

# How much is my certification really worth?

Keeping standards relevant in a changing world.



Graham Costa and Will Tung, Gemalto  
May 19, 2016

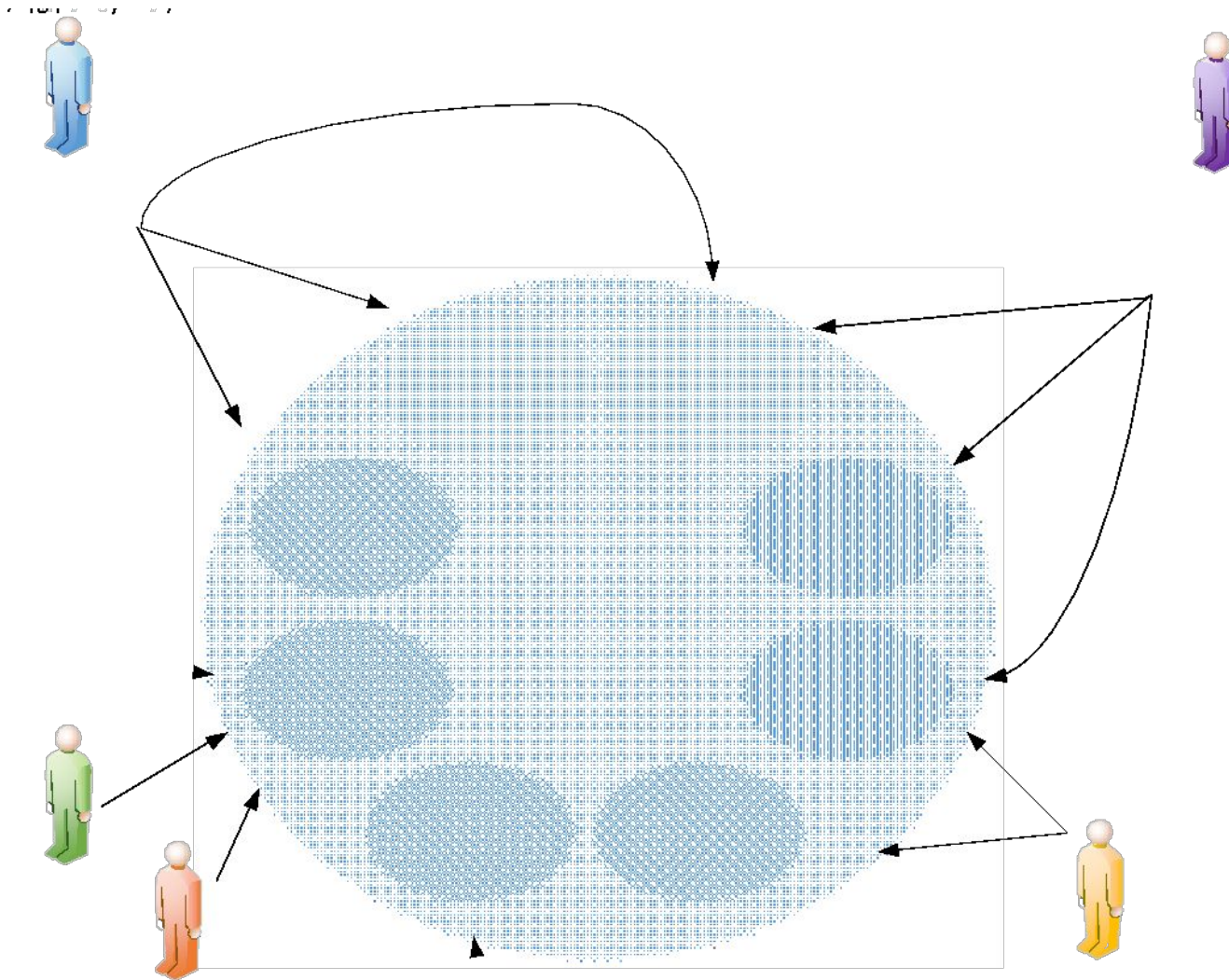
# Section 1: Who values what?

