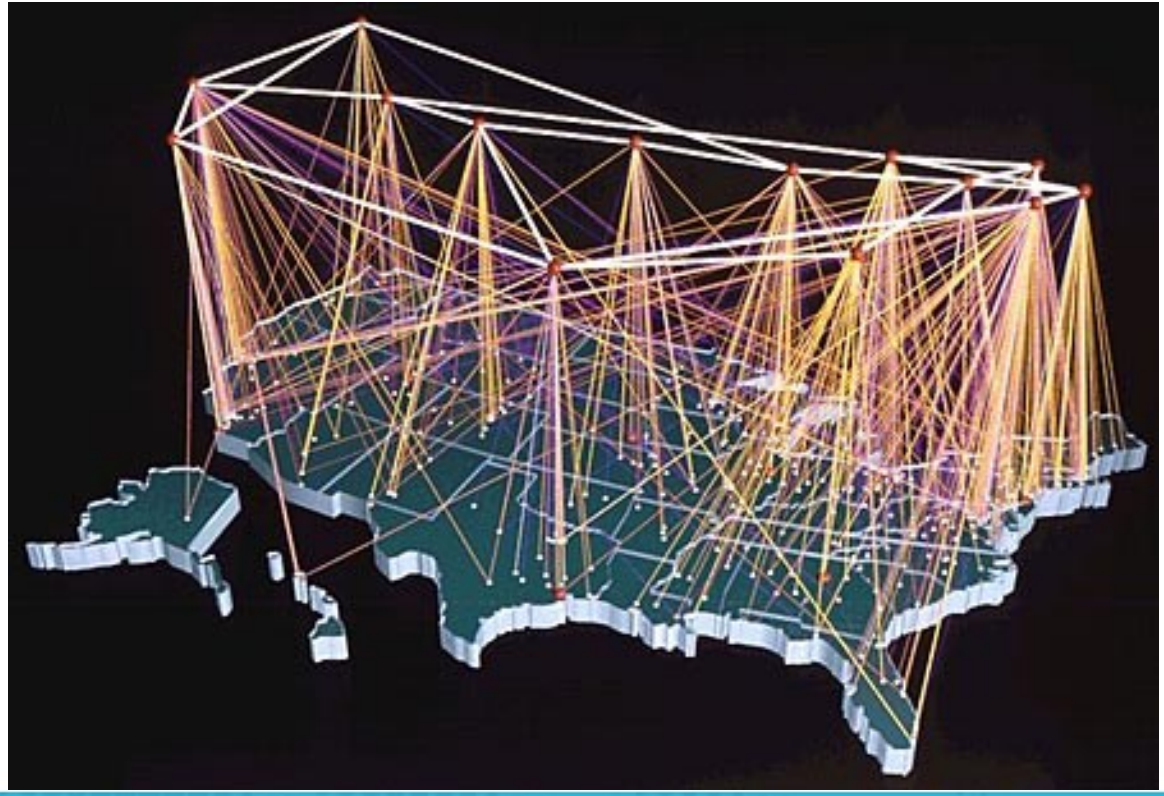


Trust and the Smart Grid

John Zic
CSIRO ICT Centre
Australia

Kerberos Conference 2010

www.csiro.au

What is CSIRO?

Australia's national science agency

One of the largest & most diverse in the world

6500+ staff over 55 locations

Ranked in top 1% in 14 research fields

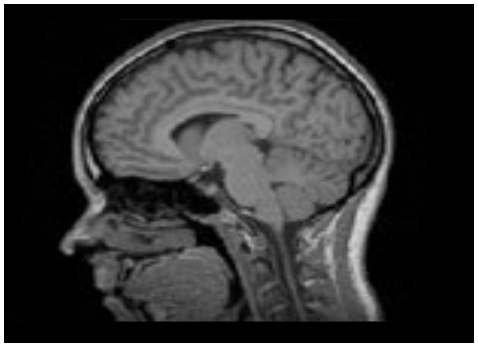
20+ spin-off companies in six years

160+ active licences of CSIRO innovation

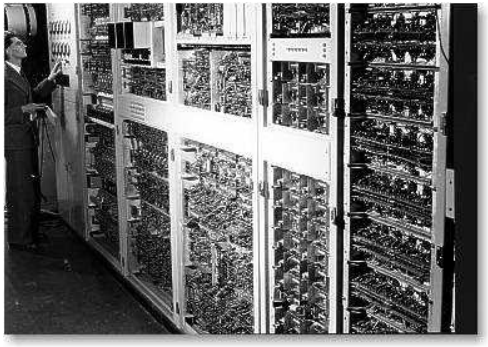
Building national prosperity and wellbeing

