

# Fractionating Identity

## The ecology of Digital Identity

---

MIT Legal Hackathon 2013  
28 Jan – 1 Feb

Stephen Wilson  
Lockstep Group



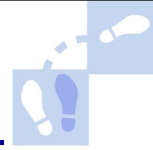
## Overview

---

- Federated Identity orthodoxies
- Hidden complexities
- Legal implications
- A new ecological frame
- “Fractionating” identity



## Harder than it looks

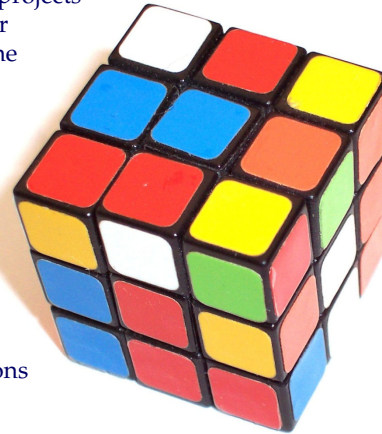


At least three major federated identity projects in Australia have been discontinued for their sheer complexity (I will explore the flaws in the classic business case later)

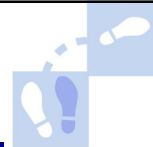
- **IIA 2FA Scheme**
- **Trust Centre**
- **MAMBO**

Promising start-ups and products similarly have failed. If Microsoft could not succeed with CardSpace, as exemplar of the *Laws of Identity* then something is wrong with the foundations

- **Sxipper**
- **CardSpace9**



## Monocultures

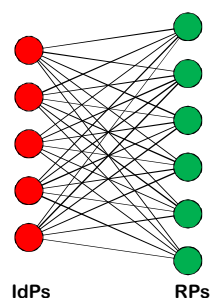


The great majority of successful identity federations are PKI-based and they are sector-specific; that is, they are two-fold monocultures. This is not a bad thing, but it does point to inherent challenges in sustainability of technologically heterogeneous cross-sector identity frameworks.

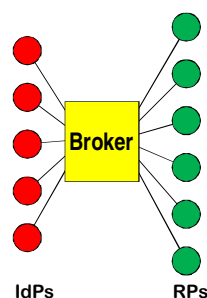
- **US Federal PKI**
- **SAFE BioPharma**
- **Australian Access Federation (tertiary ed)**
- **BankID (Scandinavian banks plus govt)**



## Problem: Legal novelty



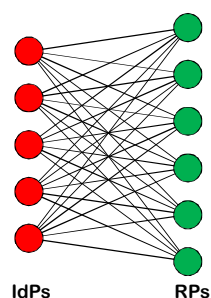
Before



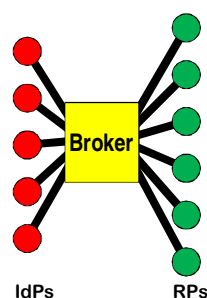
After

The business case for at least two large federated identity projects in Australia was a simple before-and-after schematic. The problem statement was depicted as the profusion of bilateral arrangements that subsist today between Identity Providers and Relying Parties. The solution was shown as a much simpler system of multilateral arrangements brokered by a central authentication hub. But this reasoning compares apples and oranges.

## Legal novelty continued



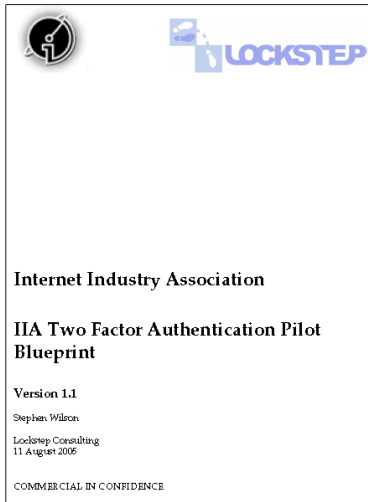
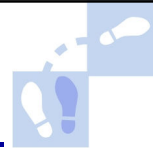
Before



After

The flaw in the business case is that the multilateral arrangements on the right are more complex and more weighty than the simple bilateral ones on the left. The sheer legal novelty of brokered identity verification means that fresh analysis is needed by parties before they can participate, adding to the total cost. It is not possible to say that reducing the absolute number of contracts through federation will in and of itself reduce the total cost, without knowing what the precise cost of the legal work really is.