Linking value to assurance

## Why do we have certifications?

- To provide independent, 3<sup>rd</sup> party verification and assurance of vendor claims.
- To provide a baseline security bar for products to meet.
- Protect markets against inferior products with 'Snake Oil' security claims.
- Gives vendors a route to avoid repeatedly re-asserting and justifying their security claims to potential customers.
- Allows shift of liability in some regulated markets where end-user is freed of some obligations if using 'certified solutions'.

# Who values security certifications?



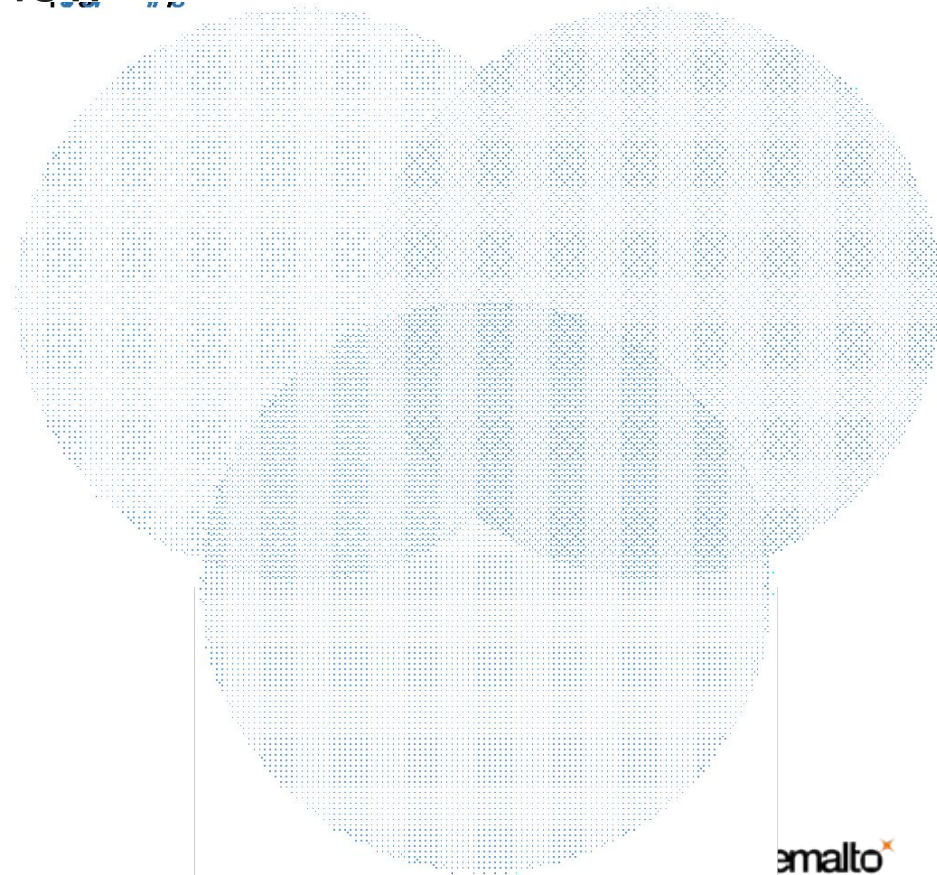
# What does assurance mean?

*Definition: “a positive declaration intended to give confidence.”*

Source: The Chambers Dictionary, 12<sup>th</sup> Edition.

