Enisa Workshop

David Martin Head of International Assurance CESG UK

9 March 2016

Introductory Background - why should we certify?

My focus here is upon Security Certification of Products

- Can provide information and confidence in products for secure systems
- Must be comprehensive - all products in an architecture - attackers don't care
- Needs to be realistic - must not waste developers' money on false security

Must be Global

- Fragmented market means all suffer (developers' money is wasted and fewer products are available for use)
- Europe could lead in the development of global open standards
- ETSI and CEN/CENELEC already operate globally with industry

A short explanation of the reformed CCRA

- Reform instigated by directors of FR/DE/UK/US agencies
- "To **IMPROVE** security level of general IT products by building Technical Communities developing collaborative Protection Profiles ("cPPs") and supporting documents, in order to reach reasonable, comparable, reproducible and cost-effective evaluation results."
- New CCRA with collaborative Protection Profiles involves industry in their development and does not limit any activities found to be necessary
- It also aims to avoid creating/supporting any WTO 'Technical Barriers to Trade'

Not about EAL4 vs EAL2

Despite how some may like to portray it!

- New CCRA and cPPs involves industry and does not limit any assurance activities found to be necessary
- Any justifiable and controllable evaluation activity is available (in principle should support even those not yet in CC)
- Historical analysis of the subjective EAL4 approach showed it to be inadequate for modern needs (hence the directors' demand for reform)
- The new approach can demonstrably provide much higher assurance (e.g. network device improvements)
- It also helps raise standards for all developers through being open and detailed.
- Involvement of industry is crucial - the standards must be industry led to be both relevant and sustainable

It cannot be based upon finding vulnerabilities

- "In 2015, 847 critical vulnerabilities were identified by the end of September for just the 11 software products (Fig. 2) which appear most frequently in the BSI traffic light system for vulnerabilities." (The State of IT Security in Germany 2015 - BSI-LB15/504e)
- So finding, even a handful, during an evaluation makes very little real difference - standards/evaluation/certification effort is much better spent on development approaches, meaningful testing, and responses

Any European certification should:-

- Be a full part of a global regime (e.g. CCRA) - *best option*
- Or be global by means of full recognition (via CCRA or Standards/lab Accreditation Scheme etc.) with open global access to standards/operating procedures development - *less efficient*
- Promote harmonised use of global standards - which includes the detailed technology specific aspects of PPs (cannot just claim underlying CC/CEM as the 'standard' - too generic for reliability/consistency of application)
- Be based upon open and global standards development (including the operation of the evaluation/certification process (which, in practice, can be just as important as the standards themselves))
- Be truly open (WTO TBT Principles)
- Avoid fragmentation of market
- Ensure industry is fully involved in order to keep the standards relevant, up to date, and sustainable.

A Clear Danger

A ‘Europe Only’ certification approach, unless backed up with full global mutual recognition, would produce a dangerous and unsustainable barrier to trade.

The UK believes that both standardisation and certification should be global

- There can be a role for Europe to provide leadership in both elements
- But only within a global framework
- Anything limited to Europe alone risks damaging security for all

Responses to questions

Is there market demand for certification? - Does demand relate to supply?

- Users (particularly risk owners) need usable and credible product security information
  - The complexity of modern architectures (and threats) means that architects and risk owners need reliable detailed information - A certificate on its own is not enough
  - The certificate can however give confidence that state of the art testing (kept up to date by experts in a technical community) has been performed - this should increase confidence
- Users (risk owners) should lead demand for meaningful assurance NOT marketeers
- Certification should meet that demand but not fuel unrealistic marketing claims

Are the certification requirements well defined? - Key challenges

- No - we have built up an expectation (*and I hold my hands up - the UK used to promote this*) that assurance can be numerically scaled. The EAL indicates amount of work expended BUT our experience (through statistical analysis and penetration testing) shows that it does not relate to true confidence
- Product certification requirements should be defined by expert technical communities
- These should include risk owners and expert threat knowledge
- Good certification should be valuable in itself
- Not forced by regulation

How can certification support Digital Single Market?

- Meaningful certification supports cross border trust
- But the internet has no real borders and hence certification should be global
- Protectionism through a 'Europe only' approach may appear attractive in the short term but is unlikely to be sustainable
- In any case certification should help European industry thrive in a world market and so needs to be global
- Europe can, of course lead in developing standards (ETSI etc.) as long as these (and the associated certification regimes) are open and not a trade barrier.
- Global certification certainly should help European industry with world markets (sell in Europe and the rest of the world without)

Which are the top five more appealing business applications for certification?

- More of a question for industry/users
- UK Government needs are for security product certifications that are:-
  - Realistic
  - Agile (change as quickly as threats and products do)
  - Global so that market is not artificially limited and industry is able to compete globally
- Possible application areas:-
  - Mobility
  - Networking and secure data in transit
  - Data at rest encryption
  - Applications (in a meaningful way)
  - Identity