

Identity Evolves

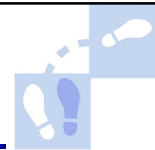
Why federated identity is easier said than done

AusCERT2011 *Overexposed*
18 May 2011, Gold Coast, Australia

Stephen Wilson
Lockstep Group



Quagmire



- Authentication vs Authorization
- How many identities do we have?

Facebook's Zuckerberg: "Having two identities for yourself is an example of a lack of integrity"

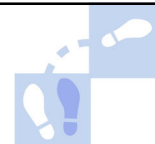
- Trust

**"To trust is good;
not to trust is better"**

Italian proverb

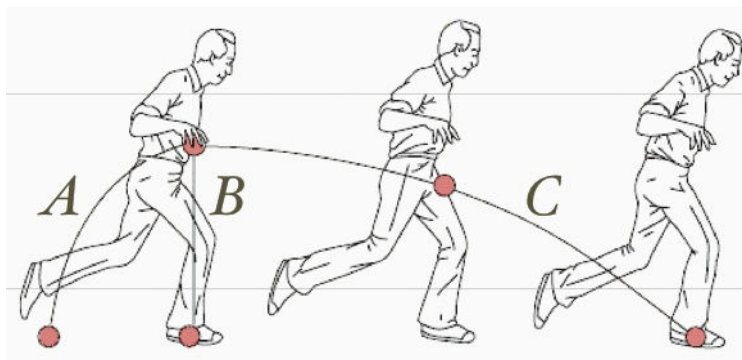
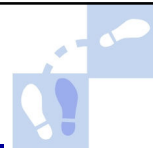


Special cases



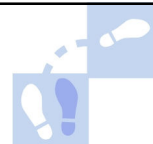
- Kantara Initiative study:
Implemented Trust Frameworks
<http://kantarainitiative.org/confluence/display/bctf/Implemented+Trust+Frameworks>
- BankID Scandinavia
- AAF & other tertiary ed
- US Federal PKI
- Octopus

Intuition



If I am known by one service provider then
I should be knowable by others, automatically

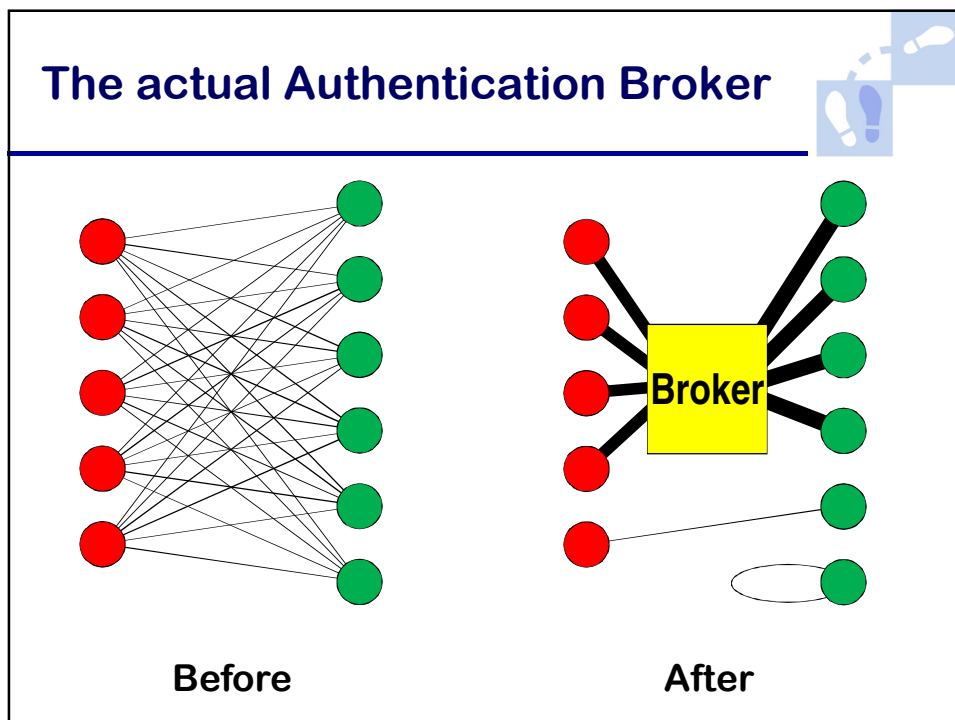
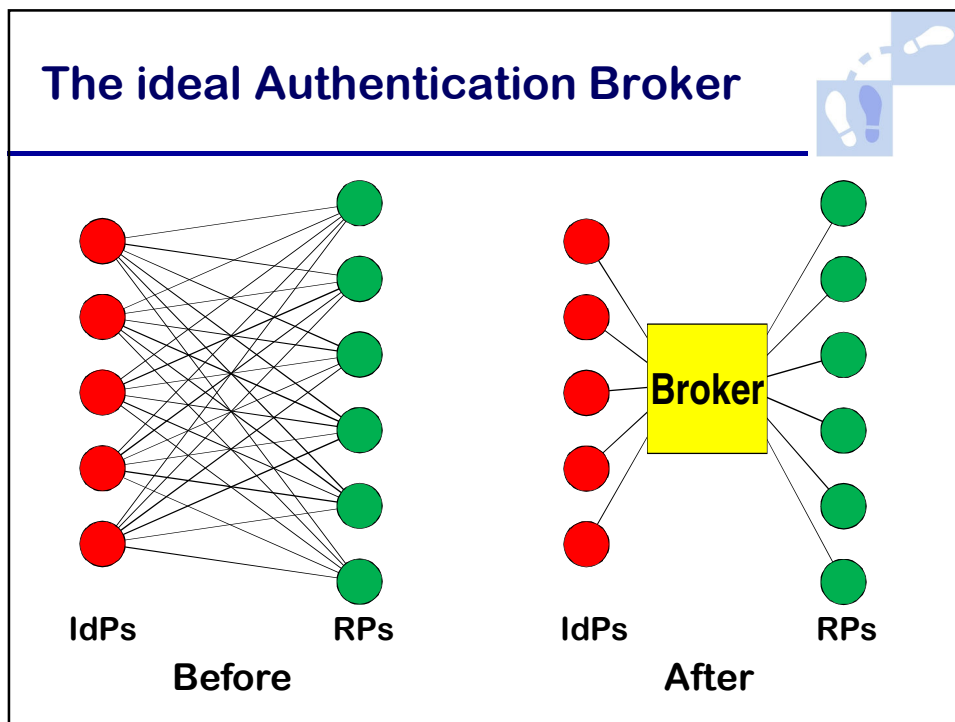
Dodgy metaphors



