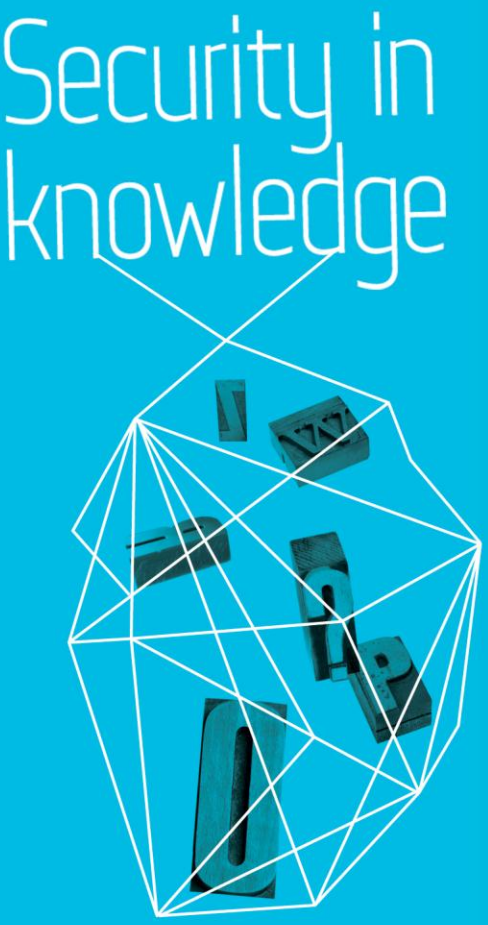
# THE CERTIFICATION OF PRODUCTS OR ACCREDITATION OF ORGANIZATIONS: WHICH TO DO?




**Moderator:**

Dan Reddy
EMC Corporation

**Panelists:**

Joshua Brickman
CA Technologies

Donald Davidson
DOD-CIO (TMSN)

Steven Lipner
Microsoft Corporation

David Martin
Common Criteria Development Board

Session ID: PNG-W23

Session Classification: Intermediate

# Selected Product Evaluations vs Organizational Accreditations

| Organizational Accreditation | Domain | | Product Evaluations | Domain |
|---|---|---|---|---|
| Capability Maturity Model Integration (CMMI) | Process Improvement | | FIPS 140-2 or ISO/IEC 19790 | Crypto |
| Open Group's *Open Trusted Technology Provider Standard* (O-TTPS) | Mitigating Taint & Counterfeit | | Common Criteria (ISO/IEC 15408) | Security Properties |
| Payment Card Industry (PCI) | Merchant Security | | Tempest | Data Loss via Emanations |
| ISO/IEC 9000<br>ISO/IEC 27001<br>ISO/IEC 27036 | Quality<br>Info. Sec. Mgt.<br>Sec. - Supplier Relationships | | Commercial Product Assurance (CPA-UK);<br>DoD Approved Product List (APL-USA) | Country & Agency Specific Assurance |

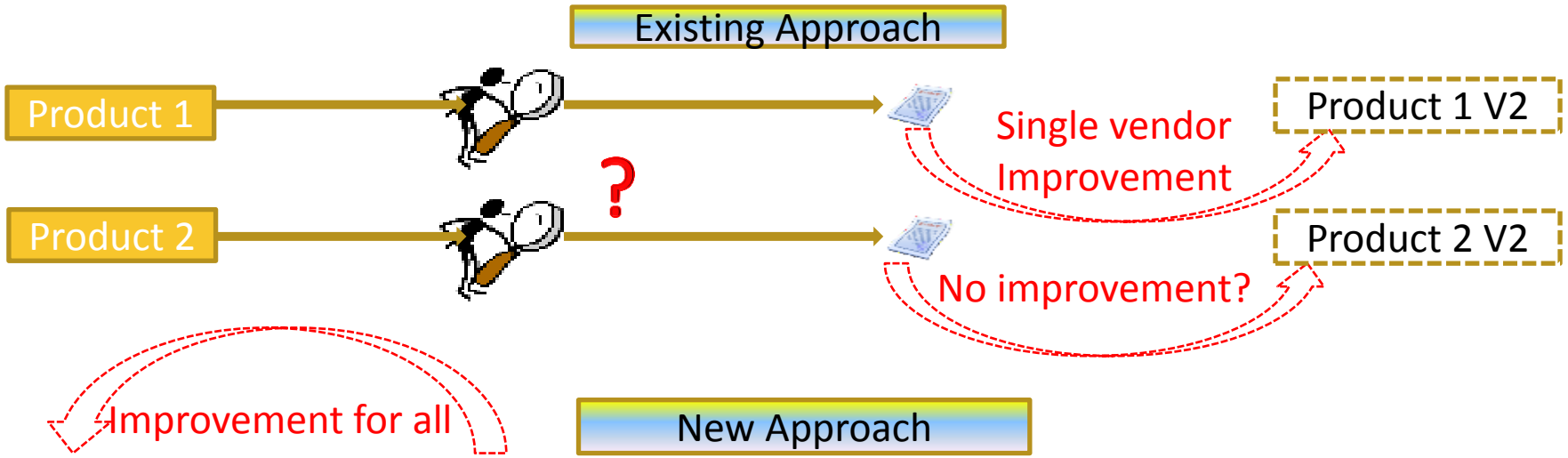
# Update on Common Criteria (CC)