## Internet Industry Assoc. 2005



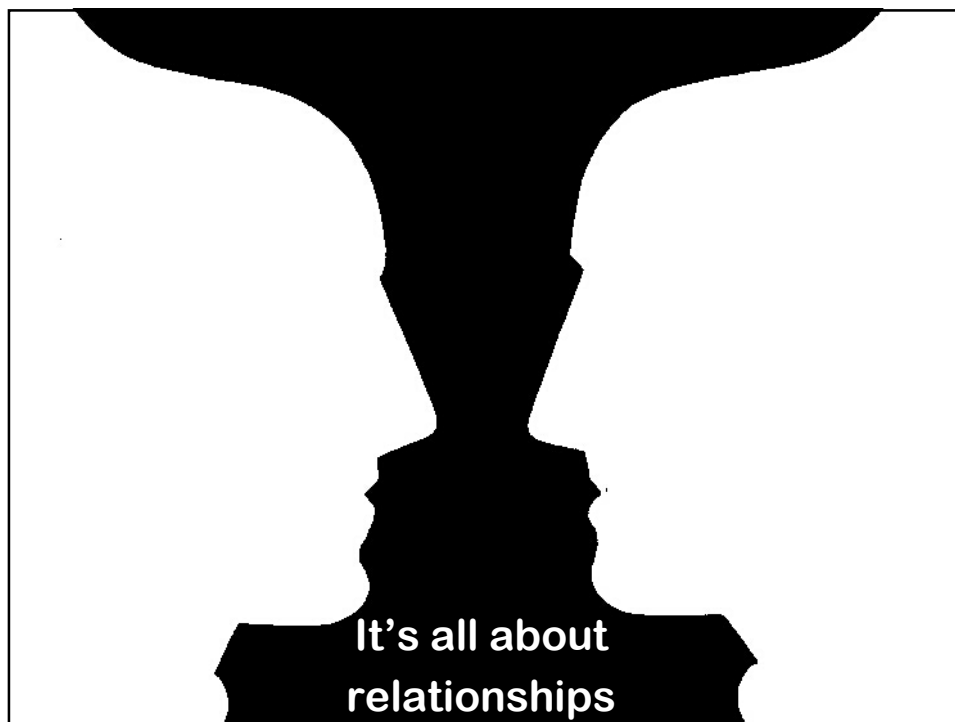
**“We’ve never seen anything like this before”**

**Legal counsel for IdPs, RPs**

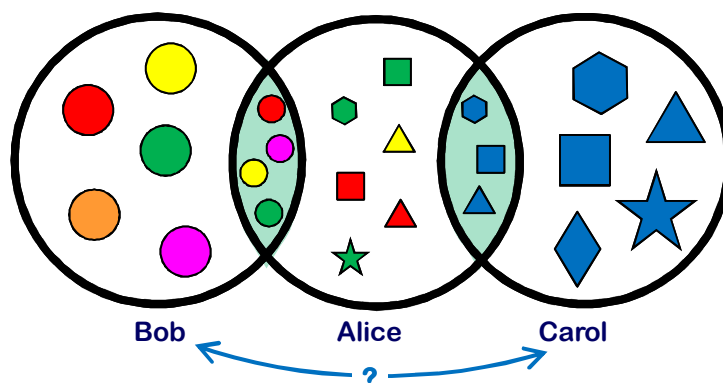
The proof that the “after” picture in the simple schematic business case is more expensive than it looks came out of the Australian Internet Industry Association’s attempted federation of 2FA providers. This project commissioned a reputable law firm to draft participation agreements for IdPs and RPs. Templates were tabled with management at retailers, airlines, financial institutions, government agencies and so on, all of whom had signed an MOU committing to the project. Yet several legal counsel responded that while they understood what we were trying to do, they had no experience in such a form of agreement, and they could not tell how long it would take to negotiate. Commercial lawyers are unaccustomed to novel forms of contract; the time & expense of negotiating such proposals are unbounded.