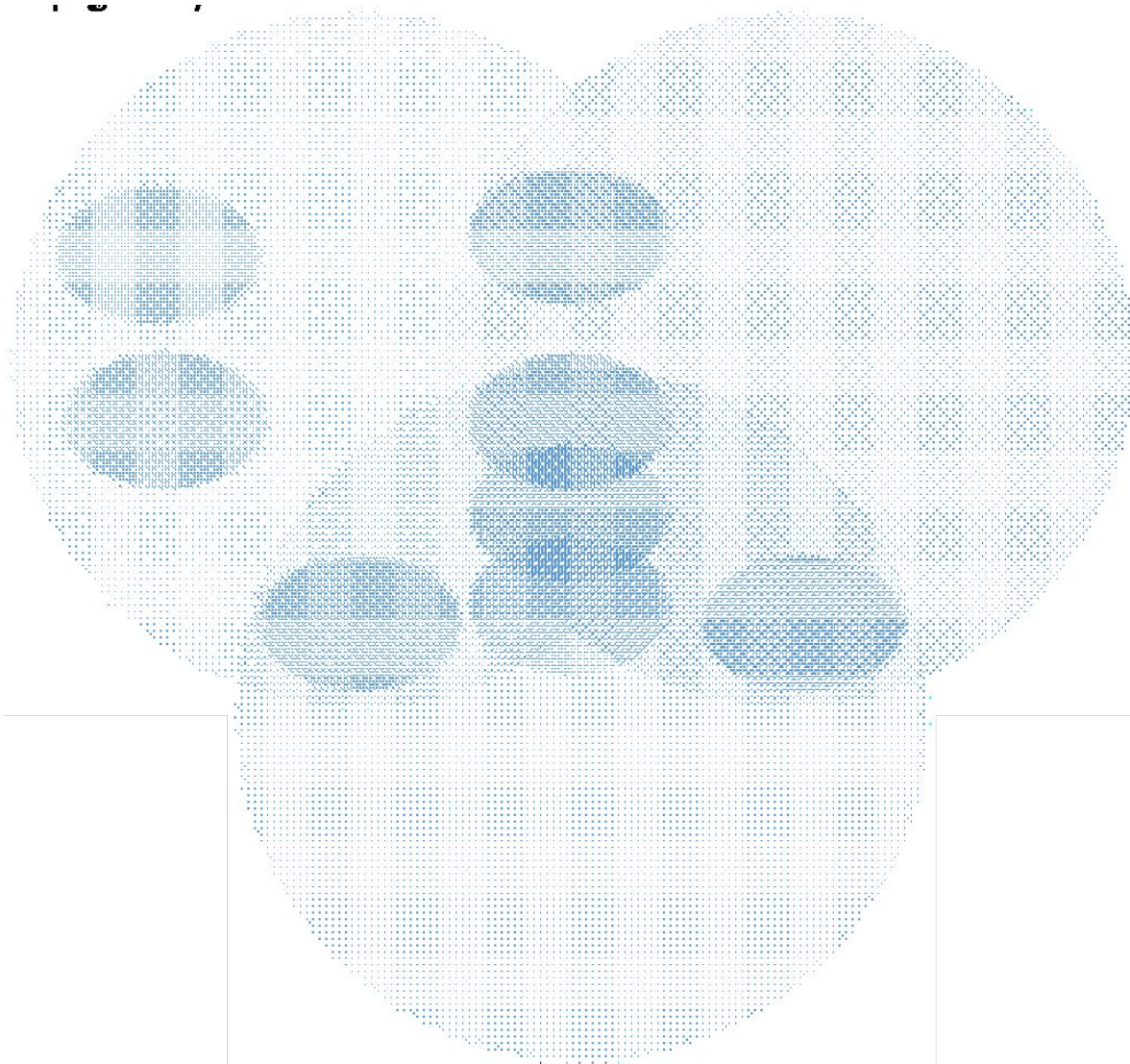
# What activities do we use to generate assurance?

- Compliance Testing
- Design Review
- Code Review
- Development Process Review
- Site Security Review
- Manufacturing Security
- Vulnerability Search
- Side Channel Analysis





# Mapping needs back to assurance activities?












## Typical problems that impact value?

- Overlaps in independent testing between different standards where products need multiple certifications.
- Compliance testers do not understand the product sufficiently or have time to find real problems.
- Square peg in a round hole situations:
  - Scope gets set too tight to be of real-world use to end-users.
  - Security certifications stops products from meeting their real-world use cases.
- Inconsistencies in labs, schemes and/or the review process undermines a consistent view on value.