Australia's most trusted research organisation

Some Achievements



Brain Atlas -- Alzheimer's



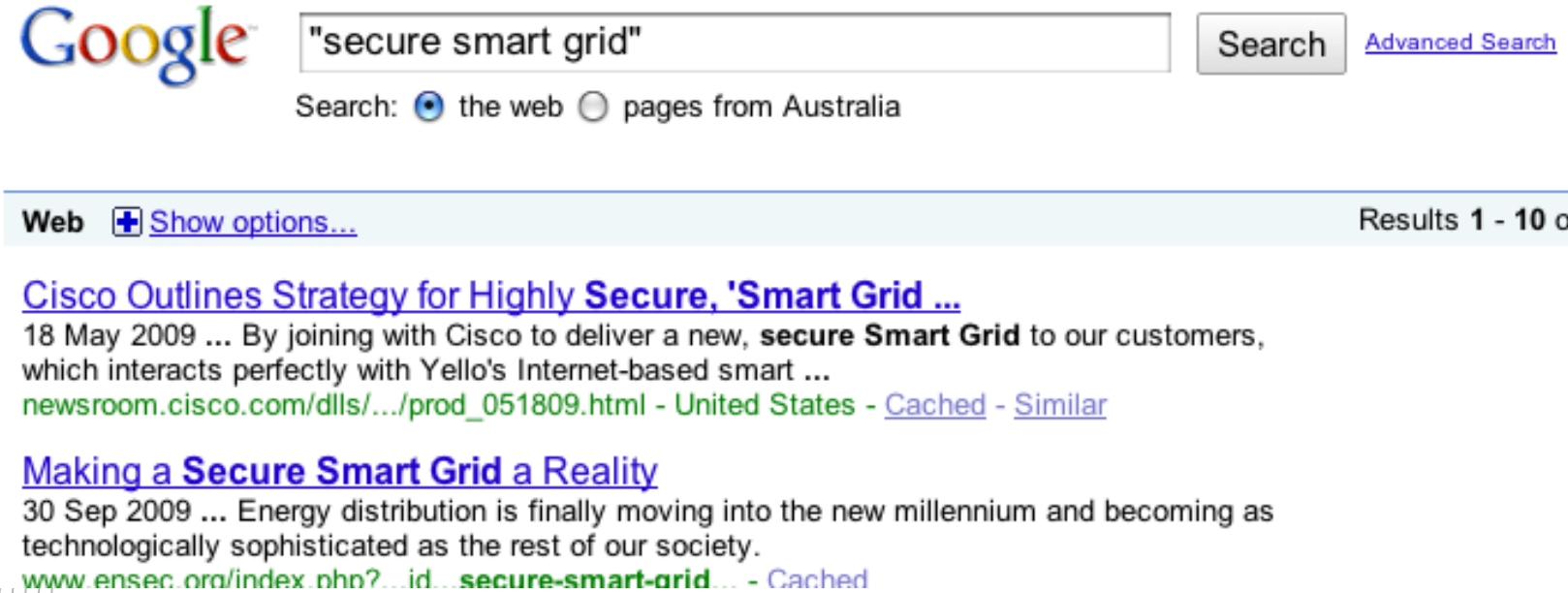
World's 5th Computer

Hi Res Imaging of Centaurus A

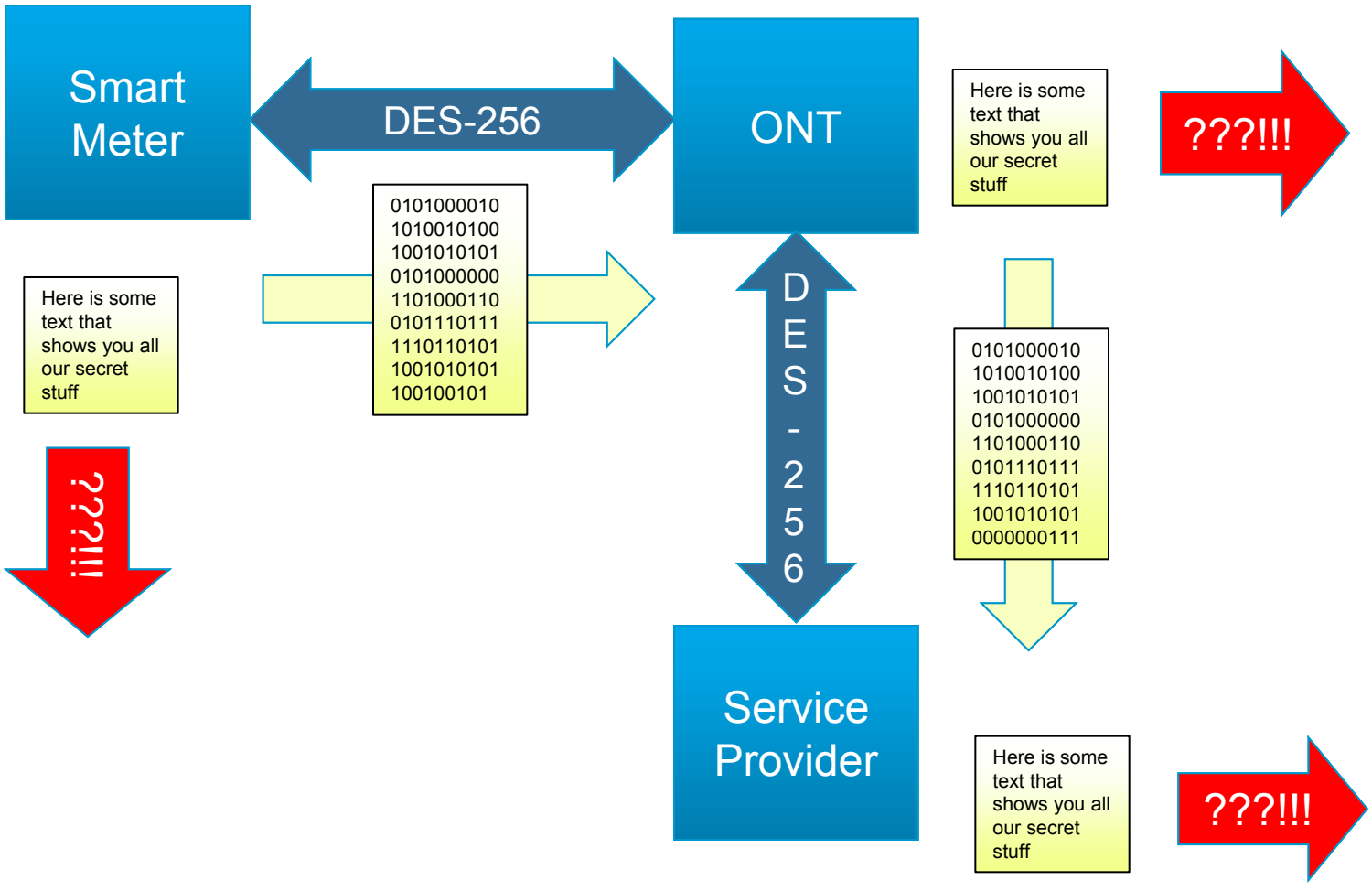
The Dish

Early Radar (1939-)

