CESG

David J Martin

Assurance Services Technical Director

The Assurance Paradigm for Lower Assurance Levels:

Should there be a greater level of testing?

David J Martin
Assurance Services Technical Director
Mike Brown
Senior Certifier
CESG

ICCC, September 2008

Outline of the talk

- CC Definition of "Low Assurance"
- EAL1/EAL2 Evaluation Issues
- Low Assurance Schemes in UK and France
- CESG Claims Tested Mark (CCTM) Scheme
- Comparison of CCTM and EAL1/EAL2
- Proposed Low Assurance Paradigm
- Proposed Refinements to EAL1/EAL2
- Proposed Refinements to Documentation
- Questions

CC Definition of "Low Assurance"

- EAL1: Functionally Tested
  - Evaluation, without assistance from the developer
  - Minimal outlay
  - Limited Security Target
  - TOE operates consistently with product documentation
  - Public domain vulnerabilities search & independent testing
- EAL2: Structurally Tested
  - Co-operation of developer
  - Should not increase developer cost/time
  - Full Security Target
  - Inputs: Sec arch, func spec, basic design, developer tests, config list & developer procedures (CM, Delivery)
  - Vulnerability Analysis & independent testing

Differences between EAL2 & EAL3

- EAL3: Methodically Tested and Checked
  - Co-operation of developer – assurance in design
  - Should not alter existing development practices
  - Full Security Target
  - Inputs: Sec arch, func spec, **arch** design, developer tests, config list & developer procedures (CM, Delivery & **security**)
  - Vulnerability Analysis & independent testing
  - More complete **testing coverage**
- In summary: not a significant difference, although vulnerability analysis may be improved

Low Assurance CC Certificates

- 847 EAL1-EAL7 CCRA certificates (20/08/08)
- Few EAL1 certificates
  - only 30 at EAL1 and 19 at EAL1 augmented
- Many more EAL2 certificates
  - 158 at EAL2 and 63 at EAL2 augmented
- But EAL3 less popular
  - 101 at EAL3 and 74 at EAL3 augmented

EAL1/EAL2 Evaluation Issues

- Costly compared to industry specific assurance schemes
- Preparation & Evaluation can be time consuming
- Security Target (ST) is significant extra document
  - SFRs are not well understood by developer or customers
  - Requires CC experts/consultants to produce
- CCRA documents are large part of overall costs/time
  - ST, ETR & Certification Report
- Emphasis on documentation rather than product security testing
- EAL2 not significantly different from EAL3
- Bottom line – too costly & slow; not value for money

Low Assurance Scheme (FR)

- "First Level Security Certification" Scheme
- Operated by DCSSI
- Addresses Security Products
- Offers certification of open source software
- Provided at reasonable evaluation cost
- Evaluation performed by Licensed Eval Facilities (not ISO 17025 accredited)
- Checks product conformity to Security Target
- Checks product efficiency/effectiveness

First Level Security Certification

- Inputs: Security Target & user guidance
- Evaluates I&A, access controls, A-V, etc
- Based on light criteria and methodology
- Uses existing CC/ITSEC processes selectively
- Based on fixed schedule and workload
- Results detailed in ETR
- DCSSI validates Security Target & ETR
- DCSSI audits evaluator skills & competencies
- DCSSI publishes ST & sec recommendations

Low Assurance Scheme (UK)

- "CESG Claims Tested Mark" (CCTM) Scheme
- Operated by CESG
- Addresses Security Products & Services
- Provided at reasonable evaluation cost
- Evaluation performed by appointed Test Laboratories (ISO 17025 accredited)
- Checks conformity to "Security Target" claims
- Checks ease of use, public vulnerabilities
- Results in award of CCT Mark Certificate

CESG Claims Tested Mark Scheme

- Inputs: IA Claims Document (ICD) & user guidance
- ICD specifies security claims & test approach
- Test Lab performs basic checks on ICD
- Test Lab (generic or specialist) evaluates security claims
- Based on light methodology (CEM test philosophy)
- Test Lab uses any existing CC/ITSEC processes
- Testing/reporting limited to about 20 days maximum
- Results detailed in Test Report (TR)
- CESG Decision Authority validates ICD & TR
- UKAS audits evaluator skills & competencies
- CESG publishes ICD & Test Report Summary
- CESG approves Marketing Statement