- Passport
- Silo
- Digital Identity

“A set of claims made by one
subject about itself or another
subject”

Laws of Identity



Risk is in the eye of beholder

| | | | | |
|--------------------------------------|-------------|-------------|--------------|--------------|
| Strength of Registration | Minimal (1) | Low (2) | Moderate (3) | High (4) |
| | Minimal (1) | Low (2) | Moderate (3) | Moderate (3) |
| | Minimal (1) | Low (2) | Low (2) | Low (2) |
| | Minimal (1) | Minimal (1) | Minimal (1) | Minimal (1) |
| Strength of Authentication Mechanism | | | | |

| Likelihood | Severity | | | | |
|----------------|---------------|-------|----------|-------|--------|
| | Insignificant | Minor | Moderate | Major | Severe |
| Almost certain | 0 | 2 | 3 | 4 | 4 |
| Likely | 0 | 2 | 3 | 4 | 4 |
| Possible | 0 | 1 | 2 | 3 | 4 |
| Unlikely | 0 | 1 | 2 | 3 | 3 |
| Rare | 0 | 1 | 2 | 3 | 3 |

But impact is *idiosyncratic*

| Type | Severity | | | | |
|--|---------------|-----------------------|--|-----------------------------|----------------------|
| Consequence rating | Insignificant | Minor | Moderate | Major | Severe |
| Release of personally or commercially sensitive data without consent | No impact | No significant impact | Measurable impact, breach of regulations | Significant impact | Major consequences |
| Financial loss to any client or third party | No loss | Minimal | Minor | Significant | Substantial |
| Risk to any party's personal safety | No risk | No risk | No risk | Any risk to personal safety | Threat life directly |

**What problem
are we trying to solve?**

Credentica U-Prove



**“Prove unanticipated properties of
protected identity assertions”**

**“It's déjà vu
all over again”**

Yogi Berra

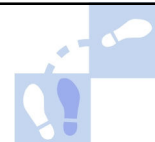
**“e-business was going to release
a massive pent-up demand for
stranger-to-stranger commerce.**

**“But truly un-vetted business
introduction is rare”**

***Trust Services – A Market Appraisal*
Rohan Freeman 2002**



Identity

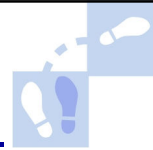


How I am known ...