***So, does federated identity turn technology problems into legal and change management problems?***

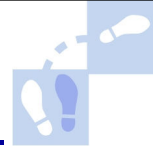
It is a truism that in large transformational projects, the technological challenges are typically relatively straightforward, while the change management and legal problems tend to be much harder. The real world experience of federated identity across the projects mentioned in Australia, and the surprising failures of international identity businesses large and small, underscores that commercial and legal issues have been insurmountable. Federated identity classically tries to address several issues at once, including security, identity theft, usability and accessibility. It strikes me that these are, on their own, reasonably straightforward technological issues, and they would be better dealt with as such, without creating new business and legal challenges.



Identity – that is, how you are known in a context – is a proxy for a relationship you have with everyone else in that context. The *Laws of Identity* defined Digital Identity as a *set of claims* about a digital entity. Federation is all about making identities “interoperate”, but what does that really mean? Does it mean *stand for one another*? It seems intuitive for identities to be somewhat interchangeable, insofar as if you are known by one service provider then you could expect to leverage that knowledge into other services, in effect porting your identity from one service context to another. But if we consider an identity to be a proxy for the relationship you have with the first service provider, it is not obvious that the relationship can mean a great deal to others. Relationships are not intrinsically transitive. That is, if Bob has a relationship with Alice, and Alice has one with Carol, Bob does not automatically have a clear relationship with Carol. Relationships are about the attributes pairs of people have in common. If Alice and Bob have roundness in common, and if Alice and Carol share the attribute of blueness, it does not follow that Bob and Carol have anything in common at all.



## Forgotten lessons of PKI



We've actually been down this road before. Many of the under-appreciated challenges in federated identity were traversed in "Big PKI" 10 to 15 years ago. For instance, hierarchical PKI advocates criticised the "Web of trust" on the grounds that trust is not transitive.

- **Trust is not transitive**

- **If A trusts B and B trusts C, can A automatically trust C?**

A widely known legal obstacle to open PKI at the time was the lack of "contractual privity" (i.e. prior legal relationship) between Certification Authorities and Relying Parties processing digital signatures of certificate holders. Legal analysis commissioned by the Australian Government in 1999 found that Australian law left significant doubt regarding liability without privity of contract with the CA [Ref: [www.egov.vic.gov.au/pdfs/publication\\_utz1508.pdf](http://www.egov.vic.gov.au/pdfs/publication_utz1508.pdf)]. Some CAs responded by attempting to have Relying Parties sign "RP Agreements" posted on the CAs' websites. Few RPs did so; after all, the agreement was drafted in the CA's favour!

