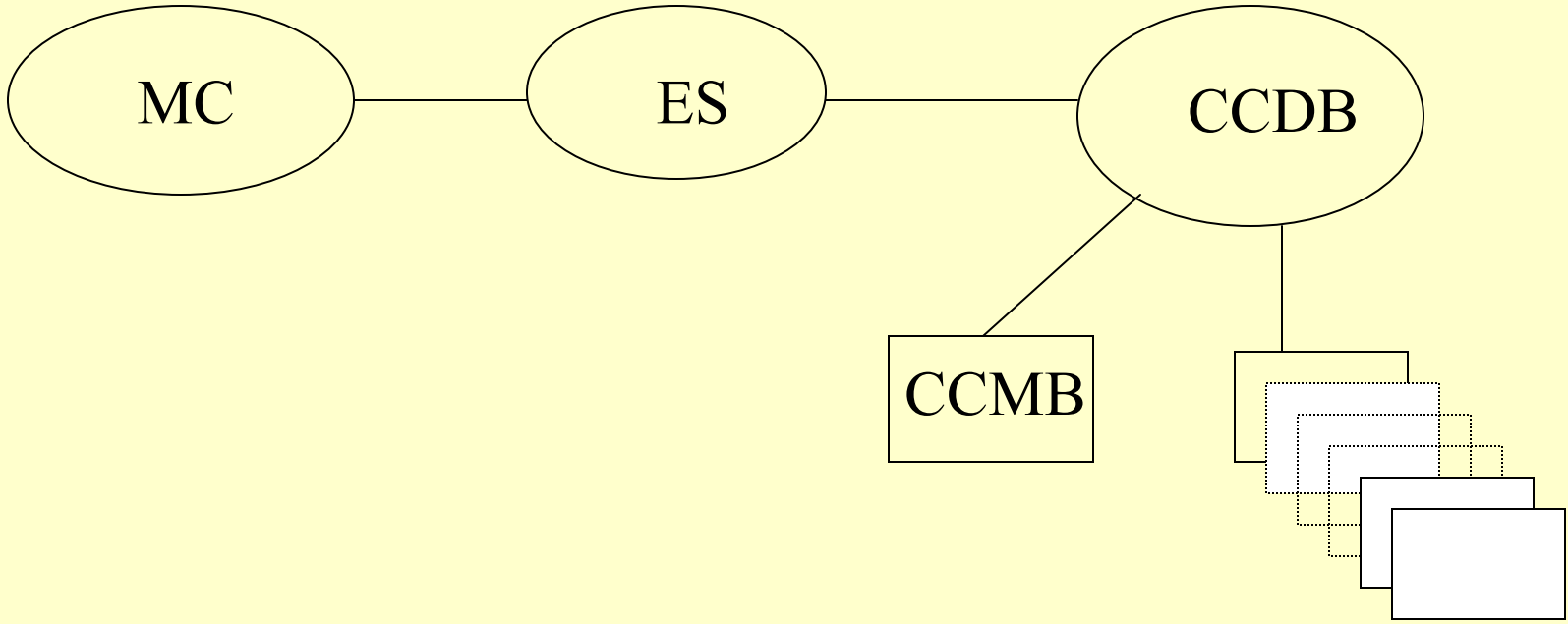


CC v3.0 Update

David Martin CESG

Chair of Common Criteria
Development Board CCDB

CCRA Development Structure



Working Groups

Schedule

- 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

Part 2 - improvements

- terminology problems were resolved
 - concepts were simplified and clarified
- underlying paradigm made more uniform
 - SFRs are at constant level of specificity
- more examples provided
- annexes gone
- 354 pages pared down to 127
- 11 classes reduced to 6

Part 2

1. Data Protection and Privacy

- actions that occur internally in the TOE, such as access control
- Internal entities, their attributes, and operations are defined

2. Identification, Authentication, and Binding

- Interaction between outside world and internals
- Linking users to subjects, dissolving this link, etc.

