Common Criteria

Common Criteria Recognition Arrangement

Common Criteria Management Committee

Vision Statement

Document Number: 2012-09-001

Version: 2.0
Date: September, 2012

Subject: Vision statement for the future direction of the application of the CC and the CCRA

Background

To a large extent the CCRA activity has in the past been focused on developing the CC/CEM and harmonization of the application of the CC/CEM among the schemes. Nowadays there is an increased interest among the participants of the CCRA to facilitate development of protection profiles[1] through collaboration between government agencies of CCRA participants, product vendors and labs. These protection profiles are then intended to be used for procurement purposes in several nations.

However, moving to a more PP-centric way of using the CC and CCRA also requires harmonization of how the CCRA participants develop and apply protection profiles. This paper highlights the key points for adapting the CCRA and continues by describing the fundamental framework for how the Management Committee (MC) have agreed to allow for proper management of such protection profiles.

This framework will 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. It also ensures that the resulting protection profiles become tools for fair competition.

The paper represents the vision of the MC focusing on the needed framework for managing the creation of protection profiles and does not address the changes required for the CCRA itself. The MC vision 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

Key points for future CCRA use

1. The general security level of general ICT COTS certified products needs to be raised without severely impacting price and timely availability of these products.
2. To support that goal, the level of standardization has to be increased by building Technical Communities (TC) developing collaborative Protection Profiles ("cPPs") and supporting documents, in order to reach reasonable, comparable, reproducible and cost-effective evaluation results.
3. Mutual recognition should be based on the achievable common level of the cPPs.
4. TCs should be defined and cPPs should be developed for all product classes where multiple manufacturers provide individual STs for similar products.
5. Whenever applicable, cPPs should be applied instead of individual STs. The application of STs should be reserved for cases where cPPs do not exist or are not applicable and CCRA mutual recognition should be limited to EAL 2.
6. The CC will be maintained as the toolbox used by the TCs to develop the cPPs.
7. Evaluation levels beyond the cPPs should be reserved for situations such as:
   - national requirements
   - agreements between individual stakeholders such as:
     i. bilateral arrangements between countries
     ii. SOGIS-MRA, and similar other communities.

   No CCRA mutual recognition above the cPP level.
8. Protection Profiles ("cPPs") and/or supporting documents will address vulnerability analysis requirements to ensure certified products achieve an expected level of security.

Note that 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. It is intended that products that comply to a cPP can be used in most situations, but certification may not always be sufficient for acceptance of certified products for use in a particular context. Other requirements or regulations may also be applicable.

Another item to note is that cPPs form a new, but additional application of the CC and CCRA. The existing application of STs and PPs still applies, but its CCRA mutual recognition should be limited to EAL 2.

Framework objective

To facilitate the above mentioned key points for the future direction of the CC and CCRA the following goal has been defined:

Have collaborative Protection Profiles ("cPPs") created as deemed necessary by Technical Communities (TC), ideally one TC 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 achievable common level of security assurance is defined
- competition is increased in order to lower procurement costs

Means

Technical Communities consisting of several stakeholders allow for:

- Collaborating with national governments or assigned representatives (members of the CCRA) in order to:
    - maximise acceptance for each cPP;
    - limit the number of available cPPs for each technology area;
    - share the costs of cPP 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 will ask the CCRA Management Committee for approval for each technology area.
- The 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.
- Technical 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 are expected to be created to give interpretations to the CEM as 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 assurance components derived from the CC part 3 to a maximum of EAL2, or higher (up to EAL4) if the TC can demonstrate a rationale that shows the activities can be repeated between schemes. The use of extended assurance components should be avoided unless a rationale can be provided and is subject to the normal approval process.
- cPPs shall define the achievable common level of security assurance and will address vulnerability analysis requirements to ensure certified products achieve an expected level of security. Assurance activities not defined in the cPP will not be recognised under the CCRA and certificates claiming conformance to the cPP shall not include higher level and/or additional assurance requirements.
- All cPPs shall define the minimum set of common security functional requirements. CCRA certificates claiming conformance to the cPP shall not include additional security functionality besides those specified in the cPP. It is highly recommended that additional security functionality is defined in a ST and evaluated separately where the mutual recognition of the resulting certificate will be limited to assurance components up to and including EAL2 (and FLR).
- For those cases where cPPs do not exist or are not applicable evaluations will be performed against a product ST where the mutual recognition of the resulting certificate will be limited to assurance components up to and including EAL2 (and FLR). This also applies for standard PPs and products claiming conformance to those PPs.

PP development

- The CEM work units related to the assurance requirements specified in the cPP still apply, but are expected to be refined as needed in a supporting document.

Footnote

The above statement is the shared vision of the CCMC from the meeting held September 17, 2012. All nations agreed on the concept of cPPs and agreed that the addition of a cPP-based approach will assist in achieving repeatable, comparable, effective evaluation results.

Two nations voiced disagreement with the sections of the vision statement which limit non-cPP mutual recognition to EAL2. Additional workshops are planned to facilitate full CCMC consensus on the above vision statement.