Common Criteria certified open source software – fact or fiction?

Tomas Gustavsson

PrimeKey Solutions AB
Andertorpsv 16
171 54 Solna, Sweden
tomas@primekey.se

Abstract: In 2012 the two open source projects CESeCore and EJBCA were Common Criteria certified [CCP], using open source tools and open source methodologies. As the actual software and its long term evolution is perhaps the most important result for most users, we will look at how certification, distribution and maintenance is managed. Can they be done in an open source way, and is certification always suitable?

The Common Criteria for Information Technology Security Evaluation (Common Criteria) is a standard for IT security certification defined by ISO/IEC 15408 [WP]. The Common Criteria provides trust that processes for specification, implementation and evaluation has been performed in a rigorous and standardized way. Recognized world wide and governed by national certification bodies, Common Criteria is used as requirement for procurement and use of security software in governments, banks and enterprises.

Common Criteria has been criticized for large costs and potential discrimination against Open Source Software [DW]. Given the rigorous system that Common Criteria enforces, how can open source software be certified, and maintained as certified? Drawbacks and benefits of a Common Criteria certification will be described, and how certification limits the maintenance of an open source project.

Common Criteria certified open source software – fact or fiction? After this presentation software developers will be able to determine if their open source project is suitable for Common Criteria certification, whilst software users will have a good idea if they should require certification.

References

[WP] WikiPedia, Common Criteria, http://en.wikipedia.org/wiki/Common_Criteria
[CCP] Common Criteria Portal, http://www.commoncriteriaportal.org/
[DW] David A. Wheeler: Free-Libre/Open Source Software (FLOSS) and Software Assurance / Software Security, , December 11, 2006, http://www.dwheeler.com/essays/oss_software_assurance.pdf
[EJBCA] EJBCA.org website, http://www.ejbca.org/
[CESE] CESeCore website, http://www.cesecore.eu/