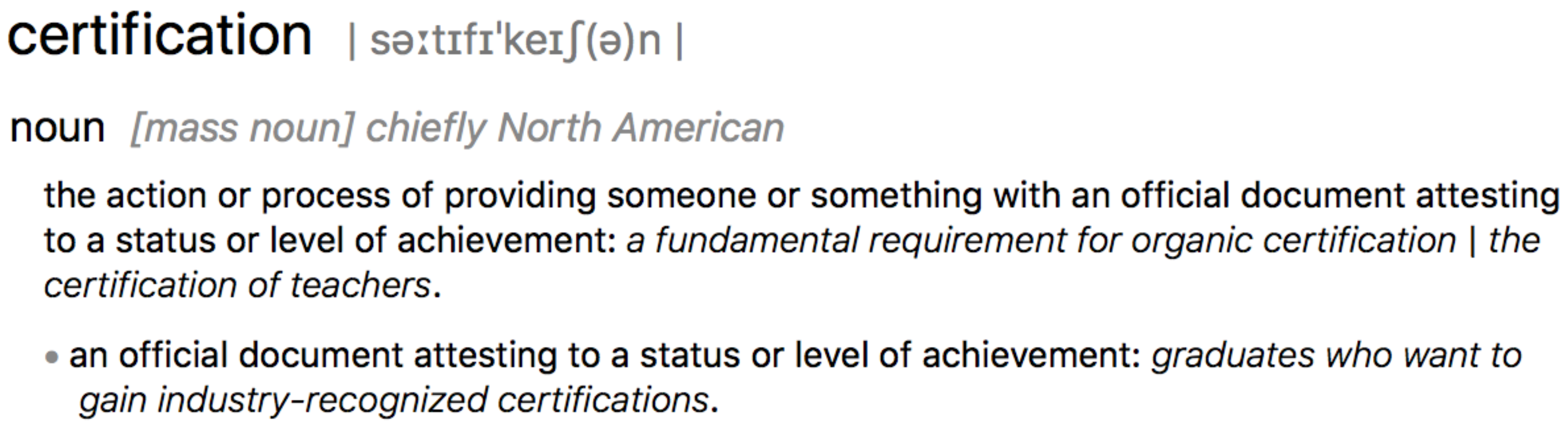
Does certification engender trust?

