. As more information is created, stored and moved around using computers, so the associated risk increases. In particular using networks or the Internet to share or move information increases the vulnerability of data.

Electronic business is expanding rapidly, bringing opportunity and risk in equal measure. E-commerce will flourish only where the security of the transaction is assured. Trading partners need to have confidence in the security of the information they exchange as well as in the subsequent storage and handling of that data.

The demands of information security are not confined to commercial businesses. Service industries are now searching for more direct ways to respond to their customer needs. Public organisations have to be sensitive to the privacy requirements of their clients and have a duty to ensure that appropriate precautions are taken to ensure the confidentiality and accuracy of personal records. Any security-dependent organisation, such as MOD, must ensure that its IT protection is continuously updated and re-aligned to cope with changing demands and the evolving threat.

Three essential elements of Information Security

Confidentiality - ensuring that only appropriate access is allowed to data - both from inside or outside the organisation

Integrity - ensuring that no unauthorised changes are made to data - either in storage or transmission

Availability - ensuring that data is accessible as required

Basic Security Measures

All organisations need to protect their information by adopting appropriate security measures. These can be organisational, physical, technical or educational. Such measures must be based on a coherent security policy. This policy must be derived from a sound assessment of the threat to an organisation's information and the impact of corruption or loss of that information. Advice on constructing and implementing a security policy is available in the Code of Practice for Information Security Management, BS7799, and in the DTI's Information Security Assurance Guidelines for the Commercial Sector.

Underpinning all of these security measures is the security assurance provided by the software or the IT system itself. The security features offered by software are aimed at ensuring the three essential elements of Confidentiality, Integrity and Availability. What is required is an objective assessment of these features to determine how well they perform their stated security functions.

Any such assessment must be carried out against clearly defined methods and objectives. The results must be documented and repeatable. The assurance level awarded must have meaningful parameters. The end result must be to provide a level of assurance which is commensurate with the environmental risk and within realistic financial boundaries.

Because information technology extends beyond national boundaries it is also vital that security assurance is defined using internationally accepted terms and standards - that way everyone has a clear understanding of what assurance is being offered. This benefits both users and developers:

- Users can easily compare one product to another to see what parts of the security functionality have been tested to what level.

- Developers can demonstrate to an international market that their product has gained an objective confirmation of the validity of its security claims.

Common Criteria - The Family Tree

Recognising the need for independent and objective testing, the United Kingdom has been working closely with other countries to formulate the rules under which this testing should be carried out. Since 1990, work has been going on to bring together a number of national and international schemes in one, mutually accepted framework for testing IT security functionality. The national communications security authorities of the United Kingdom, the United States, Canada, France, Germany and the Netherlands collaborated with the International Standards Organisation (ISO) in this project which culminated in the publication of the Common Criteria (CC). CC version 2.1 has now been recognised as a formal standard - ISO 15408.

The Common Criteria are a development of previous standards and schemes used by various nations:

The United States - Trusted Computer System Evaluation Criteria (TCSEC) and the draft Federal Criteria.

Canada - Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Europe - Information Technology Security Evaluation Criteria (ITSEC)

These previous schemes evolved and influenced each other as countries reacted to changing standards in the IT environment and in response to changing threats or attacks. Development was aimed at increasing the flexibility of the various criteria and ensuring that testing remained relevant and effective.

Common Criteria version 2.1 is now an International Standard - ISO 15408

CC Certificates issued by the UK are recognised internationally as follows:	
EAL1-4	US, Canada, Australia, New Zealand, France, Germany, Finland, Greece, Italy, Netherlands, Norway, Spain, Sweden, Switzerland
EAL5-7	France, Finland, Greece, Italy, Netherlands, Norway, Spain, Sweden, Switzerland

An International Standard

The Common Criteria aim to harness the strengths of previous standards. The TCSEC Scheme maintained that functionality and assurance were indivisible - the same standard specified both what an operating system must do, and how to check the implementation. The strength of this approach was the production of functional standards for operating systems (the C1 - A1 ratings). The weakness lay in the fact it was cumbersome to adapt the standard to address new requirements. With ITSEC, the standard only prescribed assurance activities. Security functional properties were specified in the Security Target as part of a specific evaluation. The advantage of this approach was that it adapted readily to new types of product, but the downside was that it was less easy for consumers to compare the functionality offered by two certified products.

Common Criteria provide two catalogues of components to allow the assurance and functionality requirements to be specified using standard terminology. In this way the Common Criteria unite the best methodology for IT security testing as developed by its premier exponents over the past decade.