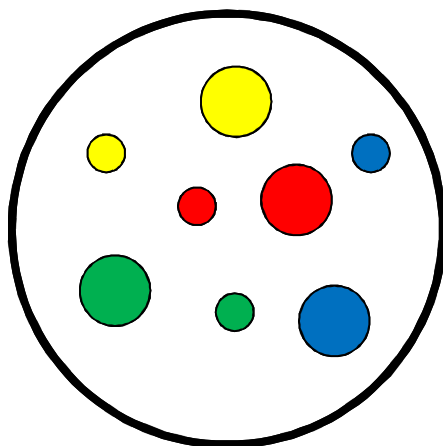


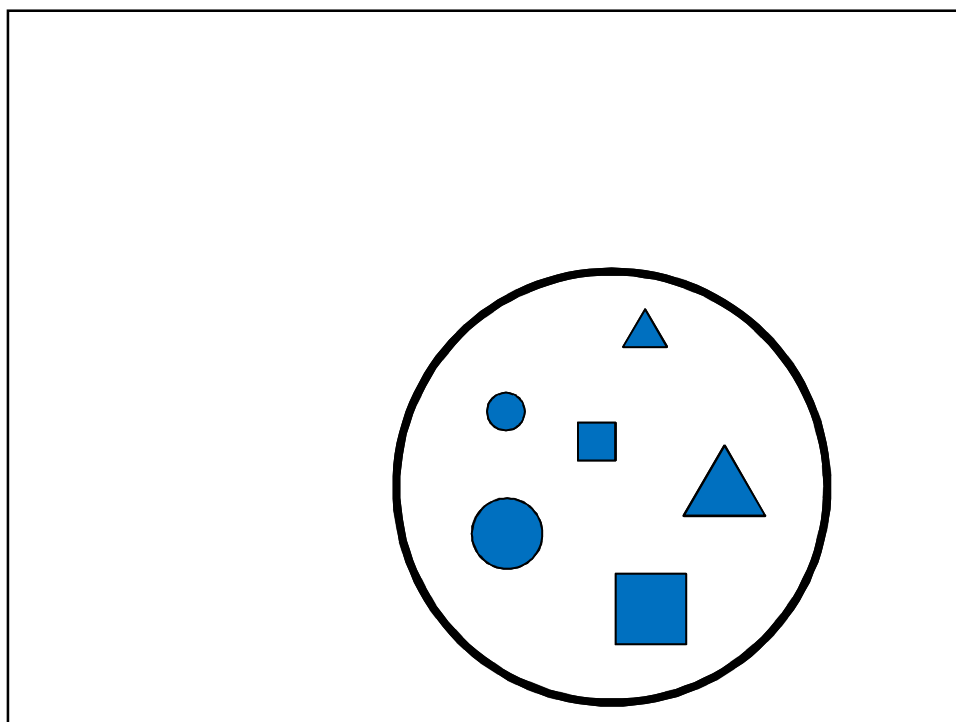
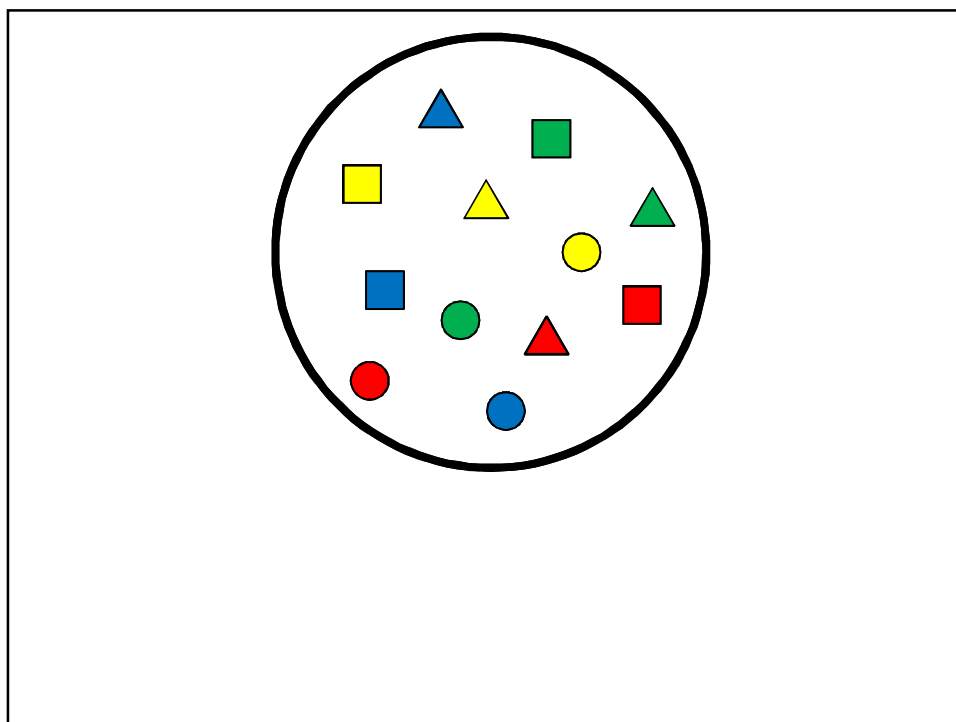
... in a circle

