Common Criteria FAQ

What is the Common Criteria?

The Common Criteria (CC) is an international standard (ISO/IEC 15408) for evaluating the security properties of IT products and systems. It defines a framework for the oversight of evaluations, syntax for specifying the security requirements to be met and a methodology for evaluating those requirements. The CC is used by governments and other organizations around the world to assess the security of information technology products and is often specified as a pre-requisite to procurement.

See www.commoncriteriaportal.org for more information or to obtain the standard.

Who recognizes CC certificates?

At the time of writing: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, the Netherlands, New Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States. The up to date list of participant nations is maintained on www.commoncriteriaportal.org. Other nations and organizations may also make use of CC certificates.

What is the CC evaluation process?

There are three parties involved in the CC evaluation process:

1. **Vendor or Sponsor.** The vendor engages an accredited lab and submits their product and associated evidence for evaluation.

2. **Lab.** The lab performs the evaluation and reports evaluation results to the scheme. Evaluation is iterative in nature and the vendor is able to address findings during the evaluation.

3. **Scheme.** Certificate authorizing schemes (also known as a certification body) issue CC certificates and perform certification/validation oversight of the lab. Each scheme has its own policies with regard to how the CC is used in that country and what products may be accepted into evaluation.

What gets evaluated?

The following provides a high-level overview of what gets evaluated:

- **Security Target evaluation.** Evaluation of the Security Target (ST) - a claims document that specifies the security functions under evaluation and the security assurance requirements being met.

- **Protection Profile evaluation.** Evaluation of the Protection Profile (PP) – an implementation-independent statement of security needs for a technology type.

- **Design evaluation.** Evaluation of design documents - at the most basic level this will simply be an interface specification. Depending on the assurance requirements this can include multiple layers of very detailed design specs and source code review (this is becoming less common).

- **Guidance evaluation.** Evaluation of all the guidance documents that are shipped with the product and any CC specific addendum or 'Secure Installation Guide' for achieving the evaluated configuration.

- **Life-cycle evaluation.** Evaluation of configuration management practices, delivery procedures and security bug tracking (flaw remediation). Can also include development practices and site security audits.

- **Functional testing.** The evaluators repeat a sample of the developer's functional tests and come up with some independent tests to confirm the operation of the security functions as specified.

- **Penetration testing.** The evaluators perform vulnerability analysis and penetration testing.

Whether a particular evaluation activity gets performed is dependent on the assurance requirements that are specified in the ST.

What is a Security Target?

A Security Target is the document that defines the Target of Evaluation (TOE), that is, the product configuration and version, and scope of security functionality being evaluated. The CC allows the TOE to be all or part of a product or system. The Security Target is put together using CC constructs and includes a threat model, environmental assumptions, security objectives, security functional requirements and security assurance requirements. A Security Target may conform to a Protection Profile but is not required to. A Security Target (written by vendor) goes beyond a Protection Profile (written by consumer) by including a description of how the product achieves the defined requirements.

Security Target examples may be found at http://www.commoncriteriaportal.org/products.html

What is a Protection Profile?

A Protection Profile is a requirements statement put together using CC constructs. Protection Profiles are generally published by governments for a specific technology type, for example, Firewalls, as part of procurement policy. A Protection Profile specifies both functional and assurance requirements. It is not necessary for a Security Target to claim conformance to a Protection Profile however some schemes will only accept products into evaluation that claim conformance with scheme approved Protection Profiles. A given product may conform to multiple Protection Profiles.

A centralized repository of Protection Profiles is published at http://www.commoncriteriaportal.org/pps/

What is a Collaborative Protection Profile (cPP)?

Work is underway to develop a set of Collaborative Protection Profiles (cPP) developed by international technical communities and approved by multiple schemes. Additional information on this initiative is published at http://www.commoncriteriaportal.org/communities/technical_communities.cfm

What is an Evaluation Assurance Level?

An Evaluation Assurance Level (EAL) is a predefined set of assurance requirements ranging from EAL1 (Functionally Tested) to EAL7 (Formally Verified Design and Tested). A Protection Profile or Security Target may reference an Evaluation Assurance Level (EAL) or may instead specify a custom set of assurance requirements.

How long does evaluation take?

Evaluation projects will typically take one year, however the time of an evaluation depends on many factors such as product complexity and assurance claims. An evaluation project includes product preparation (including testing), documentation preparation, lab engagement, lab evaluation and finally certification by the government oversight body.

What happens when a certified product changes?

CC certification only applies to the configurations and versions specified by the certified Security Target. So for example, if your product goes from v1.0 to v1.0.1, the certificate no longer applies to that new version. There is however a process called Assurance Continuity to accommodate product changes.

What is Assurance Continuity?

Assurance Continuity allows minor changes to be performed to an evaluated product and subsequent versions appended to the original CC certificate. Where changes are security related (and are classified as 'major'), Assurance Continuity allows these changes to be rapidly evaluated through 're-evaluation', which utilizes results from the original evaluation. **Note:** Individual schemes have differing policies regarding the use of Assurance Continuity.

Further details about the Assurance Continuity program are included in the Common Criteria Recognition Arrangement (CCRA) Supporting Documents at http://www.commoncriteriaportal.org/cc/#supporting

Why buy Common Criteria certified products?

CC certified products have undergone a rigorous evaluation process performed by accredited third-party security labs in accordance with internationally accepted criteria and a government-managed framework. Specific advantages include:

- Security functions have been verified and tested
- Product has passed vulnerability assessment and penetration tests
- Developer processes have been assessed
- Product meets checkbox CC procurement requirements

Why get your product Common Criteria certified?

In addition to the advantages listed above, reasons to get your product certified include:

- Meet government and industry procurement requirements
- Demonstrate a strong commitment to security through third party evaluation
- Product and process improvements may be identified during evaluation
- CC certificates issued by one scheme are mutually recognized by all participant nations
- CC certification provides competitive market differentiation

What is the CCUF and how do I join?

The Common Criteria Users' Forum mission is to provide a voice and communications channel amongst the CC community including the vendors, consultants, testing laboratories, Common Criteria organizational committees, national schemes, policy makers, and other interested parties.

You can join the CCUF by registering at https://ccusersforum.onlyoffice.com/auth.aspx