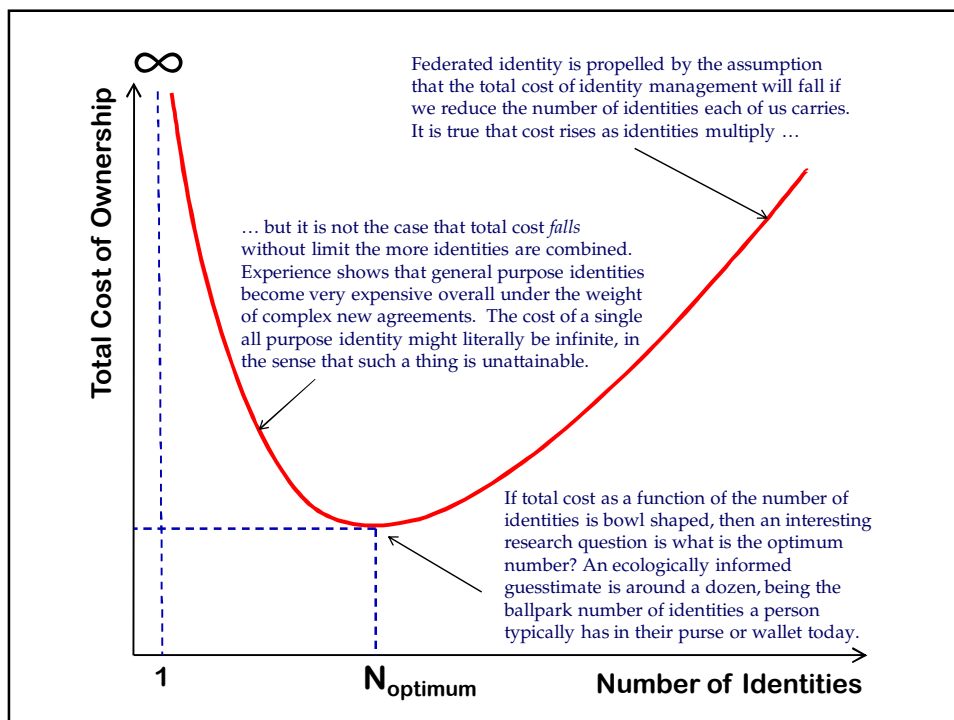
- **Lack of contractual privity**

- **What is CA's duty of care to RP?**

The RP agreement was just one example of the overarching legal novelty of orthodox Big PKI, which also included enormously weighty Certificate Policies and Certification Practice Statements. One of the clearest lessons in PKI is that it only works well in closed communities, where privity already exists, and where certificate manufacturing is treated as purely a backend matter, similar to magnetic stripe card production.

- **Cost of novelty**

- **Closed IdM schemes work best**





If a Martian security professional were to come to Earth, the first thing they'd notice would be the great profusion of authentication mechanisms ...



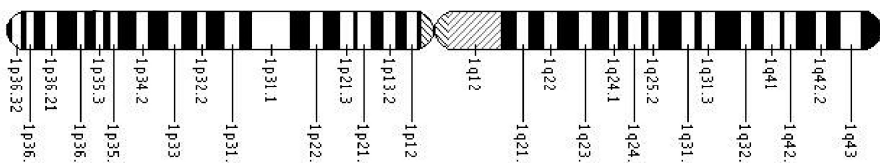
Where did they all come from? The very variety of authenticators begs an ecological sort of explanation. As with natural speciation, different mechanisms have probably evolved in response to different environmental pressures.

## Identity is memetic



The concept of memetics was introduced by evolutionary biologist Richard Dawkins, who coined the term “meme” meaning an inherited unit of human culture, analogous to the gene.

It seems likely that Digital Identities can be unpacked into discrete traits or memes. Examples include registration process, evidence of ID, user interface, number of factors, algorithms, key lengths, liability arrangements and so on. The nature of these memes range from strict standards imposed by regulators, through to simple habits for identifying people. All of them relate to risk management, and each of them shifts more or less gradually over time as local risk environments change. For example, key length has increased steadily in response to the growing risk of brute force attack. Certain memes stabilise at different rates in different ecosystems; for example, in government, the hash algorithm SHA-1 has been widely superseded by SHA-256, but the new meme is slower to take hold in commerce because a different mix of environmental pressures applies, like affordability and legacy system interoperability. Security tactics like Two Factor Authentication can jump ecosystems: retail banking got the idea of 2FA from enterprise security at high tech companies.





This ecological mindset might lead to a more generous understanding of the dreaded identity silos. We can see them now as *ecological niches* in different ecosystems, like banking, retail and government. And we might usefully temper some of the grander expectations of the new identity frameworks. We should probably be more sceptical about the prospects of taking an identity like a student card out of its original context and using it in another such as banking.\*

**It's a lot like taking a saltwater fish and dropping it into a fresh water tank.**

As MIT's Dazza Greenwood said in 2002: *All identity is 'local'. The further away from a pre-specified business context an identity credential becomes, the less valuable it is.*



\* Ref: <http://www.whitehouse.gov/blog/2011/01/07/national-program-office-enhancing-online-trust-and-privacy>.