CCTM Scheme (2)

- ICD: a lightweight Security Target including:
  - Product/service description (h/w, s/w, architecture)
  - Security environment (assets, threats, OSPs & assumptions)
  - Security functionality claims in plain English
    - Claims exclude crypto, except for simple obscurity tests
    - Claims relate to specific platforms – all claims tested on each platform
  - References to existing assurance certificates
  - Test Approach
  - Note: More content than CC (EAL1) Limited ST
- Test Report: concise report including:
  - Executive summary, test overview & test results
  - Test details (scope, configurations, etc)
  - Consumer guidance & recommendations
- Certificate: Limited life (Products: 2yrs, Services 1yr)
  - Services only: Extendible by up to 1yr under maintenance
  - (Currently under review: 2-yr certificates; no maintenance?)

CCTM – EAL1 Comparison (1)

EAL1	CCTM	ICD Requirements
ASE_CCL.1	N/A	No CC or PP conformance claims
ASE_ECD.1	Y	Plain English claims, can use CC basis
ASE_INT.1	Y	TOE Id, description & overview
ASE_OBJ.1	Y	Introduction describes TOE purpose
ASE_REQ.1	Y	TOE security functionality claims and environmental security requirements
ASE_TSS.1	Y	TOE overview and basic architecture

CCTM – EAL1 Comparison (2)

EAL1	CCTM	CCTM Requirements
ADV_FSP.1	Partial	Overview of functionality in operational user guidance, product specs (less detail)
AGD_OPE.1	Y	Operational user guidance provided
AGD_PRE.1	Y	Operational user guidance details all preparative procedures; (Test Report addresses Ease of Use)
ALC_CMC.1	Y	TOE & platform components identified
ALC_CMS.1	P	TOE documentation Id not required
ATE_IND.1	Y	**All** security claims & platforms tested
AVA_VAN.1	Y	Public domain vulnerabilities tested

CCTM – EAL2 Comparison (1)

EAL2	CCTM	ICD Requirements
ASE_CCL.1	N/A	No CC or PP conformance claims
ASE_ECD.1	Y	Plain English claims, can use CC text
ASE_INT.1	Y	TOE Id, description & overview
ASE_OBJ.**2**	Partial	Introduction describes TOE purpose
ASE_REQ.**2**	P	TOE security functionality claims & environmental security requirements
ASE_SPD.1	Y	Assets, threats, OSPs & assumptions
ASE_TSS.1	Y	TOE overview and basic architecture

CCTM – EAL2 Comparison (2)

EAL2	CCTM	CCTM Requirements
ADV_ARC.1	N	Basic architecture, not TOE protection
ADV_FSP.**2**	Partial	Overview of functionality in operational user guidance, product specs (less detail)
ADV_TDS.1	N	Only TOE description provided
AGD_OPE.1	Y	Operational user guidance provided
AGD_PRE.1	Y	Operational user guidance details all preparative procedures; (Test Report addresses Ease of Use)
ALC_CMC.**2**	N	No identifier requirement
ALC_CMS.**2**	P	**Full configuration list not required**
ALC_DEL.1	P	Operational user guidance describes consumer aspects of delivery

CCTM – EAL2 Comparison (3)

EAL2	CCTM	CCTM Requirements
ATE_COV.1	Partial	No developer evidence required; 100% coverage by tester
ATE_FUN.1	N	No developer evidence required
ATE_IND.**2**	Partial	All security claims & platforms tested No Functional Spec required No developer resources required
AVA_VAN.**2**	P	No vulnerability analysis required

Proposed EAL1 Paradigm

- Only product-supplied or vendor (website) documentation to be used as input
- Product specification & brochures used to validate TOE scope and SFR test approach/coverage
- ITSEF focusses on developing security tests of all SFRs (positive & negative tests) to provide maximum coverage & depth within set workload constraints
- Security products limited in complexity to ensure that all SFRs can be tested within set constraints
- Certificates are time expired, but maintainable (see Continuity Paradigm later)

Proposed EAL2 Paradigm

- Developer test docs & tools available to support more comprehensive security tests within set constraints
- Product specification & brochures used to validate TOE scope and SFR test approach/coverage
- Basic Design evidence may be gathered by ITSEF from developer discussion and detailed in ETR annex to aid understanding & testing
- No mapping of security tests to SFRs required from developer (not standard lifecycle documentation)
- ITSEF witnesses or repeats a reasonable test sample
- ITSEF focusses on developing any obviously omitted security tests to supplement developer security tests (positive or negative tests & boundary conditions)
- Adopt a VAN-centric approach – see CESG website

