Common Criteria

Common Criteria (CC) also known as ISO/IEC 15408 is an international standard for security evaluation and certification of IT products. It is often required by government agencies and companies as an instrument to demand a certain level of security and quality for IT products.

The process to evaluate and certify IT products can be described in three steps:

- A developer develops an IT product. The security claims for this product are specified in a document called the Security Target.
- An accredited lab evaluates the product, according to the claims in the Security Target using the Common Criteria. The accredited lab document the assessment in evaluation reports.
- A certification body verifies that the lab worked correctly and certifies the product based upon the Security Target and the reports provided by the accredited lab. The certification body will issue a certificate and a certification report.

atsec is accredited to do evaluation under the schemes in Sweden, Germany, Italy, Singapore and the US. To date, atsec has successfully performed more than 175 evaluations. We have also taken a very active part in developing the Common Criteria standard, as well as in a number of other security standards.

More information on CC

If you are interested in knowing more about Common Criteria, downloading the standard or finding certified products, please visit:
www.commoncriteriaportal.org

For more information on CSEC, the certifying organization of Sweden, please visit:
www.fmv.se/csec

Common Criteria Evaluation

The evaluation process is normally divided into six parts, so called or assurance classes:

- **Security Target evaluation**
  Review of the Security Target to ensure that this is a complete, consistent and sound specification of the security functionality for a Common Criteria evaluation.
- **Development**
  Review of the product's architecture, design and interface specifications. This is necessary to be able tp perform testing and vulnerability analysis of the product.
- **Guidance documents**
  Review of the documentation for installation and operation of the product. This is to ensure that it can be installed and operated securely.
- **Life-cycle support**
  Review of the security of the development environment, the Configuration Management Systems (CM system) used during product development, delivery of the product to the customer and bug tracking. In evaluations at higher assurance levels, also the tools used in the product development are reviewed.
- **Tests**
  Review of the developer tests, of the security functions, as well as performing the evaluator's own tests. This is to ensure that the security functions are working as specified.
- **Vulnerability assessment**
  The evaluator performs vulnerability assessment and penetration testing. This is to ensure that the security cannot be violated if the product is used as intended.

Evaluation Assurance Level

Evaluation can be performed to different depth and effort. The Common Criteria define so called Evaluation Assurance Level (EAL) for this purpose. The levels are ranked on a seven-point scale, where 1 represents the lowest assurance level and 7 represents a very high level of assurance. This scale is commonly used in evaluations, unless a Collaborative Protection Profile (cPP) is used instead. For details see below.
The majority of evaluations are performed at levels EAL 2 to EAL 5. In general, the workload and assurance (confidence) increases with each level, although the workload itself varies mainly depending on the complexity and architecture of the product.

Protection Profile

Protection Profiles (PP), are specifications for types of products produced by different authorities and organizations. There are no requirements in the standard that a certain PP is to be followed, and atsec has performed several evaluations where one has not been used.

Collaborative Protection Profiles (cPP) are also specifications defined for certain categories of products, for example network equipment, firewalls and USB flash drives. They do not reference an EAL but contain assurance activities specific for the product category they target.

CC Evaluation with atsec

Both a Security Target and the security evaluation and certification are on one hand very formal, but they are also predictable once they are understood. In such a process we do not want to have surprises.

For this reason it makes sense to involve the evaluation lab at a very early stage to identify the key issues such as the **scope** of the product to be evaluated the so called Target of Evaluation (TOE); the claimed **security functionality** and the **assurance level**. But it is also important to understand if the product and its development environment meet the selected security requirements.

atsec performs such readiness assessments to determine the scope of the TOE, the security functionality and assurance measures, but also to understand the readiness of the product and developer for the evaluation. This helps to understand the effort of the evaluation, both on the evaluator side as well as on the developer side.

atsec not only offers evaluations of IT products, but also developer support in terms of independent consultants who can provide the necessary information needed for the evaluation. Usually, atsec performs a Readiness Assessment with the developer to get an overview of the product and the development environment, before the evaluation commences.
atsec offers the following Common Criteria services:

- Readiness Assessment
  An evaluator visits the developer for a short CC training, analysis of the product to be evaluated and a review of the development environment. After this visit the developer receives a tailored offer with cost proposal, including suggestions on necessary improvements and consultant support.

- Product evaluation
  Evaluation of the product, which later on is certified by a national certifying organization. We are accredited in multiple schemes so we can offer some level of flexibility to our customers.

- Consultant services
  atsec offers consultant support in producing Security Targets, as well as some other documentation required for the evaluation. We offer this service as support to our evaluations.

- Training
  atsec offers trainings, from basic to expert levels, in Common Criteria for developers as well as for national authorities. The extent and content of the training varies and is determined in accord with the customer's requests.

Other services offered by atsec

Common Criteria is one of many security services we offer. For more information on what other services atsec offers, please visit: www.atsec.se
For more information on how we can help you or other questions about Common Criteria, please contact us on: info-se@atsec.com

atsec information security
atsec information security was founded in 2000 and is an independent, standards based security consultant and security company based in Danderyd, Stockholm. We also operate internationally, in Germany, the US, China and Italy and we have performed many successful projects with different companies and authorities. Our more than 80 employees have extensive international experience and technical expertise within the areas of information security and IT security.

www.atsec.com
info-se@atsec.com