Security vs Trust



Why *identity* and *security* are not enough

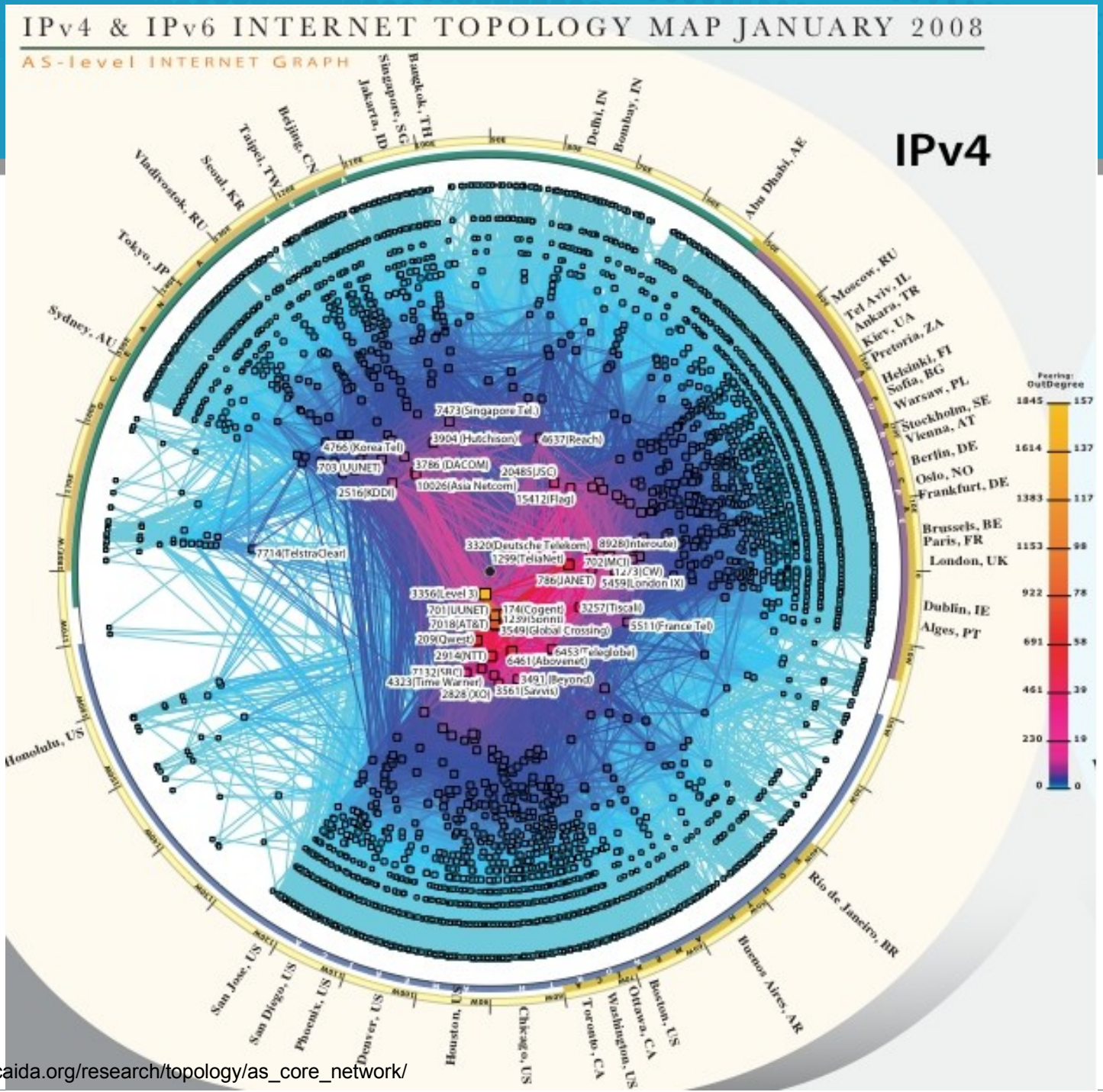


Observation

“It’s worth observing that trust doesn’t always scale well. We can establish trust among a small group of people known to us, but it’s harder to achieve trusting relationships on a larger scale.”

Vint G. Cerf, *Trust and the Internet*

IEEE Internet Computing, Sept/Oct 2010, pp 95-96.



http://www.caida.org/research/topology/as_core_network/

A question of identity and behaviour
The Internet Dog

"On the Internet, nobody knows you're a dog"

Let alone *breed* …

or *temperament* …

Peter Steiner, The New Yorker Vol.69 (LXIX) no. 20, July 5, 1993 p61

Trust is about identity & behaviour

- **Identity**
  - “No body knows who you are”
  - Multiple identities
- **Behaviour**
  - “No body knows that you are a quiet, pure bred Border Collie who loves rounding up sheep, children or any other herd”
  - Multiple behaviours
    - disposition, time of day
  - Multiple identities *may* be linked to different behaviours
- **Tied to *control of information***

Trust from the systems viewpoint

Something can be *trusted* when

- **It can be unambiguously identified**
- **It operates unhindered**
- **The user has either:**
  - First hand experience of consistent good behaviour

or

  - Someone who can vouch for consistent good behaviour.