# Quantitifying the value of assurance

- It's very difficult to make a quantitative assessment of the value of assurance.
- A qualitative assessment helps us to understand the balance of opportunity vs. costs - some examples:
  - **To Vendor:**
    -  profit in certification related sales
    -  time saved explaining product security claims
    -  cost of certification focused changes
    -  cost of test lab to perform certification
  - **To End-User:**
    -  savings from reducing need for internal testing
    -  value of reduced security risks
    -  savings from simplified compliance to industry guidelines
    -  cost of management overhead associated with maintaining certified configuration
    -  cost premium of buying certified equipment

## Section 2: How are standards developed and what can go wrong?

# How do groups develop standards?

- Open Developments

- Anyone can join group and contribute proposals for changes to the standard.
- Decisions on standards made by voting which can be by organization, country or contributor.
- Depending on the standards body, minimum/maximum windows for standards refresh may be mandated.

- Closed Developments

- Typically run by Government organization or industry body.
- Optionally include contributions from end-users and industry but more commonly developed in closed forum.
- Decisions on standard made by sponsoring organization or body.

- Hybrid Developments

- Closed groups that set themselves up to leverage open standards but look to define an overlay on the original standard.

# What's changing in the certifications landscape?

- Internet age is bringing down the cost of contributing to standards by allowing cheaper ways to collaborate.
- End-user is increasingly security savvy and interested in what a certified product gives him.
- Easier access to information on vulnerabilities is helping to raise awareness of insecurities in certified product.
- Re-use of 'certified components' is becoming common as a path to reducing certification costs.

# What can go wrong with certification standards?

- Scope becomes too narrow.
  - mismatch between standards and how target technology works and is used.
- Too expensive and too long an investment.
- Too static, too averse to change or too slow to evolve.
- Too complicated – either too difficult for labs to test based on existing skills base or too difficult for labs to test consistently.
- Requirements creep and changes to the standards.



## Section 3: Changing how we approach assurance

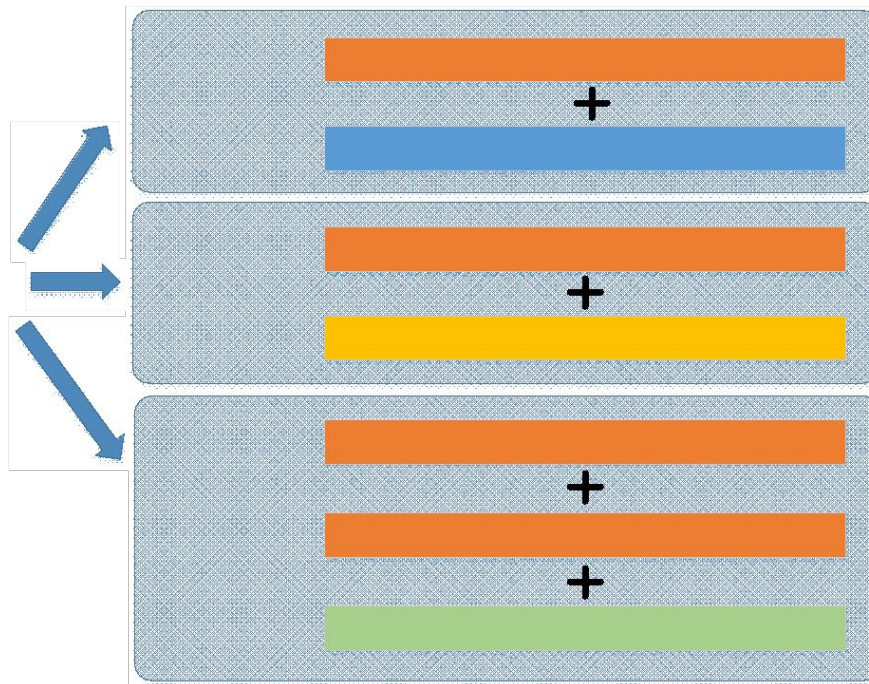
Established Changes and New Ideas....

