



CCDB report to ICCC 11

- ◆ CC Development progress
- ◆ CC Development arrangements and plans
- ◆ Wider CCDB work



CC Development

- ◆ A key responsibility for CCDB
- ◆ Identified areas to improve 2-3 years ago
- ◆ Created 5 Lead Nation work groups to address these



CC Workgroups - 1

- ◆ Evidence based approaches
- ◆ Skills and Interaction
- ◆ Predictive Assurance
- ◆ Meaningful Reports
- ◆ Tools and Techniques



CC Workgroups - 2

- ◆ Each WG was aiming to produce generic requirements for subsequent use via supporting documents (or possible CC/CEM changes)
- ◆ Reported at last ICCC that progress had been variable and some groups had produced more than others.

CC Workgroups - 3

- ◆ Also reported at last year's ICCC, was the CCDB agreement that:-
- ◆ *“Protection Profiles and Supporting Documents should be created in concert with industry led consortia.*
- ◆ *Protection Profiles should have a comprehensive threat model*
- ◆ *The security features and assurance activities should incorporate “best practices” security features and development activities to mitigate these issues.”*

CC Workgroups - 4

- ◆ For most Working Groups it has become clear that their output actually needs to be technology specific.
- ◆ The first group to discover this was the evidence based group, followed by the skills and interaction group.
- ◆ In reviewing the goals of the 'Tools and Techniques' group this week the same conclusion has been reached
- ◆ The Predictive assurance WG may be different (and has produced output recently)

CC Workgroups - 5

- ◆ The CCDB has therefore decided that the tasks set for the work groups are best seen as goals rather than overarching work items
- ◆ In general the best place to pursue these goals is in technical communities that are focussed upon the particular needs of the respective technologies.

CC Workgroups - 6

- ◆ The existing work groups will therefore suggest the items that Technical Communities should consider as part of their work
- ◆ Then four of the existing workgroups will close.
- ◆ Predictive Assurance may continue further with the production of generic requirements (that can be tailored by Technical Communities)



More background

- ◆ The following 9 slides are from ICC10 but are repeated here as they provide an important and useful background which the CCDB has reviewed this week and found to still hold.

CCDB discussion of NIAP policy change

- ◆ Broad agreement with approach
- ◆ Want to examine some of the detail in practice
- ◆ Agreed that focussed development in technical areas is sensible and a good way to engage industry (as evidenced already by smartcards)
- ◆ *Maintain existing working groups for generic development and coordination points for more specific items from technical areas. (Now changed)*
- ◆ Seek to create Workgroups/consortia (*Technical Communities*) for each technical area

CC Development Rationale

- ◆ Historically - Original criteria based mainly on OS/SK security
- ◆ Extended to cover all products
- ◆ High level aims/objectives
- ◆ Leads to:-
 - CC and CEM that are too general
 - Differing interpretations
 - Not enough detail for confidence in recognition

CC Development Rationale –2

- ◆ The creation and success of technical area for smartcards and similar devices reflected that need for tighter definitions.
- ◆ Discussion in CCDB in Korea 2008 also covered scheme concerns about consistency between different technical areas