Graham Proudler, HP Labs Bristol

See also IETF RFC4949 *Internet Security Glossary, Version 2*

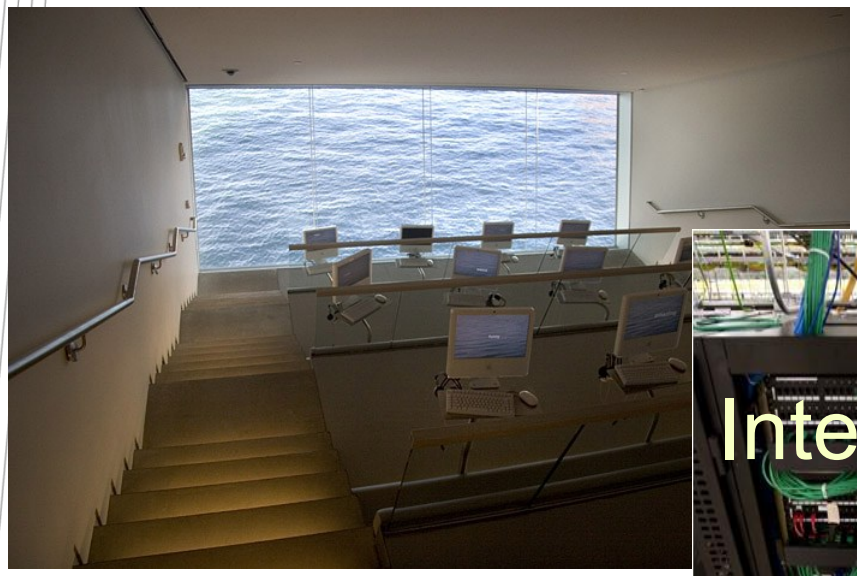
CSIRO

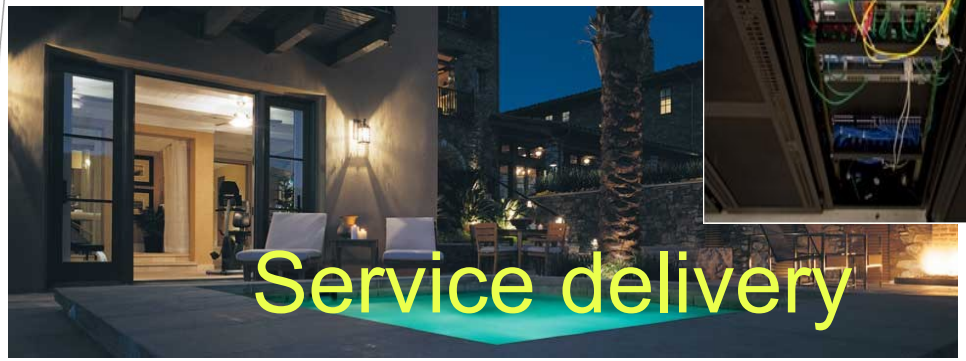
Trust from the systems viewpoint

- **A Trusted System behaves *exactly* as specified and no more, despite**
  - Disruptions by environmental factors
  - Errors cause by human or automated interaction, or
  - Hostile attacks on the system.

- **How do we build systems that we can demonstrate, at all times, that it is to be trusted?**
  - i.e. *trustworthy?*

Observations about Smart Grid systems





Service: http://www.eliteorg.com/lighting-lanscapelighting.html;
http://gregcookland.com/journal/uploaded_images/picICAFlickrSulloA-730717.jpg
Network: http://www.singlehop.com/data_center_photos/zoom/zIMG_7720.jpg
Physical: http://farm4.static.flickr.com/3640/3589862983_2db90ecf24_b.jpg;
http://www.nsf.gov/news/mmg/media/images/wind_turbine_h.jpg

CSIRO

At AusCERT09

Steven Bellovin asked some directed questions:

1. ***How are (electrical service) providers' sites protected?***

1. ***Prove to me that someone***
   - *Can't poll a thermostat in my house to see if I'm away on vacation?*
   - *Or turn my thermostat off when I go away in winter and let my pipes freeze.*

Bellovin: "*Talk about overflow attacks.*"

CSIRO

PWN

OED – *Welsh*
To break down and crush by beating, with or as with a pestle; to reduce to a pulp or powder; to pulverize.

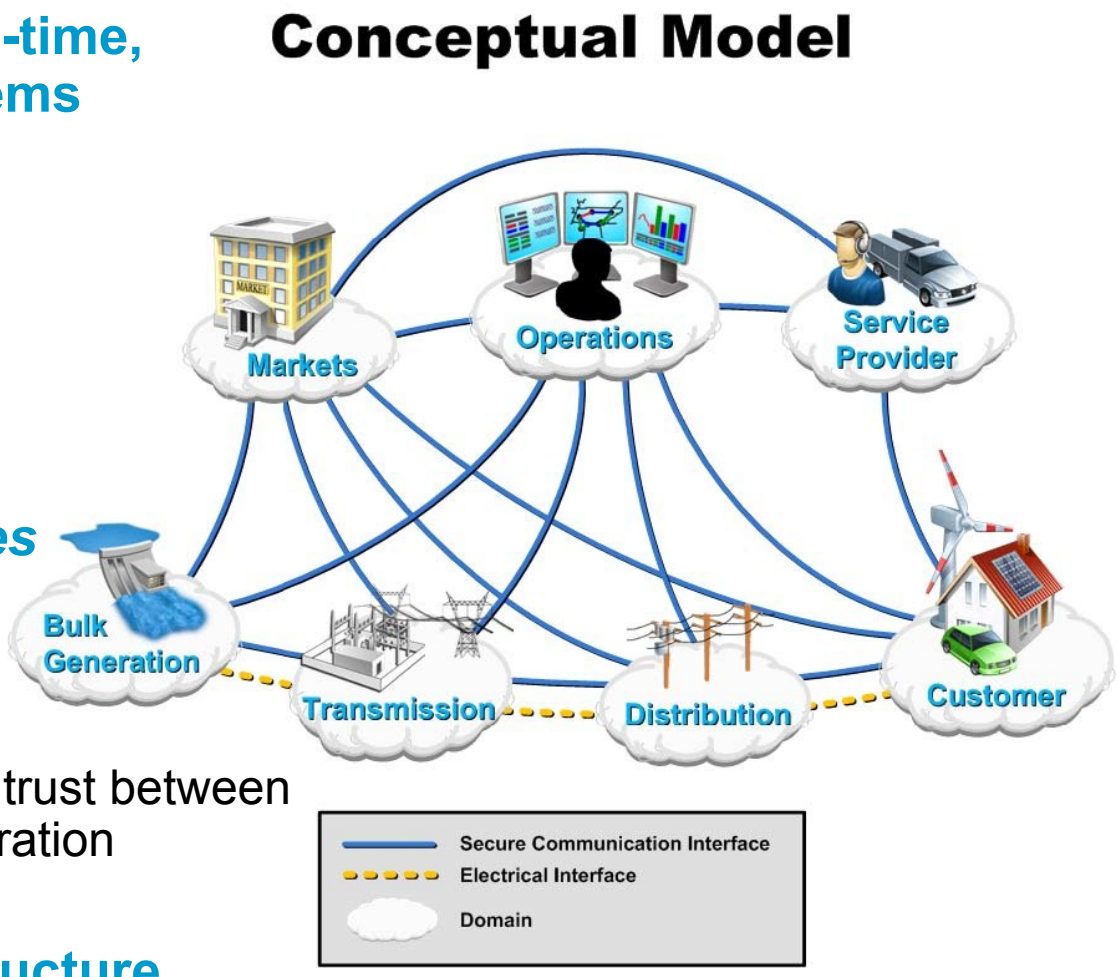
Wikipedia -- *hacker jargon*
pwn means to compromise or control, specifically another computer (server or PC), web site, gateway device, or application.