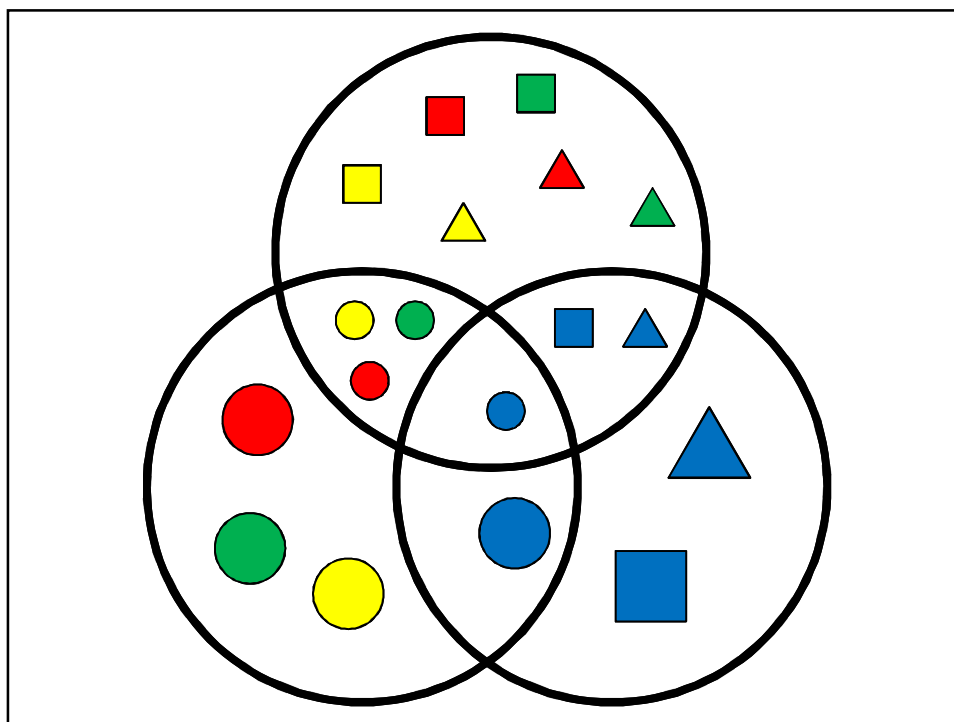
Circles



- Friends
- Family
- Work mates
- Professionals
- Alumni
- *High School Reunion Effect*