Because Common Criteria certificates are recognised by all the signatory nations, IT developers no longer have to go through different evaluation processes in different countries. Evaluation is more straightforward and no effort is wasted in duplication.

Although the Common Criteria form a new standard based on previous testing regimes, this does not mean that certificates awarded under previous criteria are invalid. While the demand exists, evaluations will be available in the UK under the ITSEC formula and the resultant certificates will continue to be recognised by the European partners and Australia and New Zealand. Where required, a dual certification can be carried out to both CC and ITSEC simultaneously. The UK Certification Body is also happy to discuss conversion to Common Criteria with developers of products certified under ITSEC. By making substantial re-use of the original ITSEC evaluation this offers a cost effective option for developers who wish to extend the market reach of their certified product.

IT Evaluation Services in the United Kingdom

Trusted Service

The UK Scheme was established in 1991 as a joint effort by the Department of Trade and Industry and the Communications-Electronics Security Group (CESG). The UK IT Security, Evaluation and Certification Body is itself part of CESG, the government organisation charged with ensuring the security of all government and military communications. CESG Certifiers operate to the highest standards of professional competence, technical objectivity and commercial confidentiality. All personnel are subject to comprehensive background checks and the Certification Body itself is housed in a secure site. The Certification Body has achieved accreditation to the EN45011 (ISO Guide 25) standard for certification bodies.

The UK has a decade's experience of operating a commercial evaluation and certification scheme

Cost Effective Service

We have always recognised however, that security has financial implications and since its inception, the Certification Body has worked alongside commercial laboratories to provide a technically stringent testing service that is competitive and cost effective. Developers can choose from five testing laboratories ensuring competitive tendering for evaluations.

The provision of a cost effective service is one of the UK CB's highest priorities

Timely Service

The UK Certification Body is committed to working alongside developers in order to meet their timescales. Developments in communications and IT software are constant and rapid for developers, so it is important that evaluation and certification take place within a reasonable timeframe.

The UK CB is committed to matching developers' efforts in obtaining timely certification

Evaluation and CLEFs

IT security testing as part of an evaluation is carried out under the supervision of the Certification Body by accredited laboratories known as CLEFs: CommerciaL Evaluation Facilities. The CLEFs carry out the analysis of design, implementation, development, production and distribution against agreed security standards. CLEFs are appointed after a rigorous process which ensures that they meet the required standards of technical expertise and operating procedures to carry out evaluations. All the CLEFs are well-established companies which have provided computer hardware and software services over many years. In each case, their operations cover both the public and private sectors and all have practical experience of the issues associated with implementing sophisticated secure systems and networks. Each CLEF is inspected annually by the UK Accreditation Service (UKAS) and conforms to the EN 45001 (ISO Guide 25) standard for test facilities.

A list of UK CLEFs with their full contact details is on page 19.

The UK Scheme has successfully tested and certified a wide range of commercial products and secure systems. Developers using the Scheme have included Argus, Baltimore, Compaq, IBM, Sun, Microsoft and Oracle. Developers are generally internationally based and the Scheme has welcomed evaluations from the United States, Canada, Europe and the Far East. As new products enter evaluation or gain certification their details are updated on the Scheme website (www.itsec.gov.uk). Certification Reports and some Security Targets are available to download. Here you can also find details of products evaluated under ITSEC and signposts to other CC products certified by Schemes recognised by the UK. For information on other services offered by CESG please access the general website (www.cesg.gov.uk).

To date, the UK Scheme has issued ITSEC or CC Certificates for over 230 products and secure systems with 70 currently in evaluation.

The Evaluation Process

A commercial decision

For a developer contemplating evaluation the decision can only be made after an assessment of the commercial factors involved. Success in putting a product through the Common Criteria testing process is linked to quality development procedures, careful documentation and adequate resourcing. Against any cost implications must be weighed the benefits of access to a broader market and gaining a competitive advantage for the product. As IT users become more aware of the risks to their information then the demand for tested and certified products increases. Legislative measures in many countries now stipulate certification for certain applications and access to the traditional high security defence market can be dependent on demonstrating a high level certification. Certification can give you the edge in the national or international marketplace.

Once the decision has been taken to seek evaluation then the UK Certification Body, or any of the CLEFs, are on hand to offer advice and to assist in preparing the product for evaluation.

The Evaluation Process

Vendor provides evidence including technical support

CLEF performs assessment of product against security target

CLEF raises problem reports and notifies Certification Body

Vendor resolves problems

CLEF documents results as work proceeds

CLEF completes evaluation and submits ETR to Certification Body and vendor

Certification Body reviews ETR to confirm certification can proceed

Certificate issued

Maintenance

Step by Step Guide to Evaluation

Preparation

Define the product for evaluation -

There may be different versions of a product in production or preparation. Evaluation can start on one release of a product and then progress through a second release. Or parts of a product may already have been evaluated under different schemes - for example under ITSEC or US TCSEC. In some cases, evidence from past testing can be incorporated into new evaluations to cut costs and timescales. Bear in mind that the CC Certificate will only apply to the precise version of the product in its tested configuration running on the supporting platforms specified.

