

CCDB Work items and development approach

David Martin
CCDB Chair

Background

- n CCDB has been listening to comments from Users, Vendors, and Schemes.
- n We want to take the opportunity, as we move towards version 4 to take account of:-
 - n Those comments
 - n New approaches that have been trialled, and
 - n General assurance developments such as increased availability of software tools for vendors



However some warnings to delegates are needed



Please note:-

- This talk covers work that is only just underway
- Some of the development work may not lead to the benefits that we expect or may prove impractical to implement
- The work that you will hear about here and in the individual work group presentations is very much 'work in progress'.
- We are briefing early because we want to encourage dialogue and input

Note Also -

- | This is aimed at general software products
- | Particularly the larger, complex, products
- | Smartcards and similar devices continue to be handled well by existing CC (with the JIWG, JHAS, ISCI support)

What does Industry need?

(As discussed at last ICC)

- | An assurance process that takes account of all of their assurance efforts
- | An efficient process (both fast and cost effective)
- | A process that helps them further improve
- | Results that are valued by end customers
- | Results that are as widely usable/recognisable as possible.

User Goals - 1

(as discussed at last ICCCC):-

Assess assurance in operation

”Confidence that an IT product will operate as intended, throughout its reasonably anticipated life cycle, even in the presence of adversarial activity”

User Goals - 2

Provide meaningful assurance information to the people building/running the systems, and to those ultimately responsible for the security of the data ”

User Goals - 3

- ▮ Evaluate *real products* as they are delivered and used in the marketplace
- ▮ Evaluate in a predictable and cost-effective manner
- ▮ Enable qualitative product assurance comparisons.

Key Idea/aim

Use direct interaction between assessment team and developers

Positives

- ┆ No need of special evaluation material (avoid waterfall pretence)
- ┆ Take account of assurance innovation
- ┆ Evaluator job satisfaction high

Difficulties

- ┆ Could become too subjective
- ┆ Too much impact on developer time?
- ┆ Evaluator skills

Key Idea/aim

Examine what is there – including code but NOT requiring any particular evaluation documents

┆ Positives

- ┆ Takes account of what developers are doing (and gives credit where this is due)
- ┆ Looks at real code

┆ Difficulties

- ┆ Have to understand all the relevant development processes tools etc - Evaluator skills
- ┆ Challenge where needed

Key Idea/aim

Examine in detail (and in action) the vendor's development and update process. Then use this to predict ongoing assurance

| Positives

- | Ongoing assurance is what customers really want/need

| Difficulties

- | How to closely examine developer process
- | Hard to bound the predictions
- | Evaluator skills

Key Idea/aim

**Support all of this with tools for the evaluator
Allowing them to collect evidence, build
evidence chains, and produce the required
reports**

| Positives

- | Makes process more efficient and effective

| Difficulties

- | A lot of work needed to get this truly usable and flexible

Key Idea/aim

**Give the user a much more detailed report
not just a pass/fail**

Positives

- What customers really want/need when building and running systems

Difficulties

- How to keep sufficiently objective (but is repeatability needed or is it really just 'justifiability' that we need?)
- How to make it truly usable for end-users
- How to target different users

Working Groups

- | At the CCDB meeting in April 08 five working groups were created:-
 - | Evidence based approaches
 - | Skills and Interaction
 - | Predictive Assurance
 - | Meaningful Reports
 - | Tools