Id is proxy for *relationship*

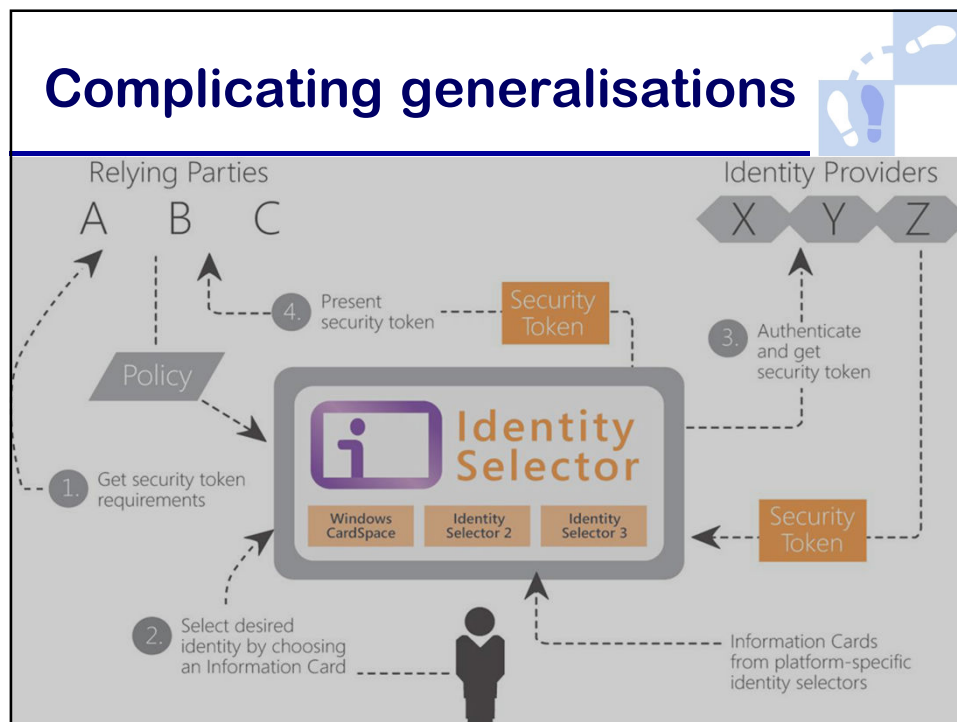
| Steve Wilson | | CONTRACT |
|------------------|---------------------|---------------|
| Best Sec Pty Ltd | 123456 | Term |
| Acme Bank | 4682749275 | Authority |
| Acme Bank | 3433309128 | Account |
| Visa | 4509 1234 5678 9010 | 100 pt Check |
| IHI | 50-345674-01 | Credit checks |
| Uni of Trees | 117811 | Legislation |
| Telco | 0414 4 | Can |
| Passport | A55598 | PIN |
| | | OTP |
| | | Scheme rules |
| | | Legislation |

Annotations:

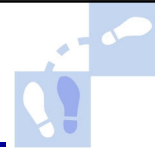
- Red arrow from "Acme Bank" to "Acme Bank" (self-loop).
- Blue arrow from "Visa" to "Uni of Trees".
- Yellow arrow from "Telco" to "Passport".
- Yellow callout box: "New Employee", "Login", "Keys", "Corporate car".
- Blue callout box: "Term", "Authority", "Account", "100 pt Check", "Credit checks", "Legislation", "Can", "PIN", "OTP", "Scheme rules", "Legislation".

**“All identity is ‘local’.
The further away from a pre-
specified business context an
identity credential becomes,
the less valuable it is”**

Darryl Greenwood 2002



Simplifying assumptions



- There are few total strangers
- There are few surprises
- Relying Party is often the Id Provider

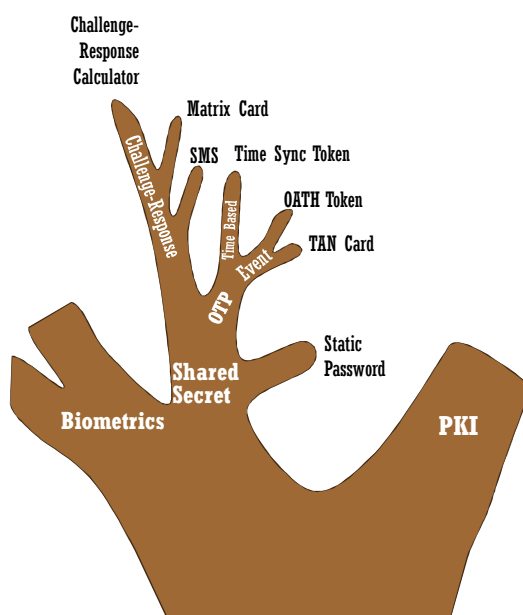
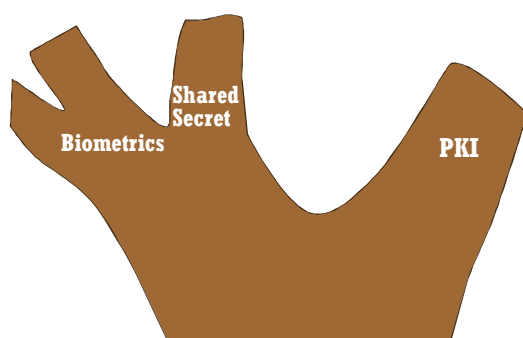
**Isn't
"closure"
a good
thing?**