Photos redacted for publication

CSIRO

Observations about Smart Grid systems

- **Very large scale, real-time, heterogeneous systems**
  - Entities
    - Types
    - Instances
  - Geographical extent
  - "Fragility"
- ***Collaborative services* environment**
  - Interoperation
  - Control
  - Privacy, security and trust between entities in the collaboration
- **Largely fixed infrastructure**
  - Mobile nodes coming…



Smart grid conceptual model – top level
(EPRI report to NIST, 2009)

So…what's the problem?

"Put simply:

The problem with smart computers is that computers aren't smart.

The problem with smart grids is that they depend on smart computers."

Fred Cohen, California Sciences Institute

IEEE Security and Privacy Jan/Feb 2010, "On the horizon"

editors O. Sami Saydjari & Vijay Varadharajan, pp 60-63

+ The problem with smart grid systems is that they *include humans*

Electric Power Research Institute (EPRI) Identified Vunerabilities

Threat Categorys	Number of Vulnerabilities
People, procedure and policy	15
Platform (physical)	47
Network (transfer of information)	20
TOTAL	**82**

"Report to NIST on the Smart Grid Interoperability Standards Roadmap", June 2009

Just a minute …

"… there are known knowns. There are things we know that we know.

There are known unknowns. That is to say there are things that we now know we don't know.

But there are also unknown unknowns. There are things we do not know we don't know."

http://en.wikiquote.org/wiki/Donald_Rumsfeld -- sourced 23/09/09

Australian Government Attorney-General's

Cyber-security strategy document (2009) key priority areas

- Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest.

- Partner with business to promote security and resilience in infrastructure, networks, products and services.

- Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions

(Strategic Priorities, p vii)

Putting *trust* into the smart grid

Three pronged approach

1. "Good behaviour" agreements between entities

- Establish rigorous, enforceable agreements between key entities in the system ahead of ANY deployment
- *Minimal* default assumptions

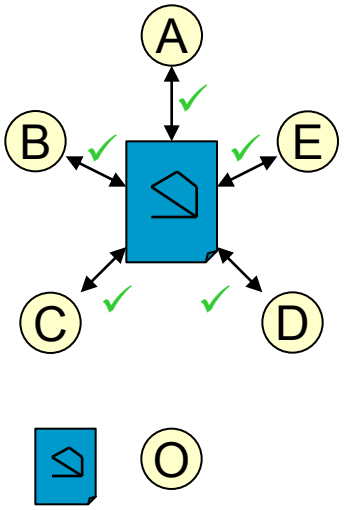
2. Proof of adherence to agreement between participants

- Mathematically rigorous proof of behaviour between entities while deployed collaboration is active
- Static check

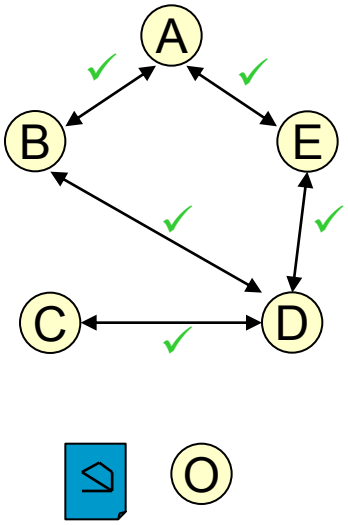
3. External verification of agreed behaviours