Specify the functionality -

The functionality required is dependent on the demands of the marketplace and will evolve in line with perceived threats. Customers will have their own requirements which may have been defined in a Protection Profile.

Specify the assurance level claimed -

These range from EAL1 up to EAL7. Each assurance level places increasing demands on the developer for evidence and testing.

Obtain costings from CLEF and Certification Body -

The CLEFs are competitive commercial organisations. Quotes should be obtained and carefully compared before a choice is made. The Certification Body is a Government organisation and is required to recover its costs. A questionnaire should be obtained from the CB and a quote for certification services will be issued based on the information supplied.

Prepare the evidence -

Some of this, such as the design documentation, is a normal product of the development cycle. The production of a Security Target is a key part of the evaluation process. In it the developer defines the security functions and assurance measures to be assessed in the evaluation. The Security Target will become a publicly available document (we can work with you to ensure that no proprietary information is disclosed) so that end users can see exactly what parts of a product have been evaluated and can match this to their own security needs. Consultancy is available either from a CLEF or from an independent specialist, to assist in the production of the Security Target or in the review of other product documentation prior to evaluation.

Evaluation

Once a CLEF has been engaged and agreement reached with the Certification Body on the suitability of the product for evaluation, then the testing process begins in earnest. There are several stages to evaluation covering the following activities:

- Production of Evaluation Work Programme
  This is where the various stages of the work to be carried out are identified. The time schedule laid out for the testing should be realistic.
- Assessment of the Security Target
  This is fundamental as all evaluation work is performed against this document. The ST should be clear, consistent and demonstrate how the TOE counters the identified threats.
- Assessment of system correctness
- Testing for evidence of security
- Assessment of the development environment
- Assessment of the operational environment
- Checking for known vulnerabilities
- Penetration testing
- Production of comprehensive evaluation reports

We strongly recommend that the developer or sponsor appoint a project manager to coordinate all the evaluation activities. Our experience has shown that close cooperation between CLEF and developer is the key to a smooth evaluation and a clearly defined point of contact facilitates that cooperation.

As testing progresses the evaluators produce detailed reports on the assessments and the results obtained. The minor faults discovered during testing are notified in the observation reports. These provide useful feeback in highlighting problem areas. The impact of these faults is assessed in the context of how the product is to be used and any advice provided by the developer to overcome the fault. If the evaluators discover flaws which could be exploited by an attacker then the Certification Body must be notified. It is our policy that such flaws must be rectified before a certificate can be granted.

Other observation reports may detail aspects of a product that have no current impact but which may become significant in future evaluations. This might include comments on the development environment or instances of unusual coding practices. Such problems are not necessarily a bar to certification.

What is a Protection Profile?

Put simply a Protection Profile is a set of requirements designed for a set of circumstances. It consists of:-

A list of threats

A list of functional requirements

A list of assurance activities

A justification that these address the threat

Protection Profiles can be designed by a group of prospective consumers who have similar IT security needs, or by the software developer himself.

A Protection Profile is not related to any given product or system, rather it defines a user's needs independent of any specific product. Certification against a Protection Profile will specify the extent to which requirements of the Profile have been met.

A Protection Profile is particularly useful in assisting the formulation of procurement specifications. A number have already been written and more are in preparation.

Protection Profiles already issued include :

Controlled Access

Role Based Access Control

Labelled Security

Oracle Commercial Database Management System

Oracle Government Database Management System

Application level Firewall

Traffic filter Firewall

Visa and SCSUG Smart Card - in draft

Certification Body role during evaluation

The Certification Body is active at all stages of the evaluation, although the bulk of the work is done by the CLEF and the developer. The Certification Body approves the Security Target and the Evaluation Work Programmes. With the exception of EAL1 evaluations the Certifier attends a task start-up meeting with the CLEF and the developer in order to discuss the evaluation and agree the schedules for activity. Potential problems can be identified here and actions agreed to remedy them.

As testing progresses the Certifier monitors the activities undertaken and examines any observation reports together with their resolution. A key objective of the Certification Body is to check that the evaluation has been conducted in accordance with the methodology laid out in the Common Criteria. The evidence provided must support the evaluation conclusions and the appropriate testing must have been carried out to justify the claimed evaluation assurance level.