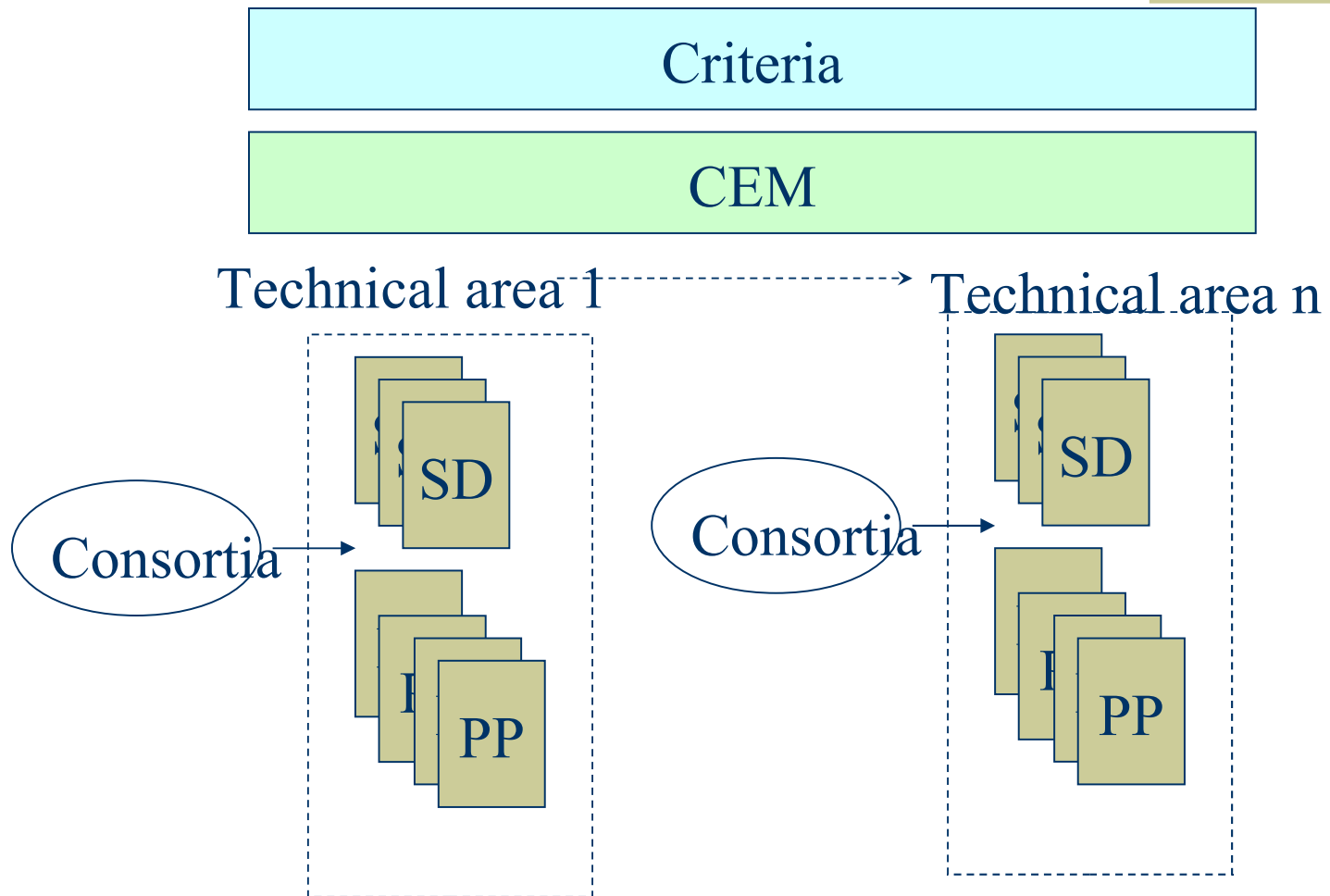
CC Development Rationale –3

- ◆ Smartcard work shows how successful a technical area can be:-
 - Working with a community
 - Relatively agile standards
 - Widespread support
 - Greater focus on vulnerability discovery
- ◆ Therefore extend this idea to other technical areas
- ◆ Key to success is the full involvement of all stakeholders including developers

Characteristics of Technical areas

- ◆ Differences in:-
 - Technology used
 - Evaluation approach
 - Evaluation skills
 - Evaluation tools
 - Development approach
 - Threat level addressed
- ◆ Possible to form collaborative groupings of vendors, users, evaluators

Simplified Overview





Scheme Role

- ◆ General Facilitation
- ◆ Form groupings
- ◆ Facilitate communication
- ◆ Provide threat input
- ◆ Ensure appropriate skills are applied

Possible Technical Areas

- ◆ Disk Encryption
- ◆ USB data storage
- ◆ Enterprise Security Management
- ◆ Firewalls
- ◆ Operating Systems
- ◆ Databases
- ◆ Browsers
- ◆ Etc.
- ◆ NB The above are in no particular order

Other Inputs to PPs

- ◆ PP and supporting document writers (and associated evaluation activities) will take account of relevant items from:-
 - Common Vulnerabilities and Exposures (CVE)
 - Common Weakness Enumeration (CWE)
 - Common Attack Patterns Enumerations and Configurations (CAPEC)

CCDB Discussion and Review -1

- ◆ All of the above represents a significant amount of work.
- ◆ Forming sustainable technical communities in particular takes time and effort.
- ◆ CCDB has been discussing many aspects of the work over the year

CCDB Discussion and Review - 2

- ◆ CCDB has also spent time to understand the national policies and requirements of each scheme around both existing CC evaluation and the role of cryptographic evaluation.
- ◆ Working towards an aim of harmonising CC evaluations involving cryptography
- ◆ Also discussing the potential for compatibility, in both directions, of FIPS (or any similar scheme) and CC related crypto evaluation.