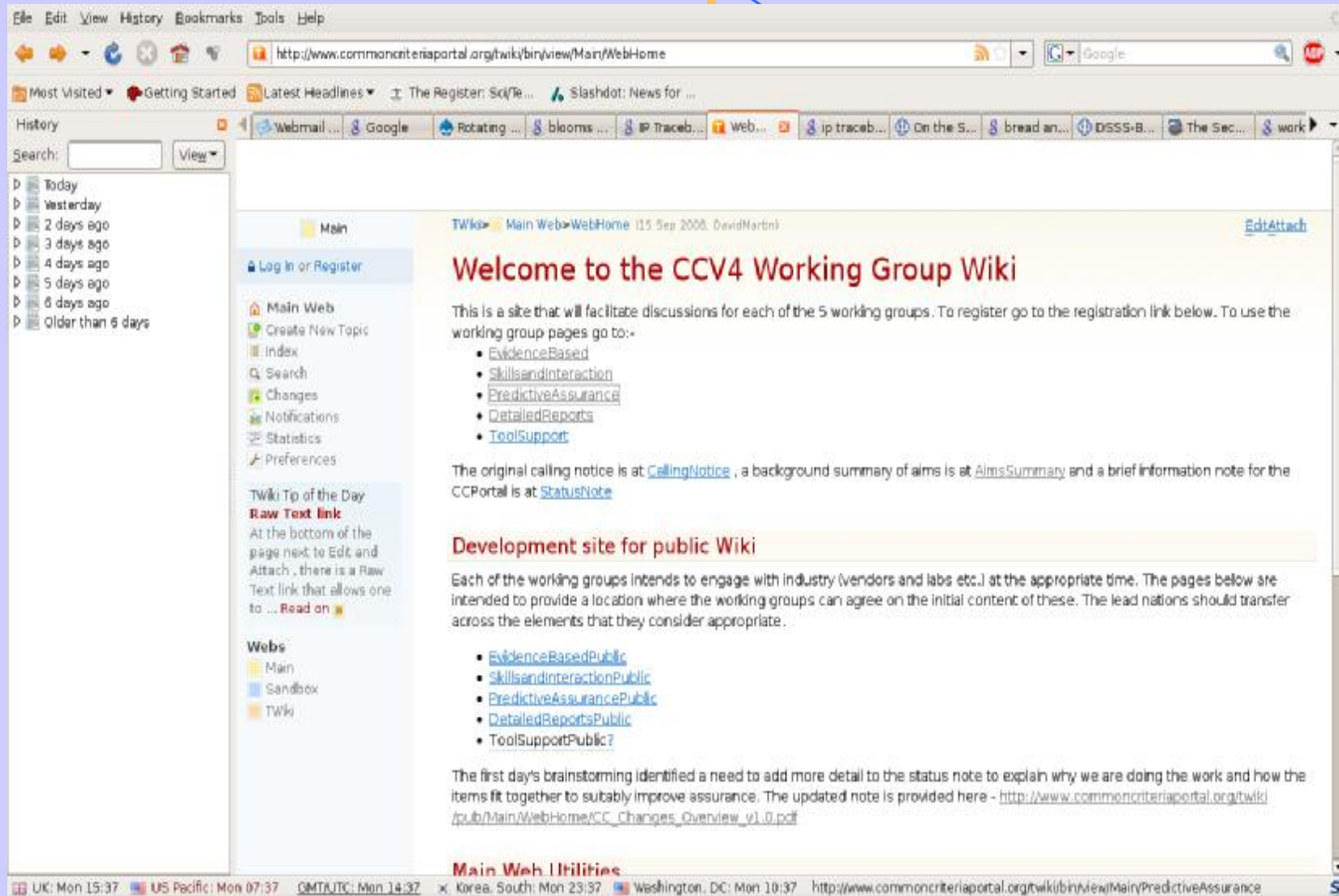
Progress

- n Working groups met in London June 08
- n Whole day discussion per workgroup
- n All agreed that these were difficult problems!
- n Brainstormed each issue and identified work items
- n Produced outline plans for progressing each task

Electronic support

- | For all schemes the costs of meeting together are quite high
- | So we aim to perform some of the work electronically.
- | We started using wikis in the London meetings
- | These are now being used to further the work before the next meetings

Example



The screenshot shows a web browser window displaying the CCV4 Working Group Wiki page. The browser's address bar shows the URL <http://www.commoncriteriaportal.org/wiki/bin/view/Main/WebHome>. The page content includes a navigation sidebar on the left with links for 'Log in or Register', 'Main Web', 'Create New Topic', 'index', 'Search', 'Changes', 'Notifications', 'Statistics', and 'Preferences'. The main content area features a heading 'Welcome to the CCV4 Working Group Wiki' and a list of working group topics: EvidenceBased, SkillsandInteraction, PredictiveAssurance, DetailedReports, and ToolSupport. Below this, there is a section titled 'Development site for public Wiki' with a list of public pages: EvidenceBasedPublic, SkillsandInteractionPublic, PredictiveAssurancePublic, DetailedReportsPublic, and ToolSupportPublic?. The footer of the page displays various time zones and the current URL.

File Edit View History Bookmarks Tools Help

<http://www.commoncriteriaportal.org/wiki/bin/view/Main/WebHome>

Most Visited Getting Started Latest Headlines The Register: Sci/Te Slashdot: News for ...

History Search: View

Today
Yesterday
2 days ago
3 days ago
4 days ago
5 days ago
6 days ago
Older than 6 days

Main

Log in or Register

Main Web
Create New Topic
index
Search
Changes
Notifications
Statistics
Preferences

Twiki Tip of the Day
Raw Text link
At the bottom of the page next to Edit and Attach, there is a Raw Text link that allows one to ... [Read on](#)

Webs
Main
Sandbox
Twiki

Twiki: Main Web>WebHome (15 Sep 2006, DavidMartini) [Edit/Attach](#)

Welcome to the CCV4 Working Group Wiki

This is a site that will facilitate discussions for each of the 5 working groups. To register go to the registration link below. To use the working group pages go to:-

- [EvidenceBased](#)
- [SkillsandInteraction](#)
- [PredictiveAssurance](#)
- [DetailedReports](#)
- [ToolSupport](#)

The original calling notice is at [CallingNotice](#), a background summary of aims is at [AimsSummary](#) and a brief information note for the CCPortal is at [StatusNote](#)

Development site for public Wiki

Each of the working groups intends to engage with industry (vendors and labs etc.) at the appropriate time. The pages below are intended to provide a location where the working groups can agree on the initial content of these. The lead nations should transfer across the elements that they consider appropriate.