What is a Security Target?
This is the specification of the security functionality and assurance and the environment in which this is designed to work.

The Certifier may attend one or more evaluation progress meetings where the conduct of the evaluation is reviewed, and on complicated evaluations, new work schedules agreed. The Certifier also normally attends penetration testing.

The evaluation process culminates in the preparation by the CLEF of an Evaluation Technical Report (ETR). This totals all the CLEF findings and presents the test evidence. The ETR is then sent to the Certification Body.

Cerification

The Certifier reviews the ETR and raises comments on areas where additional explanation might be needed or test results are unclear. All the documentary evidence provided by the evaluators is taken into account and test results are compared to the Security Target to ensure all objectives have been met. Comments are passed to the CLEF and to the developer and their responses assessed. When the Certifier is satisfied with the body of evidence presented to him he writes a Certification Report and a Certificate is granted.

What is a TOE?
A Target of Evaluation. This covers the parts of a product and its documentation that provide the functionality to counter the threats defined in its Security Target.

Re-Evaluation and Certificate Maintenance

Inevitably IT products develop and it is sensible to take steps to develop the Certificate in tandem. The Certification Body will advise on whether a re-evaluation is necessary if a product has been modified. The work involved can be minimised during the first evaluation by classifying product components according to their influence on the security features. Whenever changes are made to the evaluated product, the developer can use the classification to determine the impact on certification more easily and identify appropriate action.

Vulnerabilities can be discovered in products which have already been evaluated. In such cases it is normal practice for the developer to issue a patch. Where a product is in the Certificate Maintenance Scheme the issue of a patch, or patches, does not invalidate the certificate. It is a consequence of a graded scheme that moderate level assurances do not detect and remove all vulnerabilities. It must also be recognised that the rapid evolution of products and the environment will introduce the possibility of vulnerabilities that had not been envisaged at the time of the original certification. Countries participating in the development of the Common Criteria are in the process of formalising an assurance maintenance process comparable with the Certificate Maintenance Scheme offered by the UK Certification Body for ITSEC certificates. This maintenance is projected to be under the control of the developer, either directly or via a CLEF.

Assurance Levels

Functionality and Assurance Classes

Common Criteria have 11 functionality classes and 10 assurance classes as follows:

Functionality	**Assurance**
Audit	Protection Profile evaluation
Cryptographic Support	Security Target evaluation
Communications	Configuration Management
User Data Protection	Delivery and Operation
Identification and Authentication	Development
Privacy	Guidance Documents
Protection of TOE Security Functions	Life Cycle Support
Resource Utililization	Maintenance of Assurance
Security Management	Tests
TOE Access	Vulnerability Assessment
Trusted Path/Channels	

Each of these is broken down into families and then into components.
This gives great flexibility in describing the functional and assurance requirements.

The Common Criteria have seven Evaluation Assurance Levels (EALs), from EAL1 to a maximum level of EAL7. These have an approximate correspondence to the ITSEC levels as shown below:

Common Criteria	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6

These assurance packages are designed to provide a balanced grouping of assurance elements for general use. The levels represent ascending levels of confidence that can be placed in the Target of Evaluation (TOE) meeting its security objectives. The higher the level, the greater the degree of rigour applied in assessing whether the TOE has met its security requirements, for example, by intensifying the analysis and search for security vulnerabilities.

EAL1 Functionally tested

Analysis is supported by independent testing of a sample of the security functions in order to understand the security behaviour. EAL1 is applicable where confidence in correct operation is required but the security threat assessment is low. This assurance package is particularly suitable for legacy systems as it should be achievable without the assistance of the developer.

EAL2 Structurally tested

Analysis of the security functions exercises a functional and interface specification and the high-level design of the subsystems of the TOE. There is independent testing of the security functions and evidence is required of developer 'black box' testing and development search for obvious vulnerabilities. EAL2 is applicable where a low to moderate level of independently assured security is required.

EAL3 Methodically tested and checked

Analysis is supported by 'grey box' testing, selective independent confirmation of the developer test results and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required. EAL3 is applicable where the requirement is for a moderate level of independently assured security, with a thorough investigation of the TOE and its development, without incurring substantial re-engineering costs.

EAL4 Methodically Designed, Tested and Reviewed

Analysis is supported by the low-level design of the modules of the TOE and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities. Development controls are supported by a life-cycle model, identification of tools and automated configuration management. EAL4 is applicable where a moderate to high level of security is required, although some additional security-specific engineering costs may be incurred.

