



ISO/IEC JTC 1/SC 27 **N 8117**

ISO/IEC JTC 1/SC 27/WG 3 **N 38117**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: other

TITLE: CCDB LS Officer presentation

SOURCE: 39th SC 27/WG 3 meeting

DATE: 2009-11-06

PROJECT:

STATUS: This document was made available at the 39th SC 27/WG 3 meeting held in Redmond, US, 2nd – 6th May 2009. It is circulated within SC 27 for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Bañón, M.C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 38



CCDB Liaison

- ◆ CC Development progress
- ◆ CC Development arrangements and plans



CC Development progress-1

- ◆ One year ago we originally created 5 working groups
 - Evidence based approaches
 - Skills and Interaction
 - Predictive Assurance
 - Meaningful Reports
 - Tools and Techniques



CC Development progress-1

- ◆ Added Implementation Assurance and Entry level Assurance in March CCDB
- ◆ On review this meeting, Implementation Assurance considered adequately covered by other groups and closed.
- ◆ ‘Entry level’ – deferred until the results of existing workgroups (particularly evidence based) can be reviewed – each group will take account of entry level needs.



CC Development progress-2

- ◆ Some progress made in 2009 - Especially from Predictive Assurance, Meaningful Reports, and Tools and Techniques
- ◆ However - NIAP policy change together with associated strategic thinking regarding CC development led to a need to review and reform WG roles at March 09 meeting.
- ◆ Very useful set of workgroup meetings in June brought further clarity and set short term goals.



Summary of NIAP policy changes



- ◆ No longer automatically accepting products without Protection Profile
- ◆ Developing range of new ‘Standard’ PPs and supporting documents (in defined technical areas) – containing detailed assurance activities
- ◆ Starting at low EALs but then working with vendors/labs/users to increase assurance ‘state of the art’ in that technical area
- ◆ Changing all procurement policies to suit



CCDB response



- ◆ 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.
- ◆ Seek to create workgroups/consortia 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:-
 - Does EAL4 of a smartcard really equal EAL4 of a large OS/DB/Firewall appliance?
 - How do we address this?



CC Development Rationale –3

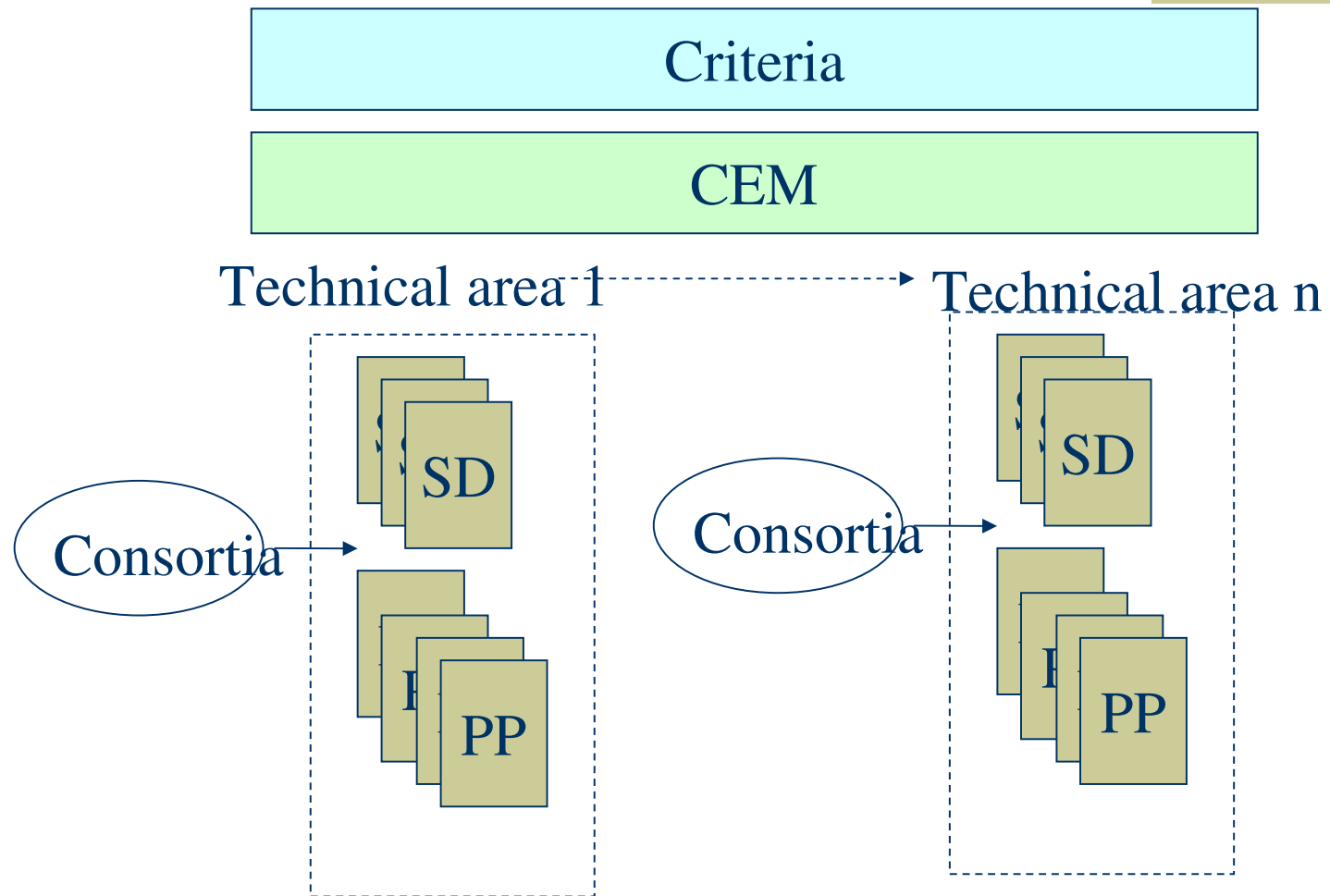
- ◆ Smartcard work shows how successful a technical area can be:-
 - Working with a community
 - Relatively agile standards
 - Widespread support
 - Greater focus on vulnerability discovery
- ◆ Therefore extend this idea to other technical areas
- ◆ Key to success is the full involvement of all stakeholders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