- [EvidenceBasedPublic](#)
- [SkillsandInteractionPublic](#)
- [PredictiveAssurancePublic](#)
- [DetailedReportsPublic](#)
- [ToolSupportPublic?](#)

The first day's brainstorming identified a need to add more detail to the status note to explain why we are doing the work and how the items fit together to suitably improve assurance. The updated note is provided here - http://www.commoncriteriaportal.org/wiki/pub/Main/WebHome/CC_Changes_Overview_v1.0.pdf

Main Web Utilities

UK: Mon 15:37 US Pacific: Mon 07:37 GMT/UTC: Mon 14:37 Korea: South: Mon 23:37 Washington, DC: Mon 10:37 <http://www.commoncriteriaportal.org/wiki/bin/view/Main/PredictiveAssurance>

An Evidence based approach to evaluation

- n Led by the US and Sweden
- n Considering how to provide a parallel paradigm that acknowledges and provides credit for alternative techniques and methods to provide assurance.
- n Any documentation produced during the development process may be considered
- n Increased evaluator and developer interaction
- n Takes account of tool use

Skills and Interaction

- n Led by the UK and US
- n Underpins the other work items
- n Considering how to provide increased commonality in evaluator -
 - n Training,
 - n Assessment, and
 - n Interaction (Both within and between schemes).

Predictive Assurance

- n Led by Germany
- n Analysis of the vendor's product development process
- n Together with a greater understanding of the product's roadmap (e.g. key future changes),
- n and the flaw remediation process
- n Longer validity for the certification report.

Meaningful Reports

- n Led by Canada
- n Making reports (and other evaluation information) more meaningful
- n Providing the end users with the information that they need to make assurance decisions,
- n Help with overall system security architecture
- n Effective use of product security mechanisms.
- n Residual risks, and strengths/weaknesses of the product and development process.

Tools

- n Led by UK and Spain
- n Original aim - to define tools that will support all of the working methods described in the other work areas.
- n Redirected to define workflows (allowing development of tools) AND
- n To encourage use of tools by vendors.

General development process

- n To minimise resource loading on schemes as much of the work as possible is electronic.
- | Although the workgroups are separate they are closely related.
- | The use of Wikis helps to ensure consistency
- | Similar approach likely for external interaction

External Involvement

- | As soon as workgroups have determined their broad direction and strategy they will engage with vendors, labs, etc.
- | The appropriate timing and method will be set by each workgroup
- | This is likely to use wikis as well

Progress Towards Version 4

Overall plan

	2008				2009				2010			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Initiation discussion		■										
Wiki Discussions			■									
Industry and ICCC feedback				■								
Wiki Discussions within group and with I				■	■							
Workgroup meeting USA				■	■							
Definition of trials						■						
Trials							■	■	■			
Review outcomes										■	■	■
Implement CCDB/RA changes										■	■	■
Finalise CCV4 changes										■	■	■

Eventual Aim

- n Once the development work is complete and the improvements have been adopted by a suitable combination of agreement between schemes, changes to the criteria/CEM etc., then evaluations will have the following characteristics:-

Eventual Aim

- n Evaluations will be performed by the optimum combination of subject matter experts and assurance experts.
- n Readily accessible body of knowledge ('case law') will exist to draw upon.
- n Supporting interactions with other evaluators both nationally and internationally (with suitable protection for developer's IP)
- n Common assessment levels for evaluator skills.

Eventual Aim

- n Evaluators will examine evidence produced as a normal part of the development of a product
- n Examine the development process including the use of tools.
- n Clear focus on the flaw remediation process and the strategic future product development plans
- n Supporting the provision of 'predictive assurance'

Eventual Aim

- n Certificates used for international mutual recognition, BUT -
 - n The most important outputs from the evaluation process will be in the form of detailed reports aimed at a range of audiences:- e.g. System accreditors/risk owners, System developers, System users, Subsequent evaluation teams, etc.
- n Reports will use language and concepts best suited to each of their needs.

Overall Aim

To ensure that CC is held in high esteem by security professionals as an effective and efficient process, providing valuable results to users.

Towards Version 4

n Questions?



Progress Towards Version 4