Possible EAL1/EAL2 Refinements

- Drop EAL1? (Small businesses may suffer)
  - Or address the intended purpose of EAL1?
- Increase differences between EAL1, EAL2 & EAL3, without changing EAL3
- Make EAL1 & EAL2 cost effective & test oriented
  - Provide lightweight evaluation approach
  - Focus on security testing
  - Reduce all documentation requirements
- Maintain mutual recognition
- Facilitate assurance continuity
  - Evaluators check changes and (if required) supplement tests
  - Evaluators produce Maintenance Report

Proposed EAL1 Refinements

- Require only Limited ST and operational user guidance, including release notes
  - Replace functional spec with product spec(s)
  - Identify TOE components & docs in Limited ST
  - (Full configuration list not normally provided with product)
- Extend Limited ST to facilitate security tests
  - ITSEF & Scheme perform basic checks during Preparation
- Aim 100% SFR testing by ITSEF
- Approx 20 days max for Evaluation & Reporting
- Reduce ETR detail (focus on exceptions & consumer)
- Scheme validates ST & ETR
- Scheme publishes ST & ETR Summary

Proposed EAL2 Refinements

- As for EAL1 refinements, but ensure developer and ITSEF together perform comprehensive security tests
  - Aim 100% testing of SFRs & external TSF interfaces
  - ITSEF witnesses/repeats 10% (min) SFR tests
  - No trivial tests repeated; aim for widest coverage
- EAL1 Limited ST unchanged to facilitate easier customer migration to EAL2
  - ITSEF & Scheme perform basic checks during Preparation
- Require developer's configuration list and SFR test docs & tools
  - To facilitate completion of thorough security tests by ITSEF
- Permit extra 5 days to assess developer test evidence & develop any new security tests (dependent on test evidence quality)
  - ITSEF completes SFR test gaps
  - ITSEF focusses on TSF interface tests
  - (Includes vulnerability analysis & penetration tests)

Proposed Limited ST Refinements

- Facilitate comprehensive security testing
  - Add Security Problem Definition
  - Add Test Approach under SARs
  - Improve TOE Description (basic architecture) – to aid testing
    - General structure & external interfaces
    - Supporting protection mechanisms (in ST Annex if proprietary)
  - State minimum s/w & h/w requirements
  - Add product provenance details
    - May influence Test Approach
- Facilitate lower production costs
  - Relax usage of CC Part 2
  - State SFRs in unambiguous, concise plain English
  - Simplify SFR labelling, but relate to I&A, audit, etc

Proposed Limited ETR Refinements

- Remove architectural description of TOE
  - Reference Limited ST TOE Description
- Remove report of evaluation methods, tools
  - Reference Limited ST Test Approach
- Reduce report of rationales supporting verdicts
  - Tests should be repeatable, reproducible
  - Report only exceptions, summarise key results
  - Reference results in Observation Reports
- Summarise conclusions & recommendations
  - Oriented to consumer not Evaluation Authority

Proposed Limited ETR Summary

- Organise Limited ETR for easy sanitisation
  - Separate annexes or referenced docs for:
  - Test specifications, any product procedure details
  - Potential vulnerabilities & observation reports
- Produce ETR Summary from Limited ETR
  - Simply by removing appropriate Annexes
- Publish ETR Summary; no Certification Report
- Archive Limited ETR in ITSEF and Scheme Evaluation Authority to assist Maintenance

Low Assurance Continuity Paradigm

- Certificates are time expired:
  - Lifetimes: EAL1: 1 year; EAL2: 2 years
  - Extendible by 1 year under maintenance
- Developer includes any additional ITSEF-developed security (Eval/Maint) tests in his test suite for ongoing regression testing
- TOE knowledge & experience resides with ITSEF

