CCDB USB cPP Working Group News Letter - November 29th, 2014.

This message provides an update from the CCDB USB cPP WG. The intent is to provide some insight into how the project has evolved since the meetings in Orlando. It is not intended to provide a comprehensive description of all activities or results. It is primarily intended for the participants of the CCRA, but may also be of interest for other interested parties.

Executive summary

- Canada has joined the CCDB USB cPP WG.
- The Essential Security Requirements for USB portable storage devices has been finalised at v2.0.
- A new approach to express endorsement of cPPs has been defined. This in order to make it easier for more CCRA Participants to express their position and/or support in relation to cPPs being developed.
- The outcome of the workshop in London 6-8 November:
    - Resolution to all comments received on the model for how to establish iTC and develop cPPs (the whitepaper).
    - Updated WG workplan
    - Discussion on guidance supporting documents for crypto
    - Discussion on cPP Maintenance
    - iTC, cPP and ESR life cycle discussions.
- Establishment of the USB iTC is in progress.
- Draft proposal to reintroduce “exact conformance” into the CC

Background

The CCDB USB cPP WG was established at the CCDB meeting in Tokyo March 2012. The task assigned to it (excerpts from the CCDB RoD):

- To form the government collaboration group about USB portable storage devices (shortly USB devices). Each government who participates in CCRA should be willing to make a peer statement regarding the intended usage of the potential cPP; how it would be used in the national procurement in each country.
- To identify security measures and problems that cPP should address; and then, if we could not agree on that, we could start negotiations and find solutions before the cPP would be written;
- CCDB to ask vendors to form an iTC with all the resources and ask them to write a ToR, that is to get an approval from CCDB;
- To publish the results on CC portal to show how to use USB-cPP for each government so that it would be visible to all members.

The WG has agreed to document the methodology it develops. The intent is to describe a general model for how to establish harmonized high level security requirements among the CCRA participants and how to establish international Technical Communities which in turn develops collaborative Protection Profiles. The document where this methodology is described is often referred to as “the whitepaper”.

Canada has joined the CCDB USB cPP WG

We are very pleased that Canada has decided to join the USB cPP WG. The WG now consist of representatives from 12 nations: Australia, Canada, Denmark, Finland, Germany, Japan, Netherlands, Sweden, Turkey, Singapore, UK, US.

The Essential Security Requirements for USB portable storage devices has been finalised

The ESR represents the use cases and high level security requirements for secure USB portable storage devices that could be agreed upon in consensus among the WG members. The WG has taken into consideration additional comments received from CCRA nations not participating in the WG. It should be noted that individual nations may also have other security needs, which have not been included in the ESR due to lack of general consensus. Such needs may be communicated by each respective nation to the iTC as well. The WG has defined a mechanism for providing 'Position Statements' that can include such comments to the iTC.

A draft version of the essential security requirements was agreed by the WG members in August. It was then circulated to the members of the CCDB and MC. Norway and Australia provided additional comments and the ESR was updated to address the comments received where a consensus could be reached. As the USB cPP project is to a large extent focused on being a test bed for how to establish the general cPP process, it was decided to limit the ESR to the most common requirements and application features. Additional features that have been asked for by some nations may be included in a later version. The WG has now (in accordance with the process agreed within the WG) finalized the ESR at v2.0. It is provided for your information. It will be the basis for the cPP to be created by the iTC.

A new approach to express endorsement of cPPs has been proposed.

The previously proposed model (i e the whitepaper v0.4) for how to establish cPPs included the notion of "Commitment levels", where nations were invited to announce themselves as being "Committed Nations", "Uncommitted Nations" or "Opposed Nations" in relation to a cPP to be established. During the meetings in Orlando, the term "Commitment level" was agreed to be changed to be "Endorsement Level".

The purpose of this model was to provide an instrument through which the iTC could be informed about the interest in the cPP of each respective nation. This would provide an important incentive for why stakeholders should take the costs of developing the cPP within the iTC.

Further discussions in the WG have shown several issues with this model and it posed a fundamental hurdle for several nations in the WG to express a statement about their level of endorsement of the cPP. The WG has after several discussions agreed to propose the following model going forward.

First and foremost, the notion of "Commitment Levels" (or "Endorsement Levels") is removed.