EAL5 Semiformally Designed and Tested

Analysis includes all of the implementation. Assurance is supplemented by a formal model, a semiformal presentation of the functional specification and high level design and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure resistance to penetration attackers with a moderate attack potential. Covert channel analysis and modular design are also required. EAL5 is applicable where the requirement is for a high level of security in a planned development coupled with a rigorous development approach.

EAL6 Semiformally Verified Design and Tested

Analysis is supported by a modular approach to design and a structured presentation of the implementation. The independent search for vulnerabilities must ensure resistance to penetration attackers with a high attack potential. There must be a systematic search for covert channels. Development environment and configuration management controls are further strengthened. EAL6 is applicable where a specialised security TOE is required for high risk situations.

EAL7 Formally Verified Design and Tested

Here the formal model is supplemented by a formal presentation of the functional specification and high level design, showing correspondence. Evidence of developer 'white box' testing and complete independent confirmation of developer test results are required. EAL7 is applicable where a specialised security TOE is required for extremely high risk situations.

For Further Information...

This guide is intended as an introductory overview to certification in the UK against Common Criteria. Further reading is recommended for developers or product sponsors intending to enter evaluation. All of these documents may be obtained free of charge from the Certification Body.

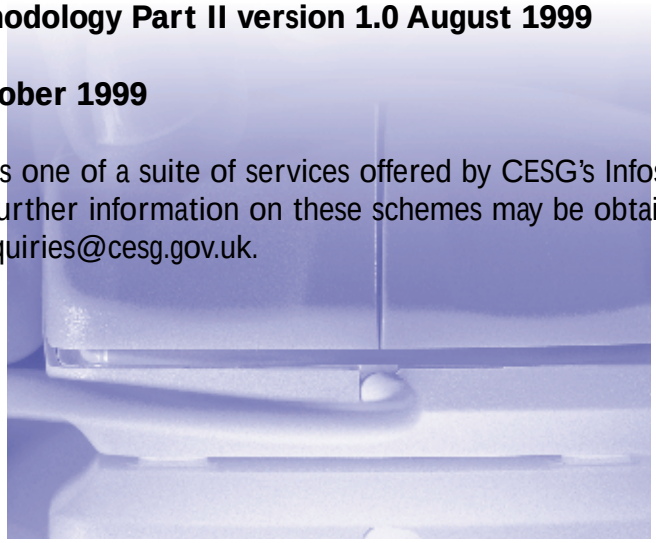
UKSP 01 Description of the Scheme updated 2000

UKSP 04 Developer's Guide updated 2000

Common Criteria Evaluation Methodology Part II version 1.0 August 1999

Common Criteria User Guide October 1999

Certification against Common Criteria is one of a suite of services offered by CESG's Infosec Assurance and Certification Services. Further information on these schemes may be obtained via the website www.cesg.gov.uk, e-mail enquiries@cesg.gov.uk.



Contact Addresses

UK IT Security Evaluation and Certification Body
PO Box 152
Cheltenham
Gloucestershire GL52 5UF

Tel: +44 (0) 1242 238739
Fax: +44 (0) 1242 235233

http://www.itsec.gov.uk
email: info@itsec.gov.uk

CLEFS:

Admiral Management Services Ltd (CLEF)
Kings Court
91-93 High Street
Camberley
Surrey GU15 3RN

Tel: +44 (0)1276 686678
Fax: +44 (0)1276 691028

Contact: Ralph Worswick
worsw_r@admiral.co.uk

Logica UK Ltd (CLEF)
Cobham Park
Downside Road
Cobham
Surrey KT11 3LG

Tel: +44 (0)1932 869118
Fax: +44 (0)1932 869119

Contact: Nigel Smith
smithn@logica.com

EDS Ltd (CLEF)
Wavendon Tower
Wavendon
Milton Keynes
Bucks MK17 8LX

Tel: +44 (0)1908 284234
Fax: +44 (0)1908 284393

Contact: Trevor Hutton
trevor. hutton@edl.uk.eds.com

Syntegra (CLEF)
Guidion House
Harvest Crescent
Ancells Park
Fleet
Hants GU13 8UZ

Tel: +44 (0)1252 778845
Fax: +44 (0)1252 811635

Contact: Julian Straw
julian.straw@syntegra.bt.co.uk

Contact: Allison Barnett
allison.barnett@syntegra.bt.co.uk
Tel: +44 (0)1252 778903

IBM Global Services (CLEF)
Meudon House
Meudon Avenue
Farnborough
Hants GU14 7NB

Tel: +44 (0)1252 558081
Fax: +44 (0) 1252 558001

Contact Bob Finlay
bob_finlay@uk.ibm.com


CESG
UK ITsec
dti
Department of Trade and Industry
ISO
IEC