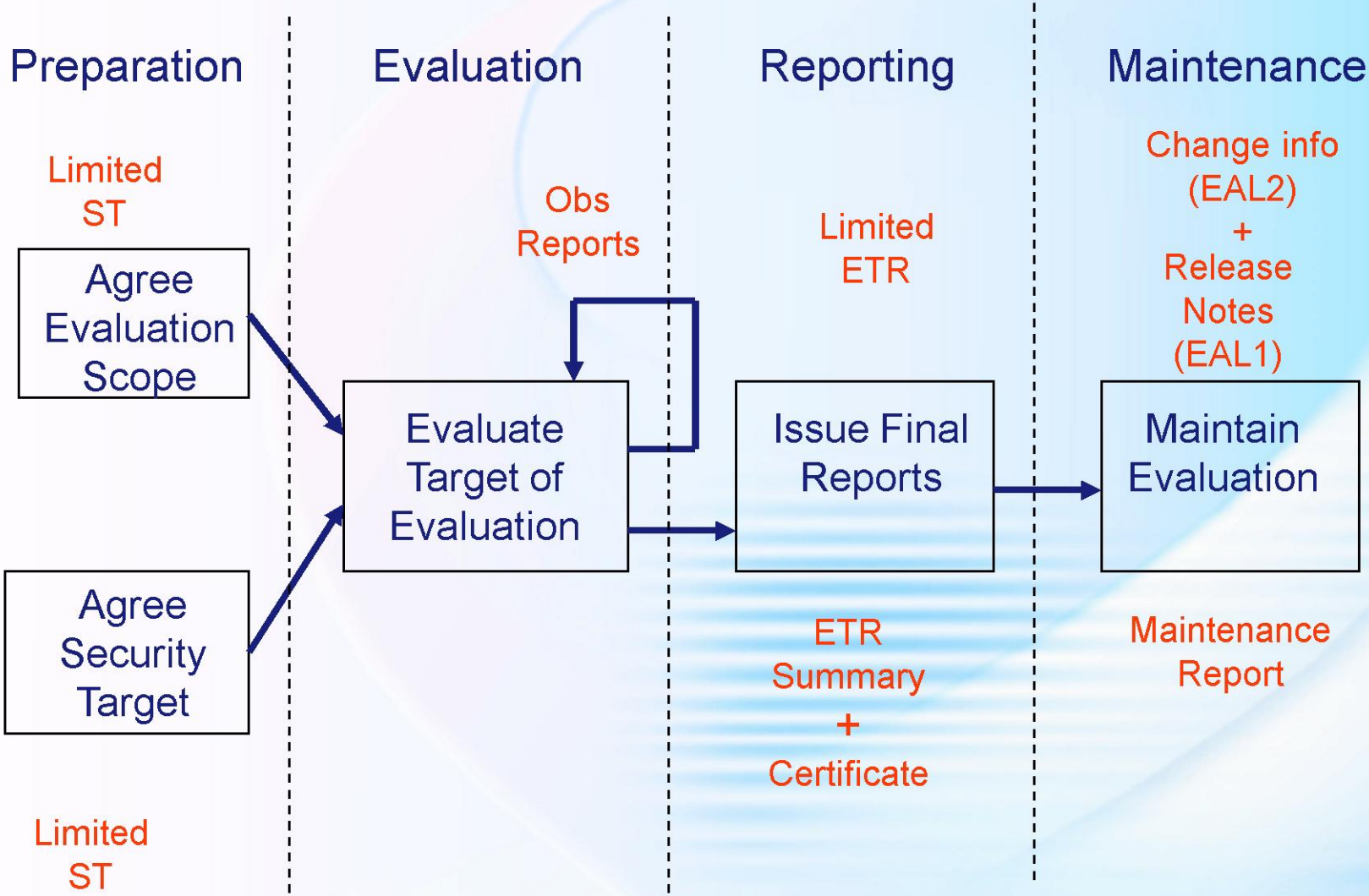
EAL1

- Any product changes are detailed in product release notes
- ITSEF assesses changes in product and product documentation & runs sample SFR tests on all platforms
- ITSEF produces Maintenance Report (10 days max)
- Scheme validates & publishes ST + Maintenance Report

EAL2

- Developer supplies:
  - Company-standard change information
  - Updated configuration list and updated SFR test docs & tools
- ITSEF also runs sample TSF interface tests on all platforms

Low Assurance Lifecycle



Questions/Comments?

http://www.cesg.gov.uk

David J Martin

Assurance Services Technical Director

email: David.Martin@cesg.gsi.gov.uk

tel: +44(0)1242 221491 ext 39297