Scott W Cadzow

Affiliations:
C3L,
ETSI Expert and Rapporteur,
StandICT.EU Expert Advisory Group

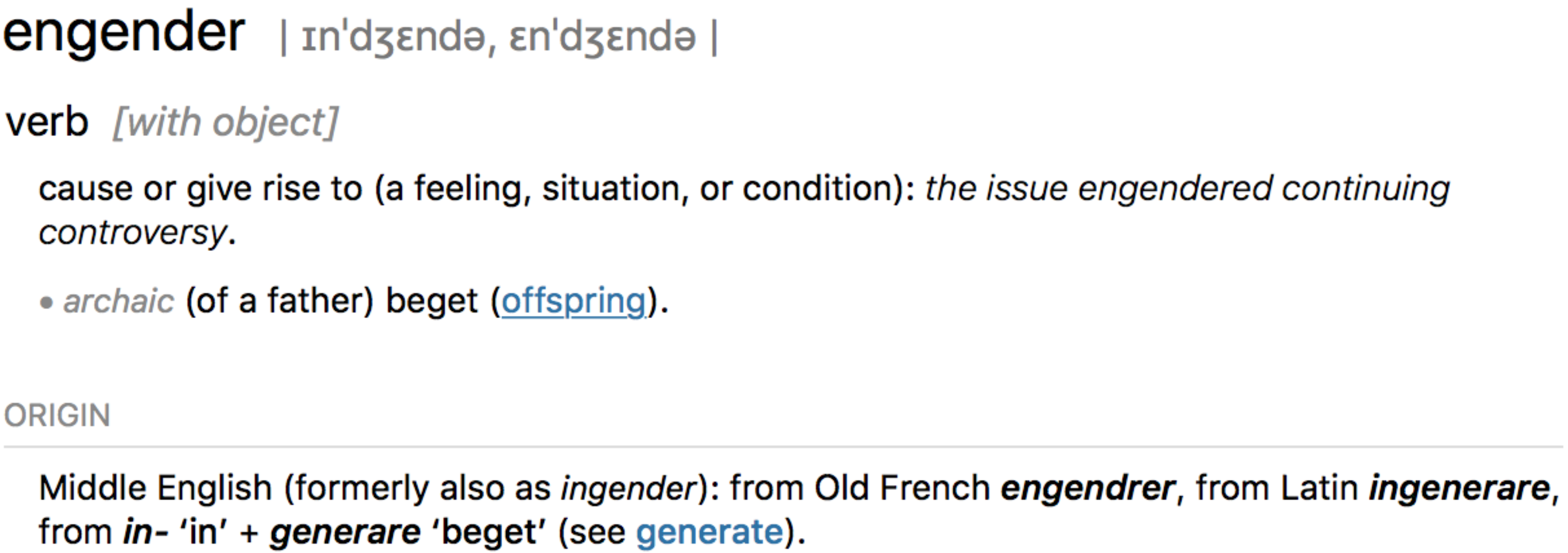


certification | səːtɪfɪˈkeɪʃ(ə)n |

noun *[mass noun] chiefly North American*

the action or process of providing someone or something with an official document attesting to a status or level of achievement: *a fundamental requirement for organic certification* | *the certification of teachers*.

- an official document attesting to a status or level of achievement: *graduates who want to gain industry-recognized certifications*.