## Selection pressures in existing ecosystems

The ecological frame illuminates that different selection pressures affect different business environments. Identity memes evolve over time within existing ecosystems and niches. Examples of selection pressures include fraud trends, privacy, convenience, accessibility, regulations (like Basel II, KYC rules, AML, HIPAA & HSPD-12), professional standards, and disruptive new business models like branchless banking demanding new methods for electronic verification of identity. Before we expend too much effort building artificial new identity ecosystems, we should pay attention to existing business ecosystems.

Banking	Security
Retail	Fraud
Employment	Privacy
Corporate regulations	Convenience
Tertiary education	Accessibility
Healthcare	Basel II, KYC, AML/CTF
The professions	Professional standards
	Electronic Verification
	Single view of customer

## Drop down a level

**Relationships**

**Identities**

**Attributes / Claims**

**Presentation**

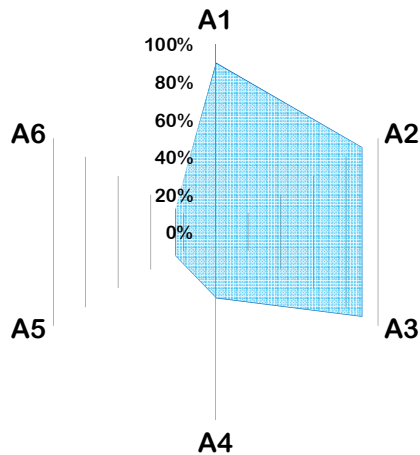
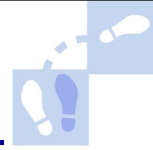
**Transport**

**Deeper network layers**

Digital Identity might be conceptualised in an OSI-like stack. Each **identity** is built as a set of **claims or attributes**. In sophisticated IdM schemes, each attribute is **presented** via protocols like Oauth, OpenID Connect, SAML and XACML, which in turn are **transported** via networking and security primitives like WS\*Trust, IPSEC and X.509. In simpler schemes like Internet banking, the attribute might be a customer specific One Time Password presented out of band simply via a cell phone or key fob.\* Identity Management to date has focused at the highest level on the sharing of discrete identities, as if each identity is a thing. If we recognise identities as proxies for complex relationships, then it will be seen to be more fruitful to drop down a level, and deal instead with component attributes.

\* A work in progress at Lockstep is to characterise all IdM techniques—RACF, RADIUS, Kerberos, PKI and so on—according to a new layered model like this.

## Fractionating identity



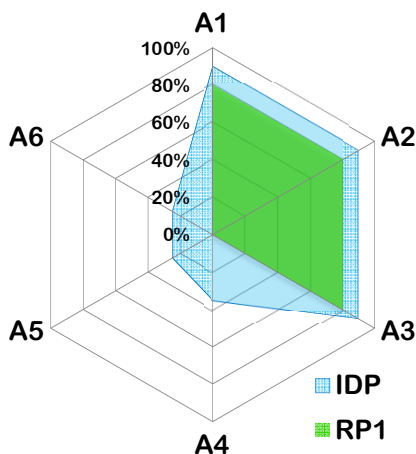
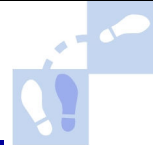
The high level identities like bank accounts and professional credentials that we have tended to think of as discrete things are actually loose mixtures made from more elemental attributes. We can *fractionate* digital identities into the component attributes, and in the process better understand the interoperability of Identity Providers and Relying Parties.

This line of thinking also leads to new ways to visualise digital identity specifications for IdP and RP. Consider an IdM environment where six attributes are of interest: given name, address, date of birth, gender, university qualifications and residential status. A given IdP is able to vouch for name, address and DOB to high level of confidence, but has less certainty over the other attributes. The IdP defines a surface for its customers in the 'attribute space'.