CCDB Discussion and Review - 3

- ◆ As a first example of the principles agreed by the CCDB and covered in earlier slides, some early technical community work around the subject of USB memory devices has been examined during this meeting
- ◆ This has been shown to meet agreed principles.
- ◆ The PP and supporting documents will now be used in some evaluations (by two schemes) and results fed back to CCDB.

Changes in National Needs -1

- ◆ The CCDB has also discussed the market linkages that exist across the international schemes. The change in policy by NIAP was discussed last year. The UK is in transition, Australia and some others are considering transitioning to similar national policies.
- ◆ Individual scheme policies are obviously driven by national needs but the CCDB has spent time discussing both the rationale behind the changes in the respective national policies and their potential effects upon the market.

Changes in National Needs -2

- ◆ Clearly there are differences between national scheme policies in respect of the management of subjectivity in evaluations.
- ◆ The overall aim of the CCDB is to manage subjectivity (particularly in vulnerability search) via technical communities and existing CCRA mechanisms (CCDB interaction, VPA, etc.) – as discussed at ICC10

Changes in National Needs - 3

- ◆ These changes in national needs for some schemes are sometimes, simplistically, portrayed by some outside the CCDB as being a choice of EAL1 rather than EAL4
- ◆ This view is incorrect - The primary aim, which is shared by the CCDB, is to use technical community developed protection profiles and supporting documents.

Changes in National Needs - 4

- ◆ So the important thing is PP (and its requirements) compliance via assurance activities not just the EAL alone.
- ◆ The key difference between schemes is that some have to work towards these ‘bottom up’ while others choose to maintain the current practice while we develop the PPs and SDs

Changes in National Needs - 5

- ◆ The UK/US (and some others) are seeking, via the use of PPs and supporting documents, to minimise subjectivity until suitable technical communities are mature
- ◆ Other schemes prefer to use the existing subjectivity management mechanisms (CCDB interaction, VPA, etc) until the communities are mature.

Changes in National Needs - 5

- ◆ The CCDB does recognise the effects that changes in national policy can have upon the international marketplace for evaluations
- ◆ The CCDB has therefore taken time to hear and discuss the rationale for the changes
- ◆ Such policy changes are, however, national matters.



Moving Forward



- ◆ Vendor involvement
- ◆ Timescales
- ◆ CC/CEM changes



Vendor involvement

- ◆ Vendor involvement in technical communities is welcomed and strongly encouraged (essential!)
- ◆ Input and discussion
- ◆ IPR issues can be managed

How long will all this take?

- ◆ Short answer is that we don't know.
- ◆ Early Technical Community formation has taken longer than anticipated
- ◆ But the first results (USB PP) have been reviewed.
- ◆ Others are close to supplying drafts for CCDB information
- ◆ Vendor involvement can help speed up the development.

How do we find out about it?

- ◆ The hosting of the CC Portal has recently changed
- ◆ Time is needed to develop a wiki like communication mechanism on the new server.
- ◆ At that time information will be placed on the server regarding technical communities, contact points, progress etc.

Criteria changes - 1

- ◆ As discussed at ICC10:-
- ◆ Radical changes to the Criteria are neither necessary nor desirable.
 - **Not necessary** - because the criteria are flexible as implemented (and can be used with suitable supporting documents)
 - They are **not desirable** because major changes produce significant overhead for those groups such as the smart card community.

Criteria changes - 2

- ◆ What does this mean for ‘Version 4’?
- ◆ At present we believe that this work can all be accommodated in the existing process of an annual update
- ◆ Majority of the innovation is in the use of criteria via PPs and SDs



Summary

- ◆ Progress has been made
- ◆ Direction has been adjusted
- ◆ Most development to be via technical communities
- ◆ Providing even stronger interaction with industry and other groups
- ◆ Watch the portal for updates