- During and at termination of collaboration
- Dynamic check

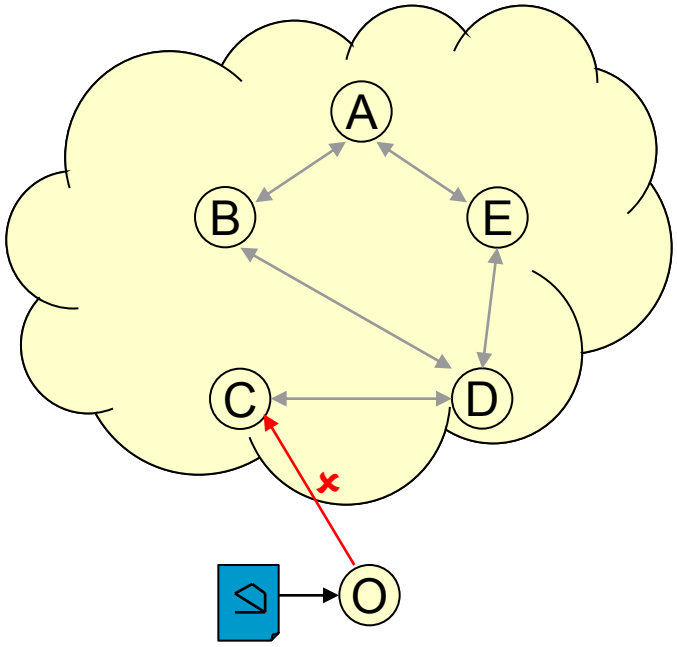
CSIRO



1. Agreement upon policies for sharing information



2. Rigorous proof of behaviour between participants



3. Ensuring externally verifiable behaviours

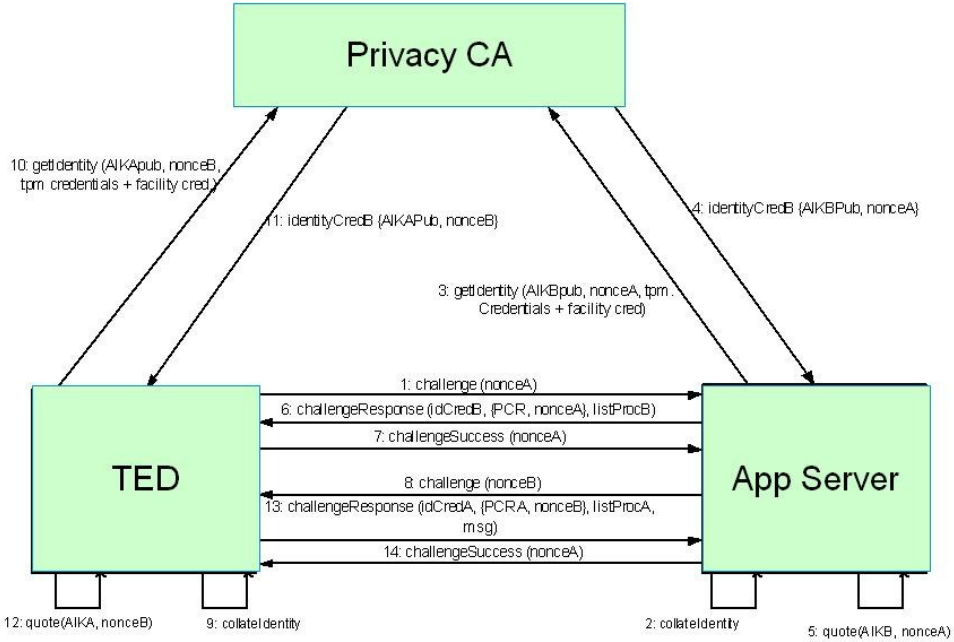
Agreement

- **There are a variety of electronic contract (eContract) systems each with their own:**
  - Semantic definitions
  - Negotiation, agreement, monitoring and termination protocols
- **Each contract typically contains**
  - Identity information
  - Role information
  - Access policies to resources
    - Internal
    - External
  - Collaboration duration
  - Collaboration participants

Proof of behaviour

(Mathematically) Strong proof of behaviour requires

- Participants' **Identities**
- **Complete characterisation** of participant(s)
- **Identity & Characterisation Information** exchanged between each participant



[2] Details in "*Establishing a Trust Relationship in Cooperative Information Systems*", Jang, Nepal, Zic CooPIS 2006, OTM Conferences (1), pp426-443, Springer

Each participant, upon receiving an ICI from another, **will only proceed with the transaction if the ICI is known and completely as expected (i.e. can be verified)**

CSIRO

External verification of good behaviour

Accountability Service – the third leg of the trust triangle

- **Evidence Recording**
  - Non-disputable operation history recorded in real-time
    - Signed and counter-signed
  - Be of sufficient detail for resolving any disputes.

- **Continuous System Monitoring**
  - Of evidential records

- **Exception or fault resolution**
  - Once an exception or violation is detected or reported, the root cause will be discovered in a provable manner
  - Actions taken to resolve exception in a timely manner.

Trusted Meter Extension (1)

- **Smart meters with a Trusted Platform Module (TPM) cryptographic microcontroller already in production**
  - Intention – provide code auditing facility through the use of TPM based attestation protocol.

Note #1: Requires the electricity to be consumed/produced as a part of normally attested and trusted environment.

Question #1: What if your plug-in electric car is at a charging station that is not known to your car or v.v.?

Trusted Meter Extension (2)

Note #2: Dealing with meter failures → revocation of TPM chip as it contains in sealed storage keys and certificates

- **What about having a *portable device* that can be attached to a meter *on demand* to make it trusted, and allows movement between end points?**
- **Device is associated with a home owner and issued by a service provider**
- **Prototype demonstrated at CeBIT Australasia 2010**

CSIRO

CeBIT 2010 demonstration system

- ***Demand Side Response* system**
  - Used a portable trusted computing platform (ESKey)
  - Issued by and controlled by an *Energy Services Company (ESCO)* responsible for providing demand management to electricity generators and cost savings to consumers

