



Request to establish an International Technical Community (iTC) for the creation of Common Criteria Collaborative Protection Profiles and Supporting Documents relating to the security evaluation and certification of USB Portable Storage Devices

Background

The Common Criteria (CC) is an internationally recognised standard that forms the basis for the independent evaluation and certification of the security of a wide range of IT products. The Common Criteria Recognition Arrangement (CCRA) is an arrangement signed by 26 nations that establishes a basis for common evaluation and certification practice, and enables international recognition of product certificates in all of those nations. This means that products certified under CCRA by one of the certificate authorising nations will have their certification recognised by all 25 of the others. Further details of CC can be found at the official website: www.commoncriteriaportal.org.

The CCRA infrastructure includes a Management Committee (CCMC) that is responsible for management of the whole arrangement, and a Development Board (CCDB) that is responsible for the management of the CC criteria and methodology. As part of the continuing development of CC usage the CCMC and CCDB are establishing international Technical Communities (iTCs) to create multi-national security requirements for individual technology types, with the aim of improving its value to end-users and risk owners of security products, and of including product developers in the requirements development process. These security requirements will be expressed in the form of Common Criteria collaborative Protection Profiles (cPPs), and the main aim of an iTC is therefore to create a cPP and associated Supporting Documents¹. As experience in using the cPP builds, the iTC will also provide a forum for sharing that experience and for updating the cPP to cover future developments in the technology type and in the attacks that are made on products.

Who we are

The CCDB has established a Work Group to assist in creating an iTC (and hence a cPP) for USB Portable Storage Devices (the Work Group name is abbreviated to “CCDB USB cPP WG”). The Work Group comprises participants from 12 nations, at present: Australia, Canada,

¹ More details of the process surrounding the creation of an iTC and cPP are given in the document ‘Establishing International Technical Communities and collaborative Protection Profiles development available at www.commoncriteriaportal.org [1]

Denmark, Finland, Germany, Japan, Netherlands, Singapore, Sweden, Turkey, the UK, and the US. Together, this group has produced a statement of ‘Essential Security Requirements’ (ESR) which represents the common needs of the WG members (as reflected in the associated ‘Position Statements’²). This letter is being sent by the CCDB as part of a call for participation in forming the official USB iTC, which will develop the cPP and respective Supporting Documents.

What is needed

iTCs are a method of consolidating skills, expertise, and security knowledge from all stakeholders in the evaluation and certification of a technology type. The involvement of product developers, and their collaboration in the work, is crucial to the success of the iTC, and relies upon the individual participants bringing technical knowledge of threats, product functionality, and potential vulnerabilities. It is therefore important that the product developers provide participants with strong technical knowledge for the creation of the cPP.

There are many skills and backgrounds needed for the creation of an effective cPP and its Supporting Documents. It is intended that the iTC will include at least:-

- Developers (technical representatives, as subject matter experts are vital - marketing and/or CC specialists can take part and may be helpful at the start up meeting but success depends upon the continual interactions between the technical experts of the developers involved as they work to produce and maintain the cPP)
- Government experts (especially those versed in the threats associated with the technology and governmental use cases)
- Evaluators - able to provide proposals and comments upon the technical and cost effectiveness of proposed assurance mechanisms

Wherever possible the end users, particularly the risk owners associated with the use of the technologies concerned, should also be included.

At this stage a group of interested participants have formed the Secure USB Alliance. This group is in the early stages of setting up the initial working structures and proposed methods for the iTC, and further members for the iTC are now being invited. The CCDB USB cPP WG will help in this invitation process, and this calling letter will be posted on the Common Criteria Portal and will be circulated to relevant local industry etc. by CCRA Participants, but the intention is that the iTC should be self-supporting in the longer term.

NOTE – Responding to this call for participation does not constitute a legal or financial commitment on either side.

The activities needed from the iTC at the beginning include:

² A ‘Position Statement’ is a public statement from a CCRA Participant (i.e. a representative of a national government) about support for the development and use of a cPP. Once the cPP and associated Supporting Documents are finalised and (in the case of Supporting Documents) approved then further ‘Endorsement Statements’ can be used to indicate steps to adopt the cPP in more detail. See [1] for more description of Position and Endorsement Statements.