Common items

- ◆ Existing working groups will continue to produce overarching documents needed by all/many technical areas.
- ◆ For example the Tools and Techniques working group will be producing a supporting document for secure software development.
- ◆ The evidence based group is producing a common PP requirements document.



Inputs for CCDB consideration

- ◆ US already have a disk encryption PP as an example of a new approach using existing criteria
- ◆ And a ‘Common Requirements’ document for PPs
- ◆ Both have been supplied to CCDB for review



Protection Profiles and Supporting Documents



- ◆ Where this is not already the case, 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.



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)



Eventual effect upon criteria-1

- ◆ 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.



Eventual effect upon criteria-2

- ◆ Changes to the Criteria may be needed to facilitate the use of supporting documents to cover development practices and a wider range of vulnerabilities such as implementation flaws.
- ◆ There may also need to be a change for entry level (eventually resulting from that working group)



Eventual effect upon criteria-3

- ◆ 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
- ◆ We are also working on some known concerns in criteria (mainly around ADV) and wording in areas such as FLR via input from schemes



Implementation Assurance

- ◆ No longer a specific group
- ◆ All Working Groups are exploring implementation issues to improve Common Criteria evaluations.



Examples of group interactions

- ◆ The following examples and others will be managed through the overall project plan which is under development.



Evidence Based

- ◆ Working with Tools and Techniques group to have ADV_* and ALC_TAT more clearly reflect how to incorporate development practices and the use of software development tools.
- ◆ The results of this work will be incorporated into a Supporting document that describes how development practices and tools can be integrated into the Common Criteria.



Skills and Interaction



- ◆ Working with the Meaningful Reports WG to explore what information has to be disclosed to Schemes when an evaluation has a subjective component that requires an expert evaluator.
- ◆ The two groups will explore what information has to be disclosed for consumers of the products to have confidence in the products.
- ◆ The groups will also work with Evidence Based WG on ‘external’ assessments such as FIPS and black box testing services



Workgroup outline plans - 1



- All currently in outline only – dates may change
- Project Manager appointed to coordinate
- Producing definition of project and project mandate to ensure interaction and coordination.



Workgroup outline plans - 2

- Planning to hold workgroup coordination meetings at next CCDB and in June 2010
- Trials are essential – Industry partners have indicated willingness
- Technical Area rationales to be produced by workgroups/consortia for CCMC approval - most drafts by next CCDB meeting
- CC and CEM will be updated in annual cycle (without major change)



Evidence Based

- Evidence Based
 - Scope definition – Feb 2010
 - Develop Scope of Work – April 2010
 - Update ADV June 2010
 - 6 Standard PPs (in priority order) – Dec 2010
 - Trials through 2011 – results at ICC



Skills and Interaction -1



- Primary Research – August 2010
- Propose Interaction Mechanisms - April 2010
- Vulnerability sharing – based upon ISO progress
- Develop examples based upon technical areas – October 2010



Skills and Interaction -2



- Work with Meaningful Reports WG on disclosure mechanisms (public and scheme) –August 2010
- Trials – completion June 2011
- All of the above to have significant progress demonstrated through interim outputs



Predictive Assurance



- ◆ Goal: Provide a degree of “predictive assurance” where the conclusions of an evaluation report could remain valid for a much more realistic and usable length of time
 - Survey performed
 - Good support from vendors

Predictive Assurance plan

Project phases	Target date for completion
Develop an expanded version of the concept Take into account: <ul style="list-style-type: none">- Feedback on questionnaire- Input from CCRA Schemes (Contributing Nations)- CCRA principles	January 2010
Conduct trial projects for a „predictive assurance process“	December 2010



Meaningful Reports



- Stakeholder identification – Oct 2009
- Gather/categorise needs – Dec 2009
- Identify areas to increase information – Mar 2010
- Agree optimal approach – June 2010



Tools and Techniques

- Paper produced in collaboration with industry
- Next stages:-
 - Working with Evidence group merge into ADV etc – June 2010
 - Producing a Supporting Document – July 2010
- Trials during this time and to follow.



Plans on Portal



- The plans above are at an early stage
- The overall coordinated plans will be published on the portal shortly
- This will be followed by the opening up of the industry discussion wiki areas.



Plans published on Portal



- The plans above are at an early stage
- The overall coordinated plans will be published on the portal shortly



ISO

- ◆ Increased interaction
- ◆ Wish to work together to align ISO Technical reports with CC Supporting Documents



Summary

- ◆ Progress has been made
- ◆ Direction has been adjusted
- ◆ New approach combines strength and flexibility
- ◆ Work group plans described
- ◆ Aiming for even stronger interaction with industry and other groups
- ◆ Watch the portal for updates



Questions?