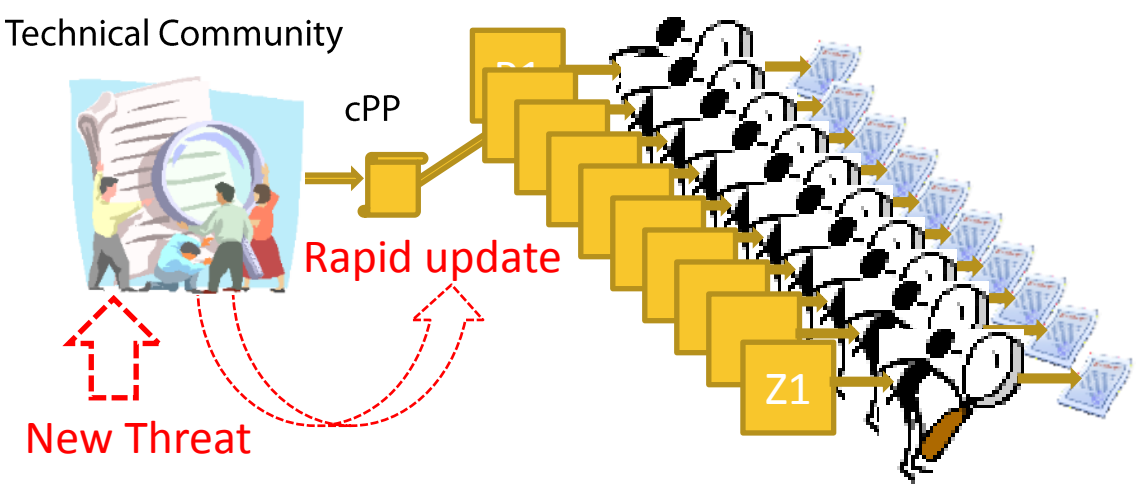
- What are the changes detailed in the vision statement published in September 2012?
- See link on front page of www.commoncriteriaportal.org
- Focusing on one key item
- Via a picture and a summary table

Note - CC Glossary:

- PP=Protection Profile
- cPP=Collaborative Protection Profile
- EAL= Evaluation Assurance Level
- TC= Technical Community

# *CC Update:* The Power of Peer Groups




**Improves**

- Speed to evaluate
- Speed to respond to threats
- Relevance to users
- Scalability – many more products
- Comparability
- Real Assurance

# *CC Update:* Comparison - EAL vs cPP

| Classical 'EAL' focussed Evaluation | TC/cPP focussed Evaluation supports:- |
|---|---|
| Mostly an 'Open loop' process | Multiple, rapid feedback loops for evaluation findings, new threats etc. |
| Evaluator judgements based mainly on their understanding of technology/threat | Harnesses the power of all experts in technical communities |
| Improvements limited to version/vendor | Expertise benefits all similar products |
| Relatively long evaluation time | Much shorter evaluation time |
| Not easily scalable | Readily scalable |
| Complex to use for product comparison | Sound basis for comparability |
| Relatively low assurance in most cases (EAL4 = more activity ≠ more security) | Assurance of peers – Highest common level of fully international assurance |
| Bespoke 20th century approach to 21st century needs? | Standards approach – linked to needs of development, users, and procurement |

# *CC Update:* Ongoing Efforts

- Continue to build strong link to CC User Forum – not just a 'government thing'
- Improve links to procurement/maximize market
- Plan to update CC standard focused on lower EALs and PPs authored by technical communities
- Work to align cryptographic functional/assurance needs
- Support pilots for Supply Chain (SC) Technical Working Group
- SC working group developed guidance for PP authors.

# Comparison for Information and Communications Technology (ICT)

| | ACCREDITATION OF ORGANIZATIONS | CERTIFICATION OF PRODUCTS |
|---|---|---|
| Focus | Practices of an organization that makes a set of products or delivers a set of services | Security assessment of a product version or versions |
| Pros | Some security attributes are inherently process rather than product (e.g. supply chain). Encompasses multiple products over time. | More specific to a particular product or version. Requirements can be more rigorous and objective |
| Cons | Evaluating practices involves both quality of process and consistency of its execution. Assessing consistency implies examining product. | Not as general as organizational certification. Some aspects of security are inherently process. Cost of assessing each product separately |
| Summary | Long-lived but limited fidelity. Some real challenges | Limited lifetime but high fidelity. Some real challenges |

# Summary: Which to Do?

- Certification of Products or Accreditation of Organizations?
  - Dichotomy is overstated –
    - Product assessment relies on evaluation of process/organization
    - To be credible, organization assessment requires some evaluation of products/artifacts
  - Customer priorities determine whether to choose one, the other, or both
    - Do you prioritize an organization that practices solid product development, secure engineering and supply chain security for its products?
    - Do you prioritize high confidence in specific security features for a product?
    - What level of assurance conveys confidence and trust?
  - Other factors
    - Government policy mandates
    - Demand by ICT Providers for accreditation from component suppliers
    - International recognition
    - Experience with results of early accreditations/certifications