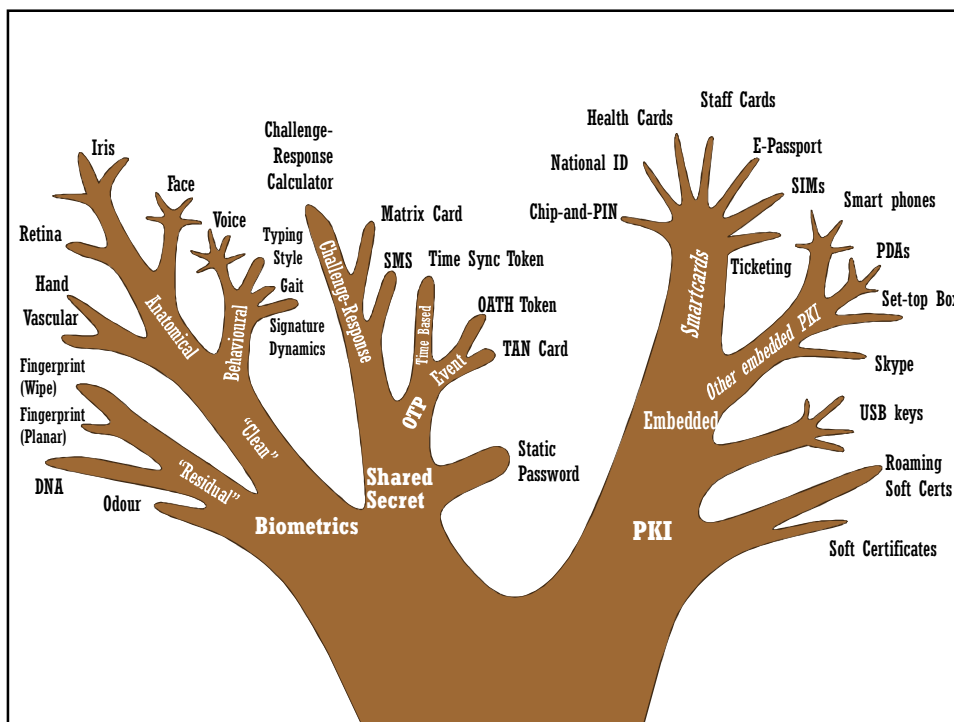
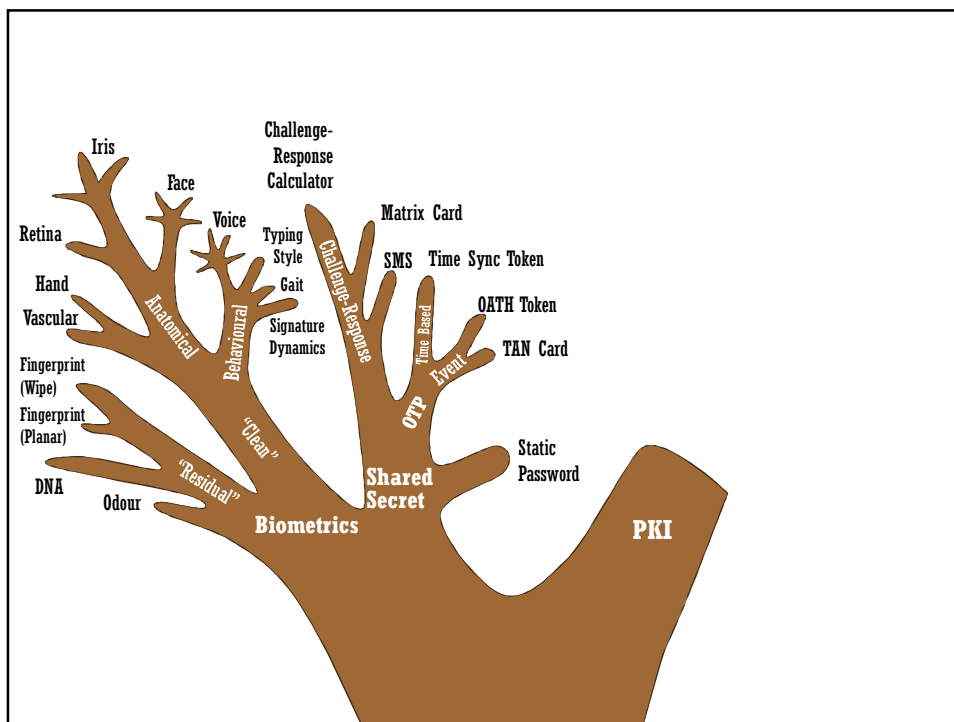