Part 2

3. Communication protection
 - Confidentiality, integrity, availability
4. Audit
 - logging of and responding to security-relevant events
5. Protection of the TSF
 - Testing, breakdown, recovery of TSF
 - Tamper-evidence, -detection, -prevention
6. Miscellaneous
 - Time-stamp, random-number generation

Part 3 – ASE, APE

- **Removed repeated work with no benefit**
- **Guidance on Threats, OSPs, Assumptions, Objectives**
- **TOE vs Environment**
- **PPs/STs that pass requirements now more meaningful**
- **No longer a SOF claim**
- **TSS: how does TOE meet the SFRs**
- **Consistency and coherence**

Part 3 - ACM, ADO, AGD, ALC

- v2.1 had lots of overlap
 - Configuration management is over entire lifecycle
 - Admin actions include start-up

- recast into two families
 - ALC: developer site
 - AGD: customer site
 - includes misuse analysis

Part 3 – ADV

- SFR-enforcing, SFR-supporting, SFR-non-interfering
 - Entire TSF no longer treated uniformly
 - Functional spec now more granular
- HLD and LLD merged into TDS
 - Removed the 2 levels of decomposition
- New ARC family
 - TSF self-protection, non-bypassibility

Part 3 – ADV (cont)

- INT.1 assignment
- RCR merged into each representation
- SPM: only formal model
- Requirements now scale with EALs
- More text but not more work

Part 3 - ATE

- Updated only to reflect new ADV
 - COV based on interface testing

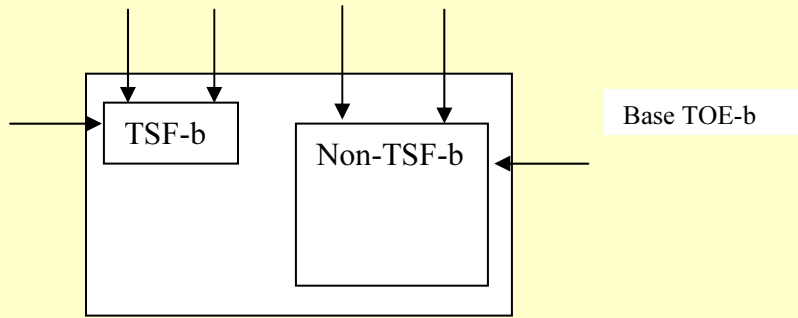
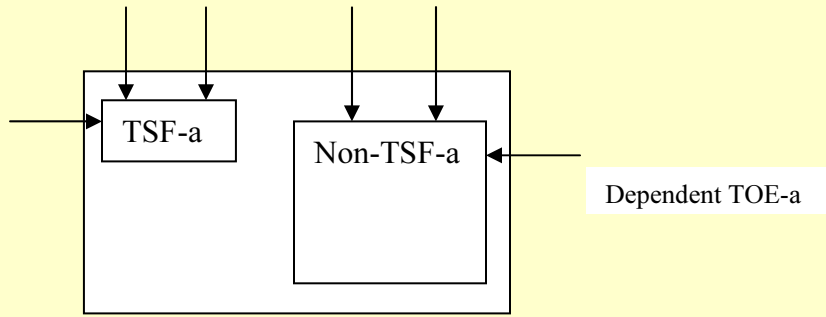
Part 3 - AVA