### Identity Provider

A1 Given name 90%	A4 Gender 35%
A2 Address 90%	A5 Qualifications 25%
A3 DOB 90%	A6 Residency 25%

## Fractionating identity cont.



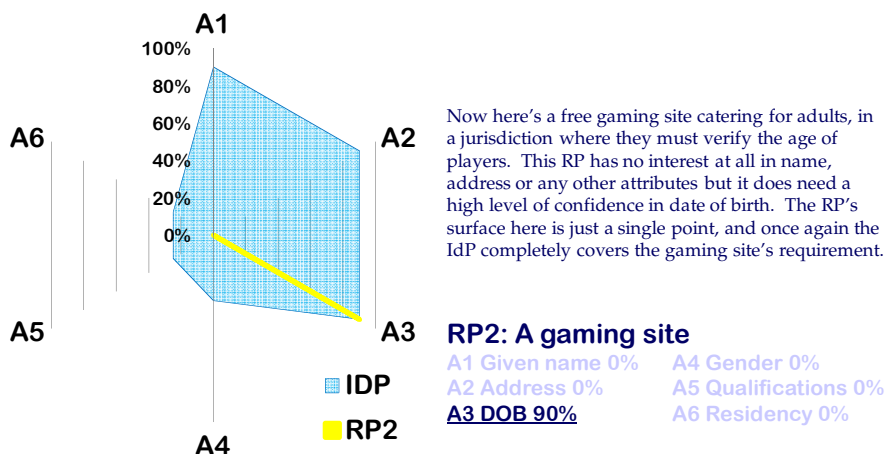
Now consider as a Relying Party a bank wishing to identify a new account holder. The bank has a high degree of interest in the new customer's name, address and date of birth, but it doesn't care about gender, residency or qualifications. The bank's identity requirement also defines a surface, shown in green, which is readily compared to the Identity Provider.

The IdP completely covers the bank's requirement.

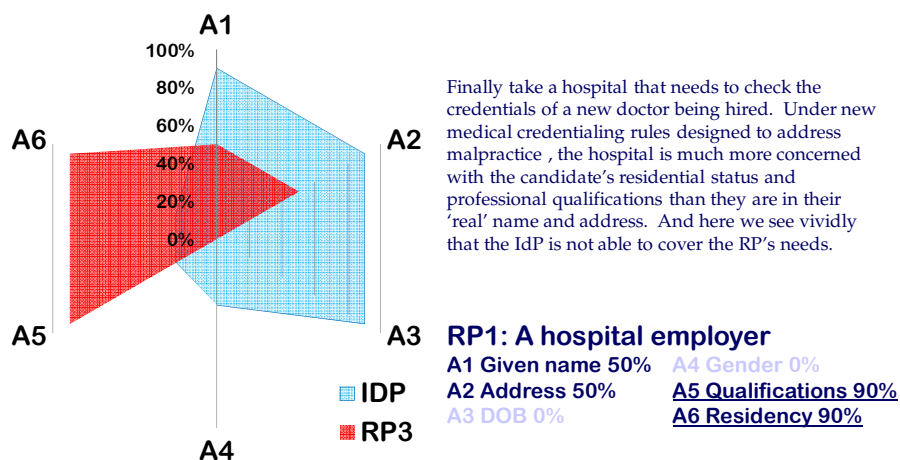
### RP1: A bank

A1 Given name 80%	A4 Gender 0%
A2 Address 80%	A5 Qualifications 0%
A3 DOB 80%	A6 Residency 0%