Gerald Weinberg



Authentication Family Tree

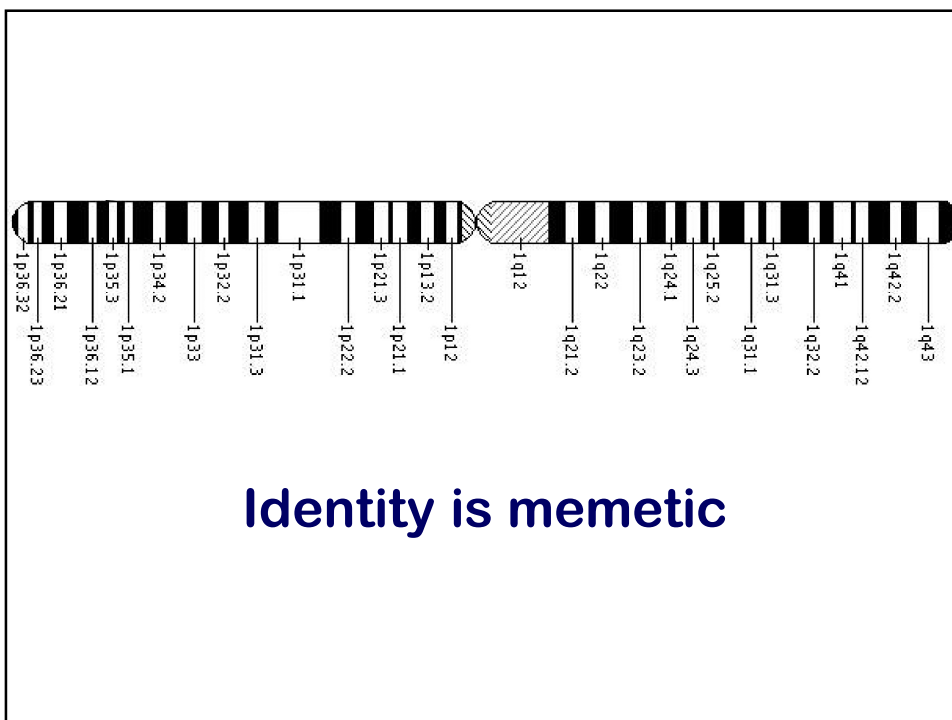




Selection pressures



- Security
- Fraud
- Convenience, accessibility
- Basel II, KYC, AML/CTF
- Professional standards
- Electronic Verification
- Single view of customer, of patient
- Privacy



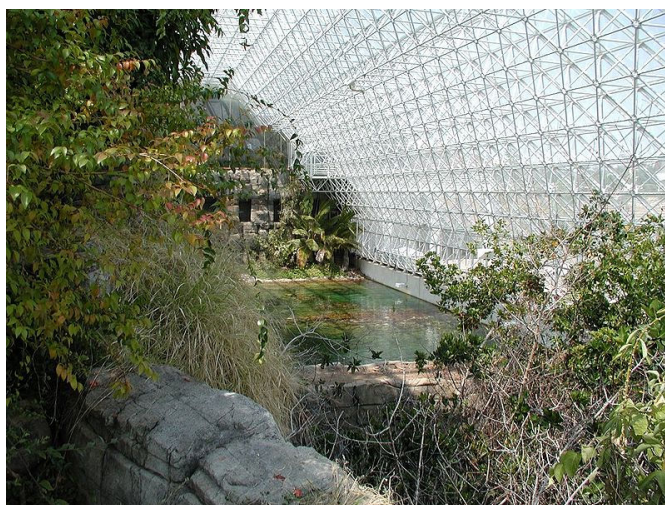
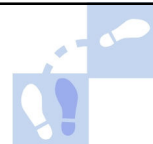


