

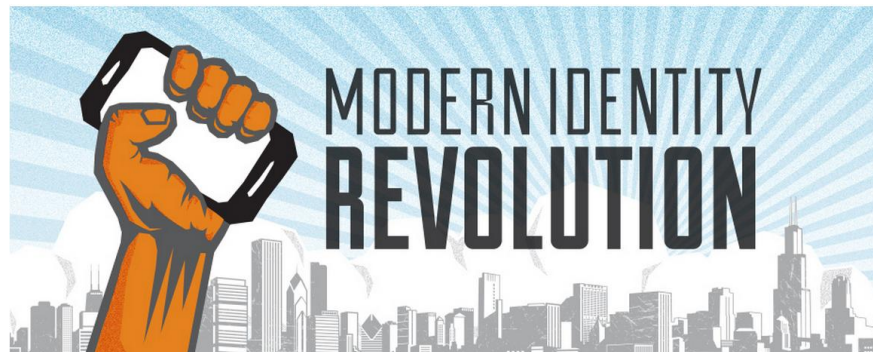
The Authentication Family Tree

CIS 2014 *Modern Identity Revolution*, Monterey, California

22 July 2014

Steve Wilson (@steve_lockstep)

Principal Analyst, Constellation Research



Authenticators



ID Proofing



Registrar

Verification
Server



Registrar

Verification
Server



Registrar

TRUSTED THIRD PARTY

Device
specific
login pