The USB cPP WG –
The collaborative Protection Profile frontrunner.

International Common Criteria Conference 2013

Dag Ströman, FMV/CSEC, Sweden

Warning!

- This will be a text intensive presentation. Sorry.

Background –
From Swedish a perspective 1(2)

- Swedish Civil Contingency Agency (MSB) responsibilities includes coordination and regulation of cyber security and infosec for Swedish government agencies.
- In collaboration with the Swedish CC-scheme (FMV/CSEC), MSB attempted to establish guidance and policies for how to use CC in procurement for Swedish government.
- We found issues with making it EAL-based.
  - EAL:s are not the only thing that is relevant…
- 2009 it was decided to try a PP-oriented approach instead.
  - About the same time as the shift in policy in UK/US.

Background –
From Swedish a perspective 2(2)

- MSB & FMV established a technical committee with about 5 experts from other agencies, and an advisory board representing users from about 15 other agencies.
- It was agreed that USB would be a suitable first project.
  - Everyone use USB memory sticks
  - The security problem is fairly small.
- Sweden used this structure to establish the first national PP
- Lessons:
  - PPs works.
  - The structure we established works.
  - It will take looong time to establish a decent sized PP-library.
  - We need more influence from the vendors.
  - The Swedish USB PP compete with other nations USB PPs
  - We should strive for collaboration with others.
- **(Lessons to others: Establish a national structure for collecting the requirements from users, riskowners and procurers)**

Establishing the CCDB USB WG

- In conjunction with discussions about the reform of the CCRA at the CCDB meeting in Tokyo March 2012, a an ad-hoc survey among the CCDB members was made about which tech areas would be good subject for piloting of cPP:s.
- The USB was selected because:
    - Several nations has already established USB PPs (SE, UK, GE, US, SK etc).
    - The limited scope of the security problem allows the WG to focus on the collaboration model and thereby develop a working model in shorter time.
- Sweden, with support of US and UK was assigned to lead the project.

The early days
March – September 2012

- A workplan was produced.
- The WG received copies of the existing USB PP:s.
- An analysis was done to compare the all these requirements.
- Based on these requirements, an initial Security Problem Definition (SPD) was compiled.
- Intent was to create an SPD that could be subject for negotiation among the nations who would like to participate.
- After CCRA meetings in Paris, it became clear that this approach would not work…

Some lessons from the early days

- We realized that the process of establising the PP (including the SPD) need to involve all stakeholders right from the start!
  - Otherwise a looot of detailed discussions of why things are as they are have to be repeated.
- That we needed another, shorter, high level language as basis for the negotiation between nations.
  - Otherwise nations will get boggled down in detail discussion that should rather should be held in the iTC, when all stakeholders are there and can make their argument.
- That we would need to avoid an ”approval” relation between the CCDB and the iTC.
  - Otherwise the CCDB may become a bottleneck.
- To clarify responsibilities, it is important that the iTC owns the result and make all decisions on the content of the cPP.

The invention of the ESR and the Endorsement Statements

- In a workshop in the US in october 2012, we discussed how to solve this.
- The Essential Security Requirements and the Endorsement Statements was proposed.
- It was then agreed that a we should establish a document (”the Whitepaper”) that describes a complete project, that would be used for the USB-project, and could serve as basis for a more general paper.
- The first version of the Whitepaper was sent out to the CCDB in december.
- A revised version (”Whitepaper 0.4) was released in February.

Main principles

- The procurers/riskowners negotiate the wording of their need at high-level in plain english in the ESR.
  - If consensus can not be reached, the nature of ”disagreements” will be forwarded to the iTC too.
- Nations may chose to issue ”Endorsement statements” that explain in free format how certification of a product against a cPP that meets the ESR relate to national policies and/or procurement.
- The iTC develops a cPP that it believes meets the ESR.
  - The iTC may deviate from the ESR if it wish.
- As long as nations are happy with the progress, they uphold their respective endorsement statements.

An more market oriented approach instead of a regulatory one.

- The iTC is via the ESR given information about what the nations collectively ask for, and is via the Endorsement Statement given an indication of the nature of the market of each nation.
- The iTC may then decide how this will affect the creation of the cPP.
- The vendor can use this to decide level of engagement in the iTC and decision to become certified.
- The more powerful Endorsement Statement, the more weight that nation is expected to receive in the discussions in the iTC.
- Good technical arguments should always be considered.
- If the cPP deviates too much from the ESR, or if details in the implementation fail, nations may adjust their endorsement statements or revoke it completely.

Status - Members

- SCCS – Singapore
- FMV/CSEC – Sweden
- CESG – UK
- JISEC – Japan
- BSI – Germany
- FICORA – Finland
- Centre for Cyber Security – Denmark
- TSE –Turkey
- IPA – Japan
- NLNCSA – Netherlands
- MSB – Sweden
- NIAP – USA
- Australian Certification Authority

Overview of activities since Ottawa.

- Established WG infrastructure:
  - CCUF Teamlab area for files and virtual discussions.
  - Citrix GoToMeeting (GTM) for virtual meetings.
- Weekly GTM-meetings at a time that with some efforts allows all members to join
  - 1100-1300 Europe; afternoon in Asia/Pacific, 5 am US east coast.
  - Prepared agendas; consensus decisions; meeting minutes and action-item lists.
- WG agreed on decision making principles and change management procedures for WG docs.
- Workshop in Bonn August 21-23, hosted by GE.

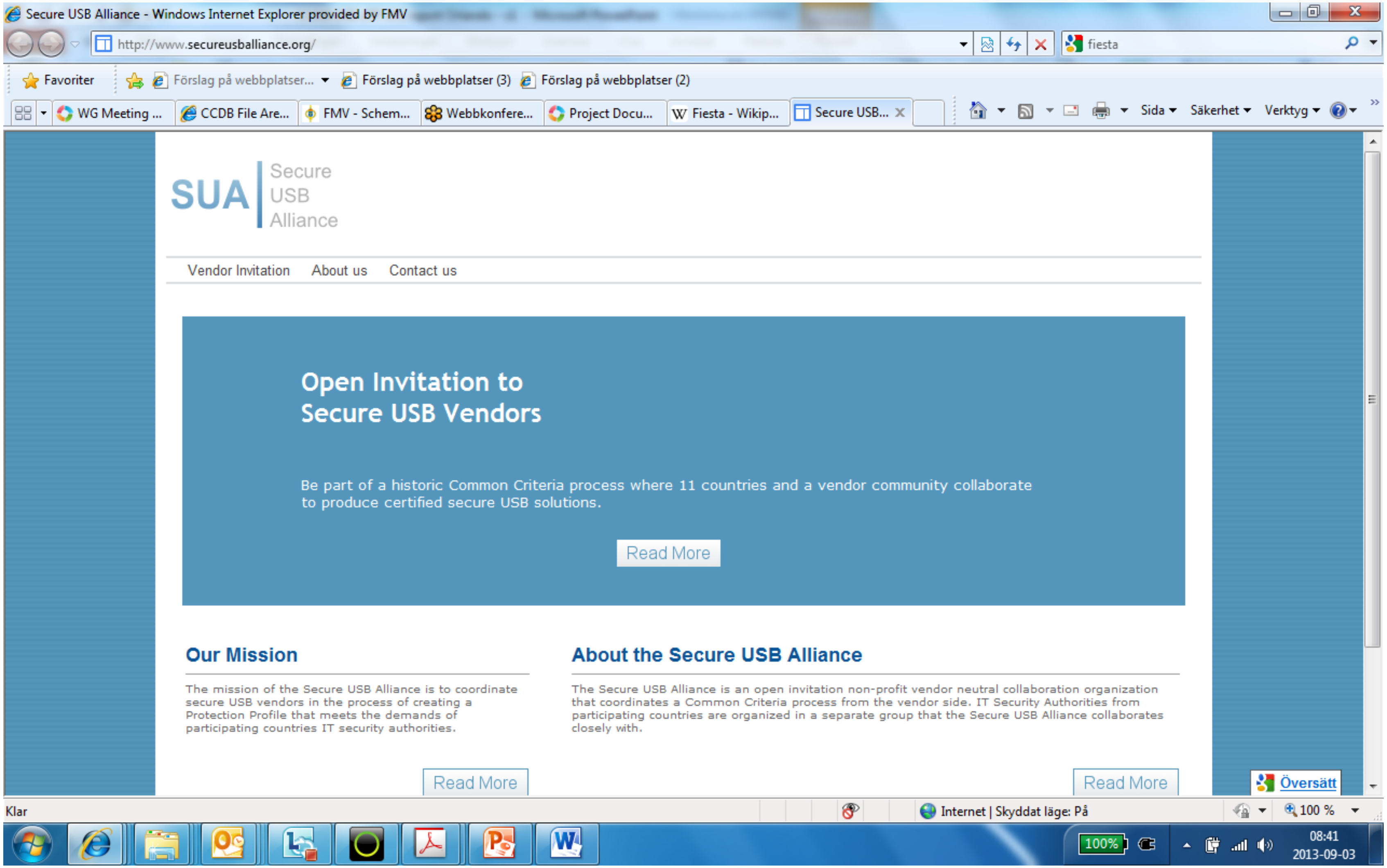
Achievements since last meeting

- Work group structure:
  - Established draft USB WG ToR and a draft Generic cPP WG ToR.
  - Established list of project members
  - Established draft work plan.
- Supporting Documents:
  - Established draft tech domain description: "Supporting Documents for Cryptography in collaborative Protection Profiles"
  - Established draft tech domain description: "Supporting Documents for USB Portable Storage Devices"
- Update of the Whitepaper:
  - Established Disposition of Comments in comments received on the iTC/cPP v0.4 process (The Whitepaper)
  - Comments received from: GE/BSI, FR/ANSSI, SE/FMV, SG, ISCIWG1, CCUF
  - We deal with all comments received and provide written response to each.
  - WG responses will be forwarded to originator of comments.
  - Several comments will need further discussion in the WG before being resolved.

Achievements since last meeting

- Essential Security Requirements (ESR):
  - Distributed ESR 1.0 to the DB and MC.
  - Established Disposition of Comments based on response on ESR 1.0 from Norway and Australia
  - ESR 1.2 now being vetted for final approval in the WG.
- Establishing an international Technical Community (iTC):
  - Established contact with interim group of vendors
  - Vendors intend to form "Secure USB Alliance".
  - http://www.secureusballiance.org/
  - info@secureusballiance.org
  - WG established draft public calling notice were the "Secure USB Alliance" is requested to form the iTC
  - All contacts to vendors we have received from schemes will be forwarded to the Secure USB alliance.
- National Commitment Statements:
  - SE, UK, US and GE agreed to start drafting their respective commitment statement.
  - (BTW: We will change the term "commitment statement")

The Secure USB Alliance


Secure USB Alliance - Windows Internet Explorer provided by FMV
http://www.secureusballiance.org/
fiesta
Favoriter
Förslag på webbplatser...
Förslag på webbplatser (3)
Förslag på webbplatser (2)
WG Meeting ...
CCDB File Are...
FMV - Schem...
Webbkonfere...
Project Docu...
Fiesta - Wikip...
Secure USB...
Sida
Säkerhet
Verktyg
Översätt
Klar
Internet | Skyddat läge: På
100 %
100%
08:41
2013-09-03

SUA Secure USB Alliance

Vendor Invitation About us Contact us

Open Invitation to Secure USB Vendors

Be part of a historic Common Criteria process where 11 countries and a vendor community collaborate to produce certified secure USB solutions.

Our Mission

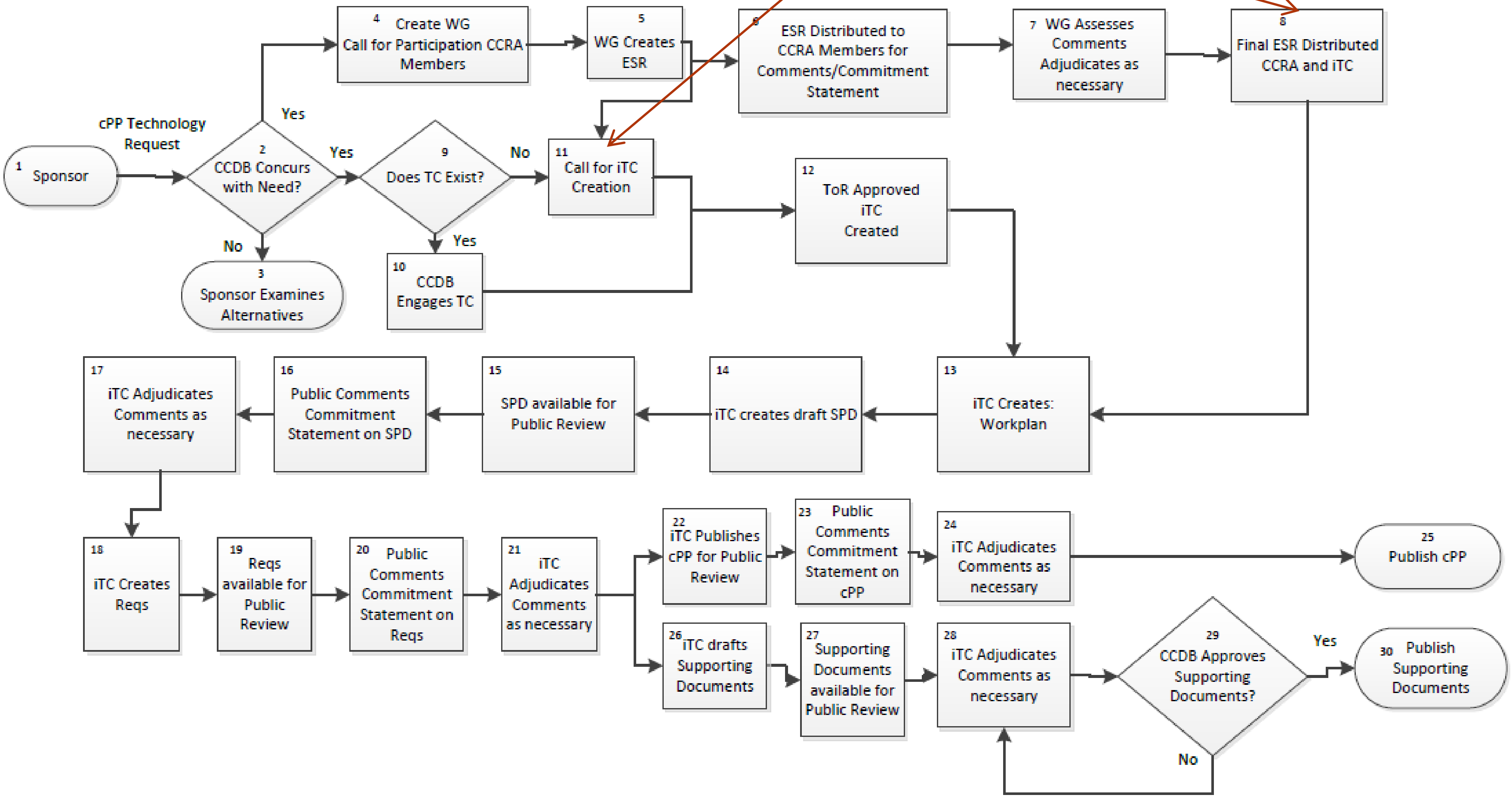
The mission of the Secure USB Alliance is to coordinate secure USB vendors in the process of creating a Protection Profile that meets the demands of participating countries IT security authorities.

About the Secure USB Alliance

The Secure USB Alliance is an open invitation non-profit vendor neutral collaboration organization that coordinates a Common Criteria process from the vendor side. IT Security Authorities from participating countries are organized in a separate group that the Secure USB Alliance collaborates closely with.

Next steps 1(2)

We have moved to here!



cPP Technology Request

1 Sponsor

2 CCDB Concurs with Need?

Yes

No

3 Sponsor Examines Alternatives

4 Create WG Call for Participation CCRA Members

5 WG Creates ESR

6 ESR Distributed to CCRA Members for Comments/Commitment Statement

7 WG Assesses Comments Adjudicates as necessary

8 Final ESR Distributed CCRA and iTC

Yes

9 Does TC Exist?

No

Yes

10 CCDB Engages TC

11 Call for iTC Creation

12 ToR Approved iTC Created

13 iTC Creates: Workplan

14 iTC creates draft SPD

15 SPD available for Public Review

16 Public Comments Commitment Statement on SPD

17 iTC Adjudicates Comments as necessary

18 iTC Creates Reqs

19 Reqs available for Public Review

20 Public Comments Commitment Statement on Reqs

21 iTC Adjudicates Comments as necessary

22 iTC Publishes cPP for Public Review

23 Public Comments Commitment Statement on cPP

24 iTC Adjudicates Comments as necessary

25 Publish cPP

26 iTC drafts Supporting Documents

27 Supporting Documents available for Public Review

28 iTC Adjudicates Comments as necessary

29 CCDB Approves Supporting Documents?

Yes

No

30 Publish Supporting Documents

Next steps 2(2)

- Update the CC-portal with proper information.
- Continue to work with the vendors to establish the iTC - ”Secure USB Alliance”
- Agree on matters of principle discovered in the Whitepaper.
- Update the Whitepaper in accordance with the DoC:s, and then have a USBWG/CCDB editing fiesta November 6-8 in UK.
- One worksessions for the WG is being planned for during ICCC.

Example on matters of principles being discussed in the WG.

- Committment statement -> Endorsement statement
- Principles of information sharing withing the WG, with the CCRA and other parties.
- Should the cPP need to be certified? Who would fund that?
- The fundamental requirements on the iTC:
  - Adhere to MC Visions statement
  - Adhere to the iTC/cPP process
  - Adhere to the six principles for international standardisation.
- How to avoid that the late approval of Supporting Documents in the process become a cause for surprises for the iTC?

Summary

- So far, by and large, the iTC/cPP process seem to be working.
  - Much of the work has been related to setting up the structure, WG ToR etc.
  - The WG has established a practical way for how to develop the docs so that everyones comments are accomodated.
  - Doing the work via virtual meetings looks promising.
- We have had to spend supprisingly little time with establishing the ESR.
- The vendors ask for two things:
  - Some formal request to establish the iTC.
  - Something like the Committment statement, since it provides a rationale to their senior management of why they should invest in the establishing the iTC/cPP
- Still several matters of princple to sort out.

Questions?