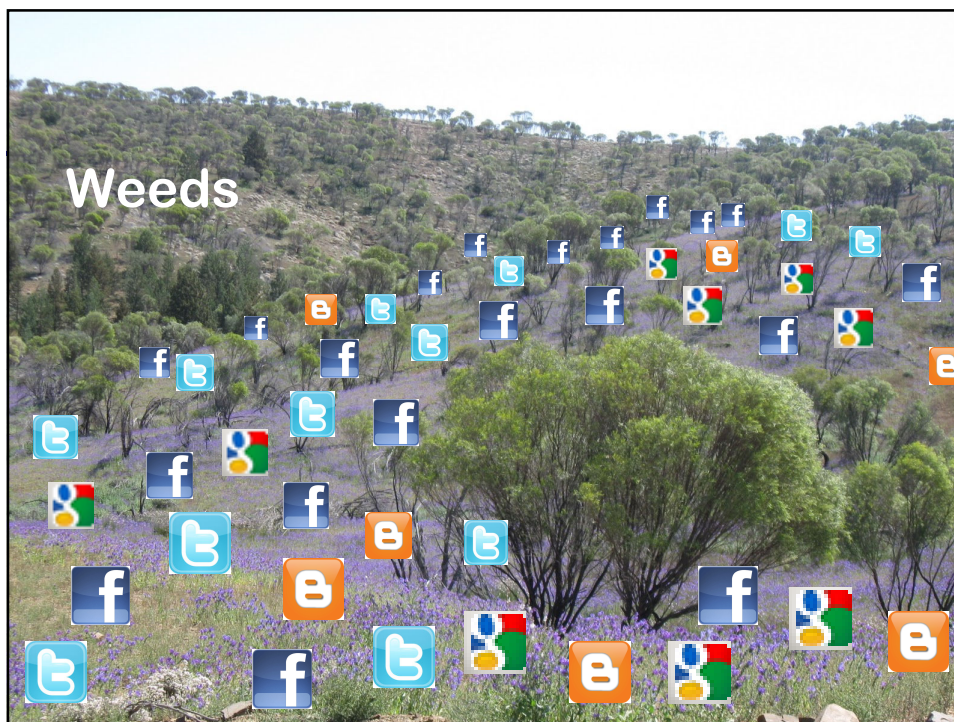
Existing ecosystems

- Banking
- Retail
- Employment
- Corporate regulations
- Tertiary education
- Healthcare delivery
- The professions



Artificial ecosystems?





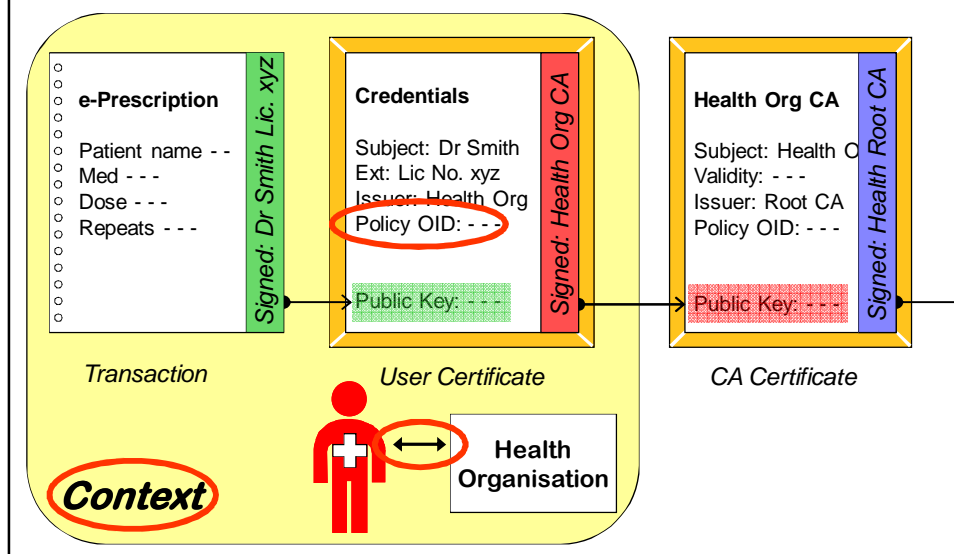
Predictions

- LinkedIn identity will thrive
- Bank ids will resist federation (KYC)
- NSTIC will fall short of expectations
- No “choice” of IdPs at higher LOAs
- Liability allocation will require government intervention
- Memetic diversity will be vital

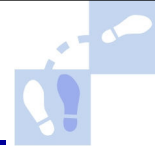
Conservation of identity

- Context is king
- Identity-in-context == Authorization
 - identity as an employee
 - identity as a personal banking customer
 - identity as a corporate banking customer
- Higgins *R-Cards*
- Gatekeeper *Relationship Certificates*

“Relationship Certificates”



Next steps



- No new artificial ecosystems
- Shift thinking to *relationships*
- Keep it simple
- PKI to conserve {identity + context}
- Research: phylomemetics of identity

Conclusion



If the hard part of any Internet project
is not technology
but business processes, change
management, people and legal ...

Then let's stick to the tech

Discussion



<http://lockstep.com.au>



LOCKSTEP

