Contact: info@appluslaboratories.com

Common Criteria Security Evaluations

Ensure the security level of an IT product under the Common Criteria (ISO 15408:2005)

What is Common Criteria?

Common Criteria is an international recognized standard to evaluate **IT products security functionalities and assurances (ISO 15408)**. The standard is based on 7 evaluation assurance levels (EAL) of increasing stringency. The vendor choses the EAL to claim and submits the product to a security evaluation process conducted by an accredited independent laboratory.
Common Criteria certifications (from EAL 2 to EAL 4) are recognized by 27 countries that signed the **Common Criteria Recognition Agreement (CCRA).** Additionally, 10 European Countries signed the **SOGIS** mutual recognition agreement for Common Criteria certification of higher levels in in two technical domains "**Smart Cards and similar devices** " and "**Hardware devices with security boxes**".

Why to certify under Common Criteria?

Common Criteria certificates have a **world-wide and cross-industry recognition**. A Common Criteria certified product has a key differentiation element in terms of security as it has been assessed by a third party under a strong and well defined evaluation methodology.
In many cases, Common Criteria is **a final user demand**. Governmental regulations in USA (NSTISSP No. 11 - NIAP PCL List) or Europe (Spanish ENS, European eIDAS or Tachograph regulations) require that public agencies purchases include third party assurance certificates (being Common Criteria the most frequent one).
In some industries Common Criteria may be a **market entry requirement** (IC or ePassport) or a specific security assurance requirement in tenders (banks, MNO).

Contact: info@appluslaboratories.com

Applus+, accredited laboratory for Common Criteria evaluations

Applus+ is an **IT Security Evaluation Facility (ITSEF)** accredited for Common Criteria and SOG-IS evaluations. We manage the process to obtain the Common Criteria Certification (ISO 15408:2005) for IT products.
Our service includes **Common Criteria Evaluations** (up to level EAL 7). Depending on the evaluation level, Common Criteria requirements include:

- **Products evaluation**: focused on risk vulnerabilities mitigation
- **Developer design evaluation**: focused on ensuring development process reliability
- **Development Site Audits**: focused on ensuring supply chain integrity and confidentiality.

Common Criteria Applications

Smart Cards and Secure Elements

Smart Cards are widely used in many industry applications: e-Passports, ID cards, transport ticketing, e-health. Common Criteria methodology can be used to certify the three layers of a Smart Card: The Integrated Circuit (IC), the card operative system (Platform) and the application.
Although some industries like payment have their own certification schemes (EMVCo), non-final
products vendors (IC, platforms and Composites) may need to certify under both schemes as their products may have multi-industry applications. In such cases, Applus+ can provide combined security evaluation to speed up time-to-market.

Security Boxes

Security boxes are widely used in many industry applications (terminals, HSM, smart meters, vehicle units, motion sensors, GNSS, connectors, amongst others) and across various sectors (Payment, healthcare, smart grids, Tachograph, eIDAS).
Although some industries like payment have their own certification schemes (PCI), vendors may need to certify under both schemes, Common Criteria and the sector specific scheme.

Telecom equipment

Routers, switches, gateways, and similar products are security-critical and final clients usually require security assurance certificates like Common Criteria. In some cases like, Governmental agencies tenders, having a Common Criteria certificate may be an entry barrier requirement.

Mobile

As new high added value applications are moving to mobile (payment, DRM, identification, biometrics, etc) security concerns are arising. Common Criteria is a perfect solution for Mobile devices or Mobile Apps evaluations.

eIDAS and Trusted Services

The eIDAS Regulation provides the european regulatory environment for digital signature, HSMs or time stamping products. The European commission has designated Common Criteria as the methodology to assess the strength of this kind of products through the definition of a set of protection profiles.

Other IT products

Common Criteria is a suitable option to claim security assurance and a marketing distinction for many kind of IT products such as commercial software, Saas, Cloud Computing platforms or Hardware Secure Modules.

Note: Because Applus+ Laboratories is accredited as a third party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.