# Established Changes

- There have been a lot of positive developments in the certification landscape recently:
  - **Development of new ‘technical communities’ to help evolve and shape standards.**
    - not a new idea but one revisited.
    - critical to keeping standards grounded in the needs of the end-user and technologies they serve.
  - **Re-use of open standards as part of hybrid developments as an alternative closed standards.**
    - positive step in increasing re-use of our certifications or certification artefacts across markets.
    - open standards often benefit from a wider set of inputs helping to maintain balance.
  - **Introduction of more requirements focused on the ‘secure development lifecycle (SDLC)’.**
    - extends assurance to ‘how a product was developed’ rather than just the traditional ‘what it does’.
    - focuses more on the ‘root cause’ of most security problems.
    - helps to justify expense of SDLC in large organizations not focused on security.

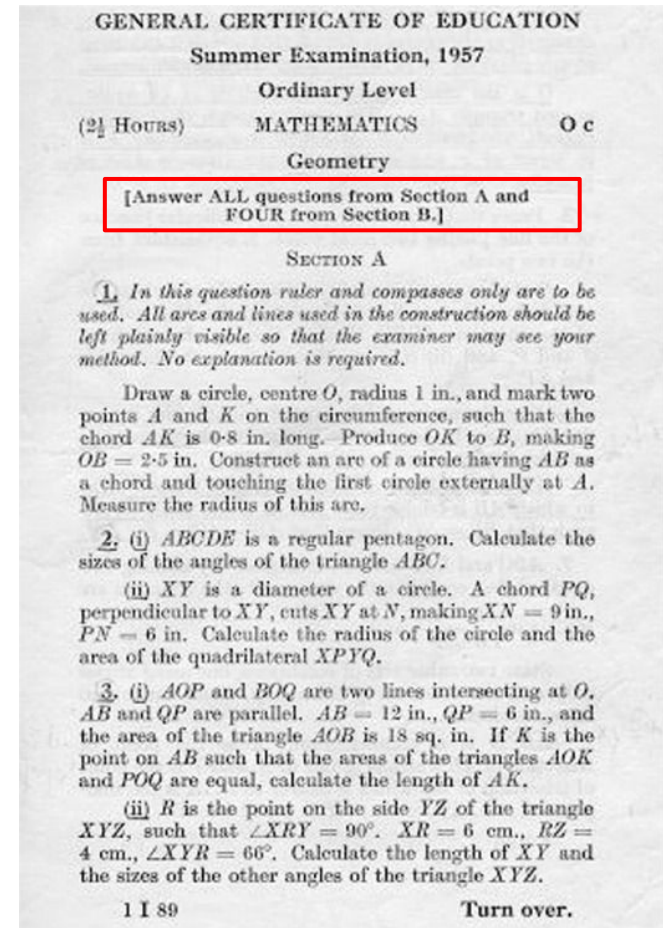
# Flexible Testing – allowing multiple paths to assurance?

- Inconsistencies in certification results can come from mis-matches in assurance activities to either the product, testing lab or tester:
  - not all paths to assurance are equally suitable to all products.
  - not all labs have the same mix of specialists leading to variations in quality.
- Flexible testing looks to give the tester multiple paths to choose from looking to identify the best fit testing plan.



# Why not introduce some entropy?

- Why do we need to test every, or always the same requirements with every certification?
- Conjecture: we don't!
- Cutting down on tested requirements is an established route to slimming certifications but could go wrong.
- Randomizing and doing sampled testing as an alternative:
  - avoids the ability to predict or choose what will be tested
  - allows depth of testing in selected areas to be maintained
  - would seem like a quick-win?



