Common Criteria Recognition Arrangement

Common Criteria Development Board

Operating Procedures

Document Number: 2011-04-001

Version: 1.0

Date: April, 2011

Subject: Vision statement for Collaborative PP and supporting document development

Background

There is an increased interest from several participants of the CCRA to facilitate development of protection profiles[1] through collaboration between government agencies from several nations, product vendors and labs. Such protection profiles may then be used for procurement in several nations.

In order to ensure that the interests of the CCRA participants are considered, as well as ensuring that vendors, labs and other stakeholders are given access and an ability to influence the work and ensure that development becomes a tool for fair competition, the CCDB has agreed that it is necessary to create a framework to allow for proper management of such protection profiles.

The initial characteristics of such a framework were discussed and agreed by the members of the CCDB in their meeting in Stockholm in April 5-6 2011.

This paper presents the CCDB understanding of the characteristics of mutual recognition in the context of CCRA, introduces the notion of “Collaborative Protection Profiles” and describes the fundamental framework for how the CCDB have agreed to manage Collaborative Protection Profiles.

The paper represents the current vision of the CCDB and is expected to be refined and expanded in future revisions. Comments and/or suggestions on this paper can be forwarded to the CCDB via the national schemes.

1 NOTE – in this document the term 'protection profile' includes, where relevant, any associated supporting documents

CCRA interpretation

'Certificate recognition' versus 'Product acceptance'
Recognition in the CCRA is related to certificates and only implies that nations recognise the work done by other compliant schemes to be in accordance with the CC and CEM. This may not be sufficient for acceptance of certified products for use in a particular context. Other requirements or regulations may also be applicable. The current CCRA mandates the recognition of certificates with assurance components up to and including EAL4 (and FLR). It allows however that nations have national policies that prohibit their scheme to certify products above or below a certain level.

'PP recognition' versus 'PP recommended for use'
As implied above a PP can only be recognised as being compliant with the CC and CEM. This does not necessarily mean that a certified PP describes the needs a certain user may have and is a suitable basis for their procurement of compliant products.

The CCDB concluded that the CCRA does not need to change to accommodate the PP development effort.

Goal

Create Collaborative PPs (CPPs), ideally one CPP per technology area, and supplemented by supporting documents that shall be considered by several nations as a de-facto standard and could be recommended for use in government procurement. This effort shall lead to an increased availability and choice of compliant and comparable products, whereby:

- the appropriate security functionality of these products is improved
- the minimum level of acceptable security assurance is defined
- competition is increased in order to lower procurement costs

Means

- Collaborating with other national governments or assigned representatives (members of the CCRA) in order to:
  - maximise acceptance for each CPP;
  - limit the number of available CPPs (ideally 1) for each technology area;
  - share the costs of development.
- Collaborating with product vendors in scope of a CPP in order to:
  - include state-of-the-art technology;
  - promote fair competition;
  - maximise acceptance and number of compliant products.
- Collaborating with IT security evaluation facilities licensed under the CCRA in order to:
  - provide consistency between labs;
  - agree on effective assurance activities.

Governance structure

- The CCDB asks the CCRA Management Committee for approval for each technology area.
- CCDB accepts a proposed PP (including supporting documents) as a CPP through an agreed voting process.
  - Only PPs that meet the baseline requirements (see below) may be subject for acceptance;
  - Only PPs that have a sufficient supporting community behind them may be subject for acceptance.
- CPPs and a reference to CCRA participant websites that wish to outline additional guidelines, recommendations and/or procurement policies, including reference to potential national refinements will be posted on the CC portal.
- Communities appointed or accepted by the CCDB are responsible for the initial creation and later maintenance of CPPs and supporting documents.
  - Terms-of-Reference (describing rules for membership, voting procedures etc) and regular liaison statements are needed;
  - Work in progress/intermediate outputs shall be open for all interested parties and will be referenced on the CC portal.

Baseline requirements

- All CPPs shall be compliant with the generic framework of the CC and CEM in order to support mutual recognition. Supporting documents supplementing the CPPs may be created to give interpretations to the CEM where needed. When a rationale demonstrates that the CPP and/or supporting documents cannot express the security needs, the CC and/or CEM may be modified, subject to the normal approval process.
- All CPPs shall only contain requirements that could be applied by all CCRA schemes, in particular no dependency on national conformity assessment schemes shall exist.
- All CPPs may explicitly specify reference standards for cryptographic primitives/protocols defined by appropriate standards bodies. CPPs should also allow use of other 'national approved primitives/protocols' so that nations can provide their own refinements. Harmonising crypto evaluation methodology for mutual recognition is a topic that is being discussed by CCDB separately.
- All CPPs shall include all assurance components of EAL 1 and may select higher components per assurance family. The use of extended assurance components should be avoided unless a rationale can be provided and is subject to the normal approval process.
- CPPs define the minimum level of acceptable security assurance. They shall allow higher level assurance evaluations against a CPP while keeping the ability to claim conformance to the CPP.
- All CPPs shall define the minimum set of common security requirements. Although the CC and CEM framework allows adding security requirements in a ST besides those specified in the CPP while keeping the ability to claim conformance to the CPP, it is highly recommended that additional functionality is defined in the CPP as optional packages.

PP development

- The CEM work units related to the assurance requirements specified in the CPP still apply, but may be refined where needed in a supporting document.
- Refinements can be made to assurance requirements by specifying assurance activities that need to be performed in addition to those derived from the regular CEM work units.