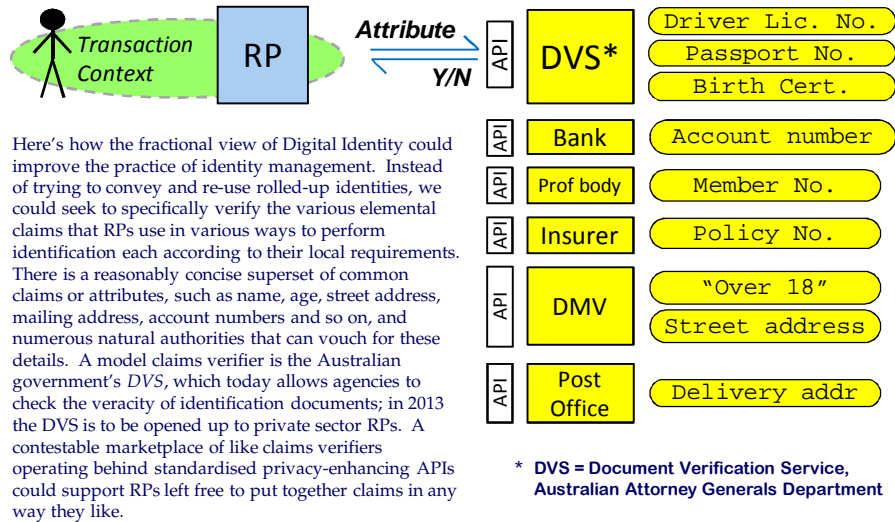
## Fractionating identity cont.



## Fractionating identity cont.

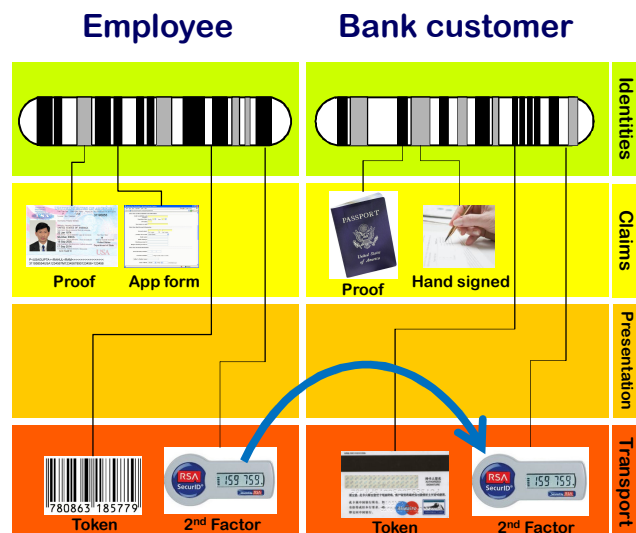


## A claims verifier ecosystem

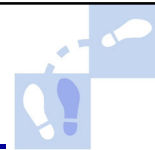


## Recombinant ID engineering

A memetic and ecological theory of Digital Identity brings several fresh possibilities. It should improve the success rate of federation by clarifying why identity elements are the way they are. Memetics provides a conceptual frame within which identities may be fractionated and their elements more carefully reassembled in the same way as recombinant genetic engineering. The ecological theory is explanatory and predictive. For instance, it explains why social logon has spread so rapidly—*literally like weeds*—as the new social business ecosystem is like a bare fertile field, with no dominant species as yet. And we've actually seen identity memetics at work in the wild. For instance, Two Factor Authentication jumped from high tech firms in the 90s to Internet banking in the 00s, in much the same way as genes jump between bacteria.



## Conclusions



Echoing Dazza Greenwood's observation that all identity is local, the reality of identity management is that we can "think global" all we like but every organisation is always going to "act local". When it comes to getting to know its people, risk management means that every business is always going to do identification in its own particular way.

- **Each *Digital Identity* is a proxy for a relationship**
- **Elements of identity are *memetic***
- **Digital Identities evolve to match niches in business ecosystems**
- **Beware of transporting identities across ecological niches**
- **Fractionate identities into attributes or claims**

### Further reading

- *Identity Evolves: Why Federated Identity is easier said than done*  
AusCERT 2011 Security Conference, Gold Coast, May 2011  
[http://lockstep.com.au/library/identity\\_authentication/an-ecological-theory-of-digit](http://lockstep.com.au/library/identity_authentication/an-ecological-theory-of-digit)
- Lockstep's identity blog  
<http://lockstep.com.au/blog/identity>