- Establishing a suitable membership for the iTC
- Defining Terms of Reference for the group (using guidance from the CCDB USB cPP WG). The iTC should meet the six principles of international standardisation determined by the WTO-TBT³.
- Defining a workplan and schedule for the production and ongoing maintenance of the cPP and related documents
- Establishing working methods for the iTC members to communicate and share documents.

The Terms of Reference are a particularly important task, since these are the main requirement on which CCDB approval, and CCMC endorsement, of the iTC is based. Obtaining CCDB approval is on the critical path for the process of developing the cPP itself.

Supporting documents will also need to be approved via a CCRA approval process⁴ and, in the case of the USB Portable Storage Devices, these will certainly be required in order to define cryptographic assurance requirements. The CCDB USB cPP WG is in the process of producing such Supporting Documents and the iTC will be expected to use these.

What are the timelines?

This is the first such international Technical Community to be created and much of the timing will be in the hands of the industry members and set by the iTC itself. However the preferred target is for the iTC to produce a first version of the cPP and Supporting Documents by the end of the second quarter of 2014. The iTC would then be expected to continue with further development and maintenance of the cPP and SD as needed.

The work will probably start with an initial teleconference in January 2014.

NOTE – Although work towards a cPP could be undertaken by the iTC members before the iTC is formally approved by the CCDB (based on approval of the iTC Terms of Reference), the iTC will need to proceed according to the defined steps of the iTC/cPP process (see [1]), meaning for example that the next step after iTC approval will be SPD creation and public review.

How to become a participant

The iTC formation is currently being co-ordinated by the Secure USB Alliance - Please see www.secureusballiance.org and make contact via info@secureusballiance.org

The working group can also be contacted if necessary via usbwg@ccdbinfo.org (NB this will go to the whole working group and will take time to result in a coordinated reply)

³ See G/TBT/1/Rev.9 (8 September 2008) “DECISIONS AND RECOMMENDATIONS ADOPTED BY THE WTO COMMITTEE ON TECHNICAL BARRIERS TO TRADE SINCE 1 JANUARY 1995”

⁴ Approval of the need for each Supporting Document, by means of an iTC rationale, by the CCMC, with subsequent monitoring against the needs of the CCRA (assurance and iTC requirements) by the CCDB.

Further Information

The Common Criteria portal website (www.commoncriteriaportal.org) provides the definitive source for further information. On this site will be found all of the documents referenced here together with contact details and membership lists for the iTC⁵.

More details of the process surrounding the creation of an iTC and cPP are given in the document ‘Establishing International Technical Communities and collaborative Protection Profiles development’ [1] and an outline of the scope for the cPP is given in ‘USB Portable Storage Device Essential Security Requirements’ [2].

References

- [1] “Establishing International Technical Communities and collaborative Protection Profiles development,” [Online]. Available: www.commoncriteriaportal.org/communities/technical_communities.cfm .
- [2] “USB Portable Storage Device Essential Security Requirements,” [Online]. Available: www.commoncriteriaportal.org/files/communities/ESR-USB.v2.0.pdf .

⁵ Or links to where such information can be found

Appendix 1 Key items for iTC Charter

The initial iTC membership should:-

- Establish an iTC in accordance with the MC Vision statement, the updated CCRA (when approved) and the whitepaper [1], that in turn will develop an USB cPP:
- Set up infrastructure. (May use Teamlab as a start).
- Establish Terms of reference
 - May use CCUF Guide as basis.
 - Must adhere to the six principles and MC Vision statement.
- Provide a point of contact that can be published at the CC-portal.
 - Email-adress, URL and if possible a phone number.
- Seek participation from relevant interested parties (labs, vendors, schemes, users).
 - Can use the document “Request to establish an International Technical Community (iTC) for the creation of Common Criteria Collaborative Protection Profiles and Supporting Documents relating to the security evaluation and certification of USB Portable Storage Devices” for this
 - .CCDB USB cPP WG is happy to assist and/or comment.
 - The call is to also be published on the CC-portal.
- Manage members so that all can participate in creating the ToR, cPPs, and Supporting Documents.
- Together with CCDB USB cPP WG organize a walkthrough of the whitepaper for the iTC membership.
- Collaborate regularly with the CCDB USB cPP WG.
- Within itself agree on final ToR and appoint representatives.
- Seek approval as iTC by the CCDB and endorsement by the CCRA MC.

After this the iTC is established and should act in accordance with the ToR to establish the cPP, based on the ESR and other inputs from its members.