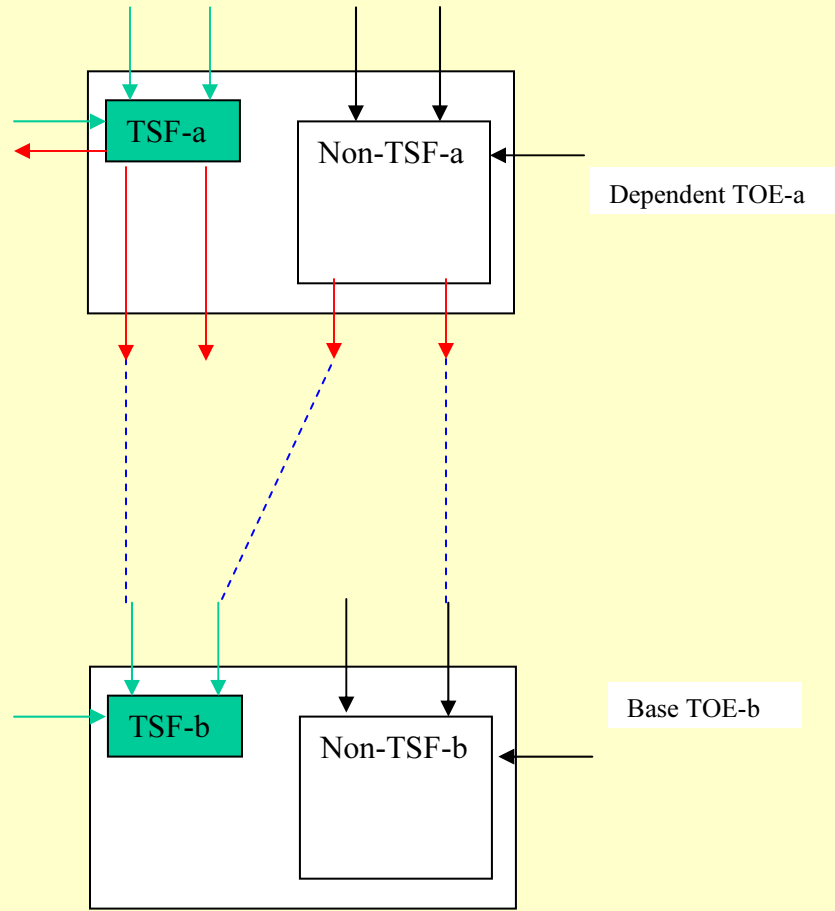
- AVA_MSU moved into AGD
- AVA_SOF removed; methodology merged into Vulnerability Analysis
- AVA_CCA removed (Vulnerability Analysis application note)
- New AVA_VAN.1 includes public domain search by evaluator

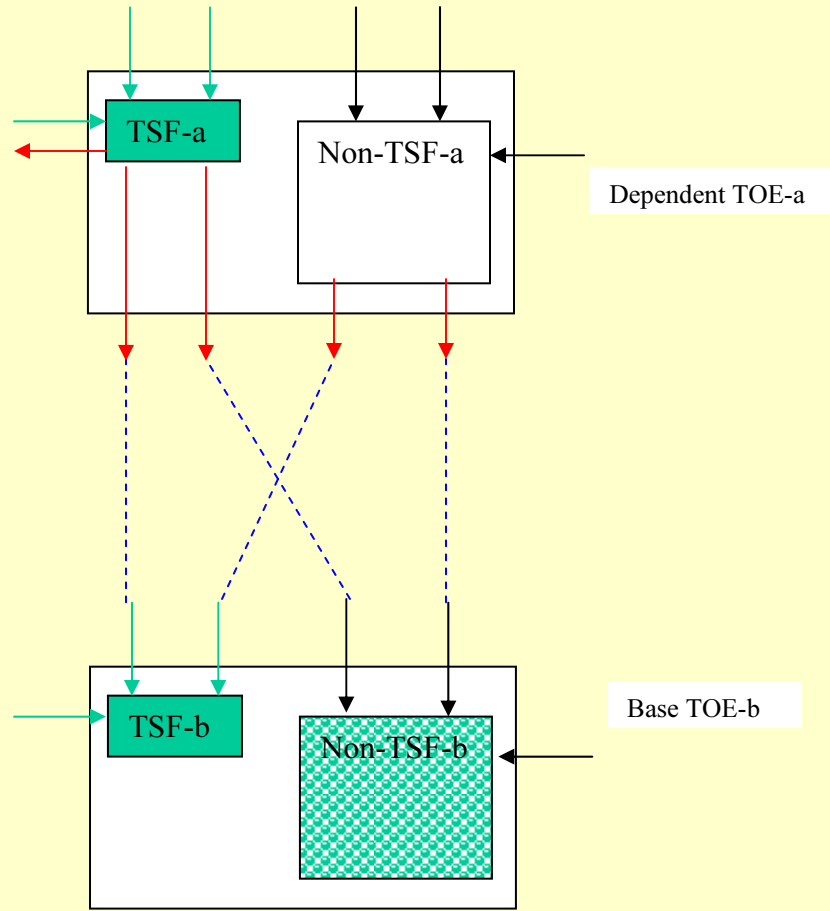
Part 3 - ACO

Composition

- TOE uses an already-evaluated underlying environment
- No other definition of “composition”
- Use of underlying interfaces







Methodology

- **Arranged by Class/Family/Component**
- **Not limited to EAL4 components**
- **MR still limited to EAL4**



Questions?

<http://www.commoncriteriaportal.org>