

# Common Criteria – Where Next?

David Martin CESG

Chair of Common Criteria  
Development Board CCDB

# Schedule for Version 3

- 4 July – public review and trial use
- 1 November – comments due
- May 2006 – v3.1 released (ISO)
- July 2006 – MC endorsement
- Jan 2008 – no new v2.1 evaluations

# DB Technical Vision - Objectives

1. Long term technical vision and strategy for the development and evolution of the information security evaluation criteria, methodology and guidance
2. Serves as a baseline for accepting new work items and for communicating the CCRA technical strategy to external organisations, consumers, etc.

# DB Vision Statement - Vision

- Continuously improve the cost and time effectiveness of the evaluations
- Reduce the uncertainty of the end user in the use of IT
- Embrace new technology areas, and be continuously maintained and evolved, in rapid adaptation to the technology development.

# DB Vision Statement - Strategy

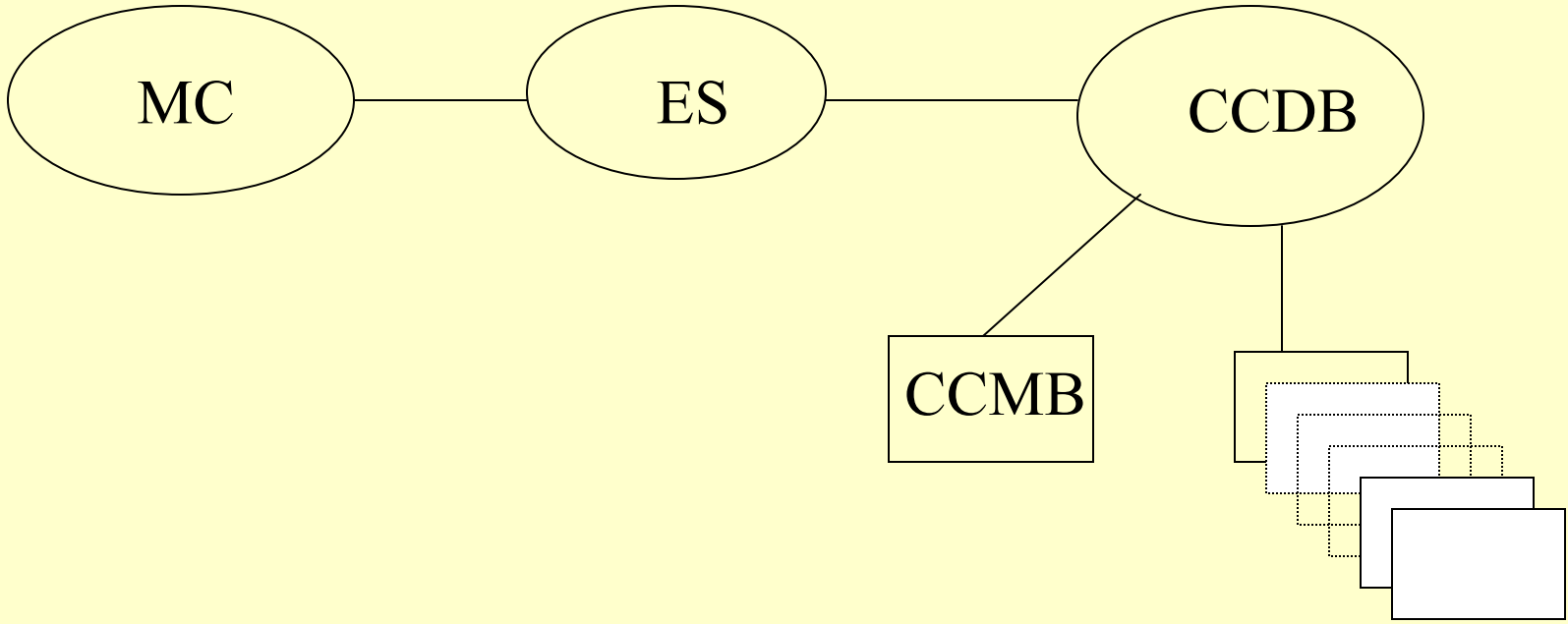
- Structure documents to provide responsiveness (Example - Supporting documents)
- Incorporate measurement where possible and sensible
- Identify new technology areas,
- Focus on harmonisation issues

# Supporting Documents

- Smartcard and similar hardware – current documents are being converted
- Platform (standard hardware)
- Operational System evaluation
- Biometrics (later )

*NOTE: All the above areas are subject to approval from Management Committee*

# CCRA Development Structure



Working Groups

# Working Groups

- Certificate maintenance processes – FR lead
- Probabilistic Methods – UK lead
- Certification of Developer Sites – GE lead
- Develop the PP/ST Guidance for Version 3
- Develop Guidance for Developers on how to produce evaluation evidence.
- Transitional mapping guidance to V3

# Metrics -1

- Some schemes collecting statistics on the value of individual elements of CC
- One study of changes to a product over a significant length of time found that increased code analysis would be of great benefit.

# Metrics – A study (early results)

- Errors found -
  - 29% *Design Flaws*
  - 71% *Implementation Flaws*
- *CC Activity (awarded to earliest first – structure of CC)*
  - *Functional Specification 13%*
  - *Design Activities 21%*
  - *Implementation Representation 56%*
  - *Independent Testing 4%*
  - *Penetration testing 3% (but 86% confirmation)*

# Metrics – Vulnerability detection

- EAL1 - 12%
- EAL2 - 19%
- EAL3 - 37%
- EAL4 - 71%
- EAL5 - 95%
- Realistic ‘black box testing’ – 29%

# Metrics Study - Possible Conclusions

- Code analysis has significant benefits (ADV helps guide this – especially version 3)
- Even simple tools help – (developers should be using at least these)
- Approach the evaluation from a ‘flaw hypothesis’ viewpoint

# Harmonisation

- Assurance Continuity
- Security Targets
- Scope of TOE
- Evaluator skills/training
- Various Others

# Communications and Interaction

- Marketing work from Sweden suggested a need for increased interaction
- Working Groups can already incorporate industry and others (ideally via existing industry groups)
- Other levels of interaction welcome but need to be in a focussed way.

# Scheme Director relaxation

- The Scheme Directors of:-
  - Australia/NZ
  - France
  - UK
  - US
- Relaxing after a hard week of meetings!







# Questions?

**<http://www.commoncriteriaportal.org>**