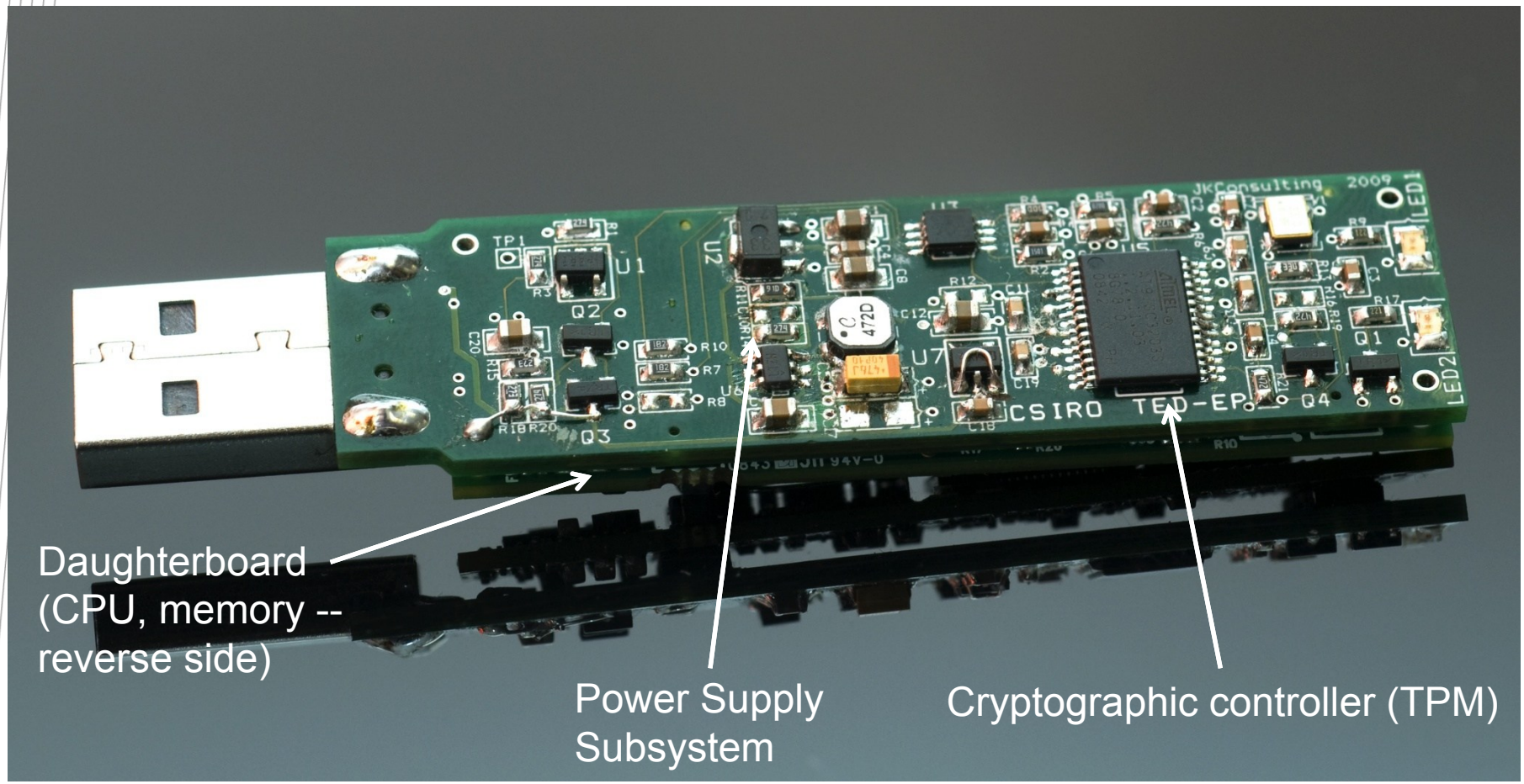
- **The ESKey contains:**
  - Secure storage for customer information, credentials a hash of the measurement of the *entire* platform, and cryptographic keys
  - Hardware cryptographic engine
  - Identity management
  - Policy management statements and enforcement mechanisms

- **The ESKey is sent by courier or physically collected by the customer once it has been configured by the ESCO**

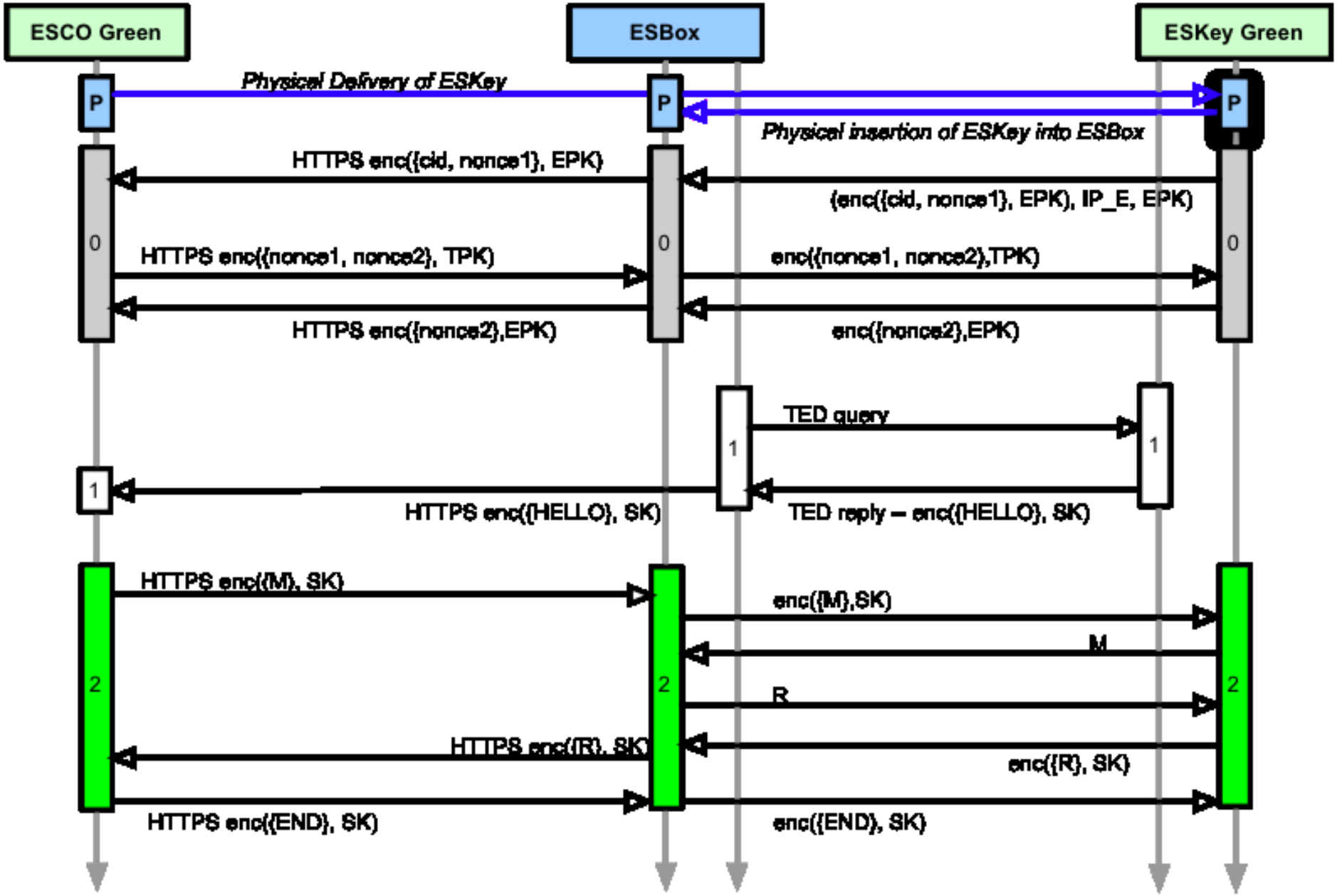
- **Plugs into a generic *Energy Services Gateway Box***