engender | ɪnˈdʒɛndə, ɛnˈdʒɛndə |

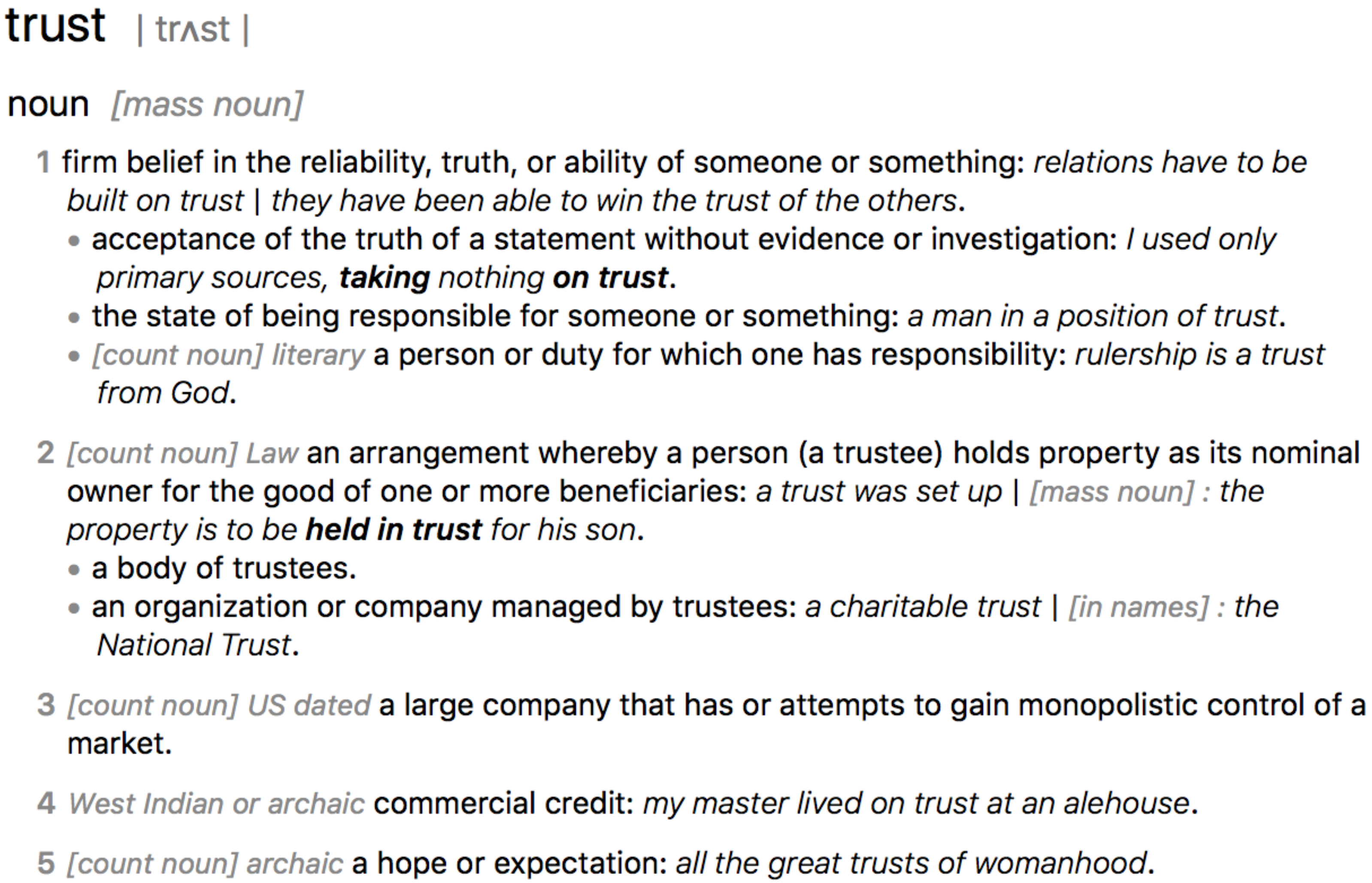
verb *[with object]*

cause or give rise to (a feeling, situation, or condition): *the issue engendered continuing controversy*.

- *archaic* (of a father) beget (offspring).

ORIGIN

Middle English (formerly also as *ingender*): from Old French ***engendrer***, from Latin ***ingenerare***, from ***in-*** ‘in’ + ***generare*** ‘beget’ (see generate).



trust | trʌst |

noun *[mass noun]*

1 firm belief in the reliability, truth, or ability of someone or something: *relations have to be built on trust | they have been able to win the trust of the others*.

- acceptance of the truth of a statement without evidence or investigation: *I used only primary sources,* ***taking*** *nothing* ***on trust***.
- the state of being responsible for someone or something: *a man in a position of trust*.
- *[count noun] literary* a person or duty for which one has responsibility: *rulership is a trust from God*.

2 *[count noun] Law* an arrangement whereby a person (a trustee) holds property as its nominal owner for the good of one or more beneficiaries: *a trust was set up | [mass noun] : the property is to be* ***held in trust*** *for his son*.

- a body of trustees.
- an organization or company managed by trustees: *a charitable trust | [in names] : the National Trust*.

3 *[count noun] US dated* a large company that has or attempts to gain monopolistic control of a market.

4 *West Indian or archaic* commercial credit: *my master lived on trust at an alehouse*.

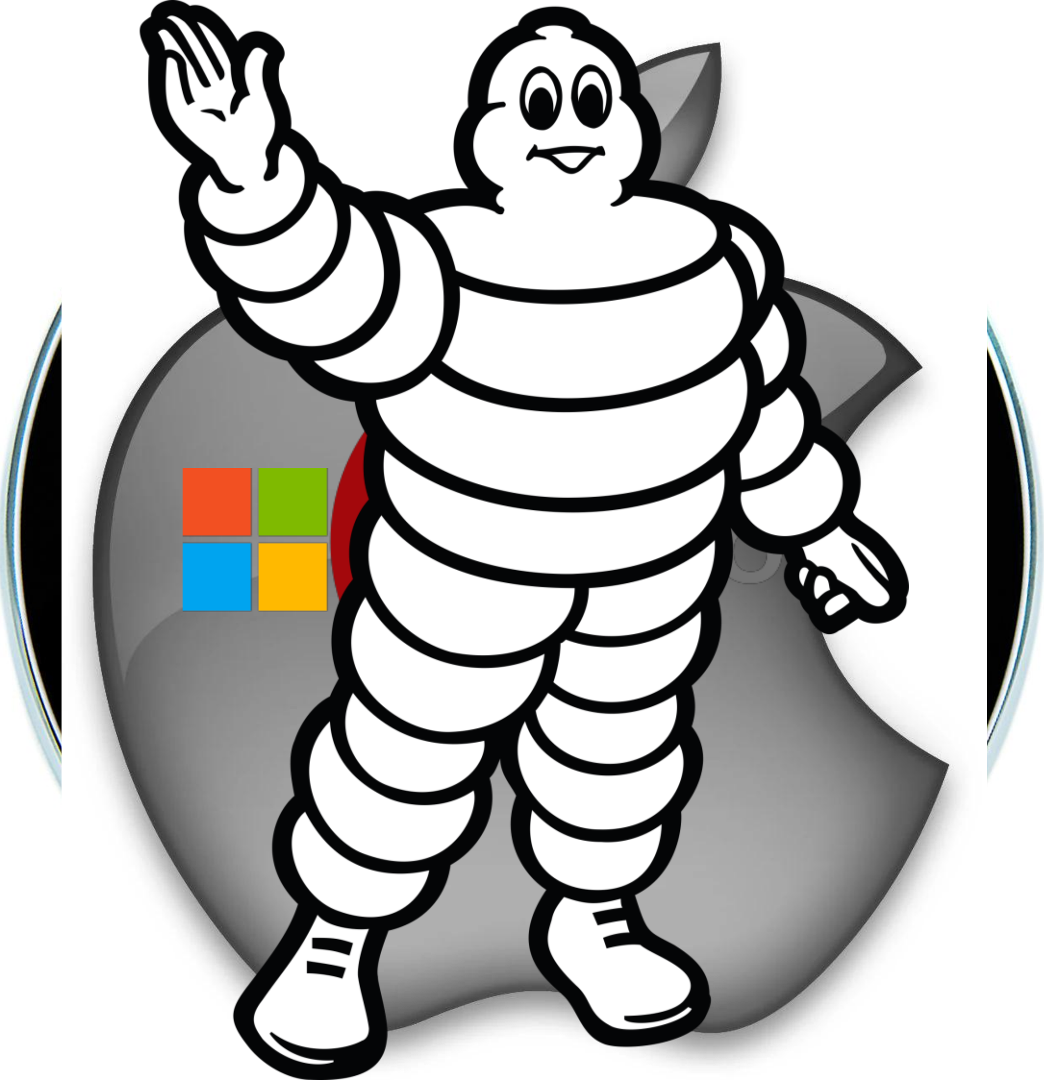
5 *[count noun] archaic* a hope or expectation: *all the great trusts of womanhood*.