Instead each nation having an interest in the cPP and its development is invited to issue a public *Position Statement (PS)* at any time it deems appropriate. The Position Statement can be either positive (i. e., the issuer of the PS expresses that the iTCs work is progressing satisfactorily and is in line with requirements) or negative (i. e., the issuer of the PS has concerns that may be a concern for the issuer to later endorse the resulting cPP).

Once the cPP and related Supporting Documents have been finalized, nations (and other stakeholders) may issue an *Endorsement Statement,* through which the issuer makes a positive statement about how products certified against the cPP is related to procurement rules and/or regulations.

The WG are in agreement that this new model avoids several of the issues we discovered with the former model, while at the same time still provides an instrument through which the iTC could be informed about the interest in the cPP of each respective nation.

The outcome of the workshop in London

During 6 – 8th of November there was a workshop organized in London. The main purpose was to walk through outstanding issues regarding the whitepaper and proposed resolutions. We are very pleased that the WG did agree on the principles for how to resolve all issues. An updated version of the whitepaper is now being created. After review and agreement within the WG, the updated whitepaper will be distributed to the CCRA participants for further discussions.

We updated the WG workplan, which contains a list of deliverables to be produced by the WG together with identification of the responsible editor and other notes and comments.

At the CCDB meeting in Orlando it was agreed that the WG should create proposed guidance supporting documents for crypto. These were discussed at the workshop. See the status of respective document below:

- "Cryptographic Definitions" Supporting Document: The WG believes we have a fairly complete list of crypto terms and we are mostly in agreement on the definitions. Still some future discussions remain.
- "Specification of Cryptography in cPPs" Supporting Document: This work will focus on how to specify crypto algorithms and (for other cPPs) protocols that could be agreed by several nations, as well for how to manage needs that are particular for some nation(s).
- "Extended Security Functional Requirements for Cryptography in cPPs" Supporting Document: Currently contains a proposed SFR for random number generators. One other proposed extended SFR for an RNG has been submitted for consideration. Further work is required to harmonize a standard expression, but intentions are to allow for national standards for RNGs as well.

At the workshop we also had an initial discussion of the maintenance process for cPPs, and explored the cPP and ESR life cycle, and the conditions for how the iTC could be approved by the CCRA. This area will need more work before we have any more mature conclusions and are able to provide proposals to the CCRA.

Establishment of the USB iTC is in progress.

The WG has updated the invitation letter for establishing the interim iTC. As agreed in Orlando, this will be provided to the CCDB for comments before it is sent out to the stakeholders who volunteered to assist in setting up the iTC.

We are working on details for how to provide support and assistance to the iTC while it is being established, as well as some guidance for the content of their Terms of Reference. This will partly be based on the Guidance for Terms of Reference developed by the CCUF, combined with some examples of ToRs from existing Technical Communities.

Draft proposal to reintroduce "exact conformance" into the CC

The WG has noted that the updated CCRA introduces the new cPPs as a mechanism that may be used by procurement bodies to specify their security needs. The specific cPP related requirements in the CCRA annex K.3 state that CCRA certificates can only claim conformance to a cPP if it only covers the defined SFRs and SARs in the said cPP. This introduces a new type of conformance claim that the current CC and CEM does not provide.

To address this need, the WG is intending to provide a proposal for "exact conformance", that is based on some work that was produced by the CCIMB several years ago, to be incorporated in a new revision of the CC and CEM.

Summary

As can be seen from above, the WG continues to develop a model, develop documents and perform all activities that are necessary to establish iTCs and cPPs in accordance with the MC Vision statement.

The WG conducts virtual meetings with screen sharing and joint editing sessions almost on a weekly basis and all twelve nations are regularly participating in the discussions. It is actually quite amazing how well this works.

Even though the discussions are complex and take some time, we are making good progress. It is very encouraging to see how the twelve nations currently engaged in the WG collaborate in a very constructive manner to find a way through which the USB cPP could be developed that could be used by several nations.

Best regards,

Dag Ströman,
On behalf of the CCDB USB WG

Disclaimer
The information in this newsletter is provided "as-is" and the WG may or may not answer questions in relation to the newsletter.

When next version of the Whitepaper has been finalized, it will be made available to CCRA and relevant stakeholders and the WG will ask for comments and questions on that.

No member of the WG or any other party is to be held liable for the information provided in this newsletter.
///