CSIRO

ESKey Prototype



Portable trusted computing platform


ESCO Green
ESBox
ESKey Green
P
P
P
Physical Delivery of ESKey
Physical insertion of ESKey into ESBox
HTTPS enc({cid, nonce1}, EPK)
{enc({cid, nonce1}, EPK), IP_E, EPK)
0
0
0
HTTPS enc({nonce1, nonce2}, TPK)
enc({nonce1, nonce2},TPK)
HTTPS enc({nonce2},EPK)
enc({nonce2},EPK)
1
1
1
TED query
HTTPS enc({HELLO}, SK)
TED reply – enc({HELLO}, SK)
HTTPS enc({M}, SK)
enc({M},SK)
M
2
2
2
R
HTTPS enc({R}, SK)
enc({R}, SK)
HTTPS enc({END}, SK)
enc({END}, SK)

Service Layer Security for Smart Grids (1)

- **Smart Grid systems are readily described in terms of a service oriented architectures (SOA)**
  - All actors and systems expose their functionality and interaction through specific message interfaces and protocols.
  - Internal operation is abstracted away
  - SOA approaches are (mostly) *stateless*

- **Opportunities result from**
  - intersection of the scale of the Smart Grid systems
  - the adoption of SOA

Service Layer Security for Smart Grids (2)

- **End-to-end key management solutions for massively scalable smart grid systems**
- **End-to-end authentication and authorisation**
  - SOA approach is stateless – resource updates occur at any time
  - How does a service respond in a timely, accurate manner?
- **End-to-end trust negotiation**
  - Adaptation of Public Key Infrastructure (PKI) to massive SOA systems

CSIRO

Trusted Information Sharing and Auditing Infrastructure

- **Advanced Metering Infrastructure allows remote access of end user electricity information**
  - this has impact on users' privacy
- **Proposal: add a privacy aware data sharing engine for managing smart meter readings.**
  - User control of how the meter is read and by whom:
    - Utility
    - Other service providers to which the meter has a subscription
  - Balances privacy requirements with energy efficiency
  - Audit information is maintained in a secure manner, allowing transparent decision making
    - User can find out why a service provider turned off an appliance
- **Currently, *no mechanisms exist to justify decisions made on behalf of a user***

CSIRO

Secure Smart Grid $\not\rightarrow$ *Trusted* Smart Grid

- **A trusted system is one that is (uniquely) identifiable *and* has a completely known behaviour**
  - May use security and privacy preserving technologies to achieve trust
  - Must maintain predictable behaviour under a variety of conditions: hostile attacks, failures of critical components, etc
- **Substantial research and development "opportunities"**
- **Need to have Guilds working together**
  - Electrical Power and Energy Distribution
  - Trust, Security and Privacy
  - Government Policy Makers
  - Consumers' Guilds

CSIRO

Wrapping up

- ***Trust*, security and privacy need to be built into smart grids from initial designs, not bolted on afterwards.**
- **Interoperation is critical**
  - Without sacrificing predictable, controllable, observable behaviour
- **Standards are allowed to evolve over time and still maintain integrity**
- **Solid foundations!**
  - Please take care! Needs excellence in specification, excellent engineering, excellent management, ….
  - Security and trust architectures appropriate to smart grids

CSIRO

CSIRO ICT Centre
John Zic
Research Team Leader, Trusted Systems
Information Engineering Laboratory

National Research Flagships

Climate Adaptation

Light Metals

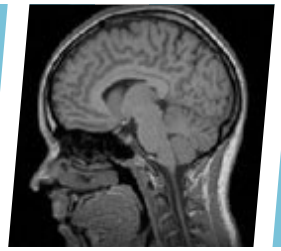
Sustainable Agriculture

Energy Transformed

Minerals Down Under

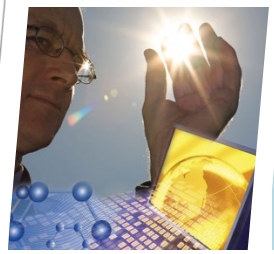
Water for a Healthy Country

Food Futures



Preventative Health

Wealth from Oceans



Future Manufacturing

CSIRO in 2008-09:

- Total revenue of $1.3 billion
- Federal funding of $668.1 million
- $634.8 million external revenue
  - With $229.6 million from IP revenue

National collections and facilities are a core part of our role

Host 3 major National Research Facilities