Certification and trust in ICT security

- Cryptographic trust demonstrates faith in mathematics
    - Actions using a key equate trust with the key management capability of the key holder (e.g. the secret part of an asymmetric key is really secret, a symmetric shared key is only held by the communicating parties)
- Requires clear binding of attestation to claim
    - Public key certificate in asymmetric cryptography binds public key and associated private key to an attribute with the claim upheld by a trusted third party (the Certification Authority)
- The modern era
    - Proof of security of device, process or system – much greater than attestation of a single attribute

What determines trust?

- Reputation
  - Takes time to build
  - Is somewhat contextual (trust in context *A* does not imply trust in context *B*)
- Community
  - How Alice trusts an entity may encourage others (the Bobs) to trust an entity
- Responsiveness
- Trust does not equate to quality/safety/security



Where does security fit in a brand?

- Most end-products rely upon a [long] supply chain
  - Supply chain integrity is important to ensure a good end product
  - Vendor assessment is an integral part of supply chain management
    - Addressed in ISO-9000, ISO-27000 and ISO-14000 amongst other management standards
- Some ICT products have disturbed supply chains
  - Computer hardware and software have independent supply chains
    - If Windows™ crashes is the hardware, a driver, an application responsible?
- Who owns and has responsibility for the final security solution?

Does brand engender trust?

- Everything has faults
  - The impact of those faults determines the risk if those faults are exploited or made real
- Brand value is impacted by how the brand responds to faults
  - Fast response and fix improves brand status
- A brand becomes a certificate of quality
  - All part of a brand’s offering impacts the value of the brand
- Security performance in ICT will be part of the brand
  - Part of the “brand” certificate

Certification and trust issues

- Certificate has to come from a trusted entity
- The CA has to have a stake in the product to be part of the trust equation
    - This is how we deal with trust in human relationships, the guarantor of trust may lose out if the endorsement/endorsee is shown to be at fault
    - This is not the common model of PKI like trust
- Static certificates and labels of security function are not valid for dynamic environments
    - All security functions exist in dynamic environments

Modes of certification

- Self asserted, self generated label or certificate
  - Trust is determined not by the label or certificate but by the brand reputation
- 3rd party label or certificate
  - Level of trust is determined by reputation of both the brand and the tester/evaluator
  - Scope of trust is independent of content of label or certificate

Conclusion for debate

- Labelling or certification of security is of restricted and contextual value
  - Label/certificate has to be clear about any caveats (e.g. specific context, specific attacks, specific time taken to test)
- Trust in the vendor is not impacted by a label or certificate
  - If the label or certificate is not displayed/available the brand will succeed or fail based on how the vendor/brand reacts to issues (proactive vs reactive, leader vs follower, risk averse vs risk tolerant)