# Using Feedback (1)

- Why don't certifications schemes or testing labs ask for feedback?
- It's not a new idea and is one that's been penned about for millennia...

*"Study the past, if you would divine the future."*

Confucius, 551 BC – 471 BC, Chinese Philosopher.

*"Life is divided into three terms - that which was, which is, and which will be. Let us learn from the past to profit by the present, and from the present, to live better in the future."*

William Wordsworth, 1770-1850, English Romantic.

*"We must respect the past, and mistrust the present, if we wish to provide for the safety of the future."*

Joseph Joubert, 1754 – 1824, French Novelist.



## Using Feedback (2)

- Feedback shouldn't be confused with 'review'.
- Ample and easy opportunities for feedback:
  - Feedback forms for vendor and test-lab on completion of an evaluation?
  - Targeted feedback from lab and vendors on abnormally long, stalled or abandoned certifications?

**Feedback Form – Super Security Certification 'X'**

How would you rate your experience of this certification?

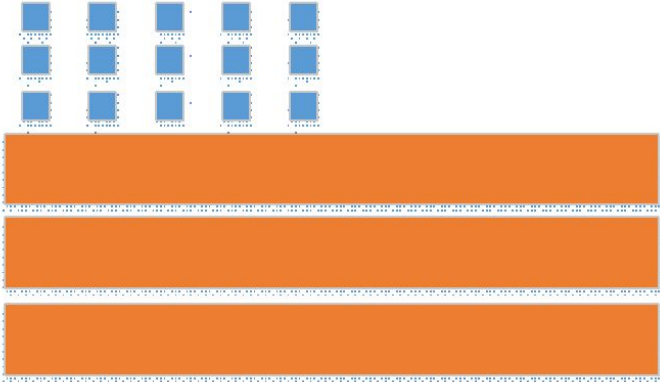
How would you rate the clarity of our requirements?

How would you rate the supporting information?

Why do you use this certification scheme?

Have you encountered any problems you'd like to share?

Can you suggest any improvements to the scheme?



## Better managing conflicts of interest (1)

- Certifications inherently involve conflicts of interest that can skew standards or hold them back from developing.
- Examples:
  - Vendors want to 'Monetize Security' but don't want to increase the costs of development.
  - End-users want to maximize the value of their investment in certified product but don't want to pay a premium for it.
  - Test equipment and specialist test software vendors only want to create an increased opportunity to sell their specialist equipment.

## Better managing conflicts of interest (2)

- Paths to managing conflict and maintaining balance:
  - Decisions relating to changes to standards should be transparent and directly linked to a rationale.
  - Open proposals for changes should be able to be put forward but should only be considered when a balanced groups of stakeholder are involved.
  - Standards groups need to be able to show that they are pro-active in reaching out to canvas for inputs from a range of stakeholders alongside representatives from different technology classes.

# Maintaining a Standards Balance Sheet

- Security certifications like it or not are a business and are either making, saving or losing money for someone.
- Typically the health of a business is assessed based on its balance sheet - why not try this for a standard?
  - tracks where the value in a standard is coming from and for which stakeholders.
  - identifies the cost of assurance and who it's being met by.
  - allows an assessment of whether the net value of a standard is positive or negative.
- Easier to do in a 'qualitative' rather than a 'quantitative' way.
- This is an idea in its infancy that can be expanded in the future.

## Section 4: Summary and Conclusion



## Looking forward – Final thoughts...

- Value proposition of standards isn't a simple thing and means different things to different people.
- We've discussed a number of good developments in certifications alongside some new ideas that will help address problems identified.
- “*Certification Monetization*” as a phrase is one to keep hold off – if it loses its value, it will lose its relevance in an evolving world.
- We shouldn't be short of ideas when it comes to trying to keep our current standards relevant ahead of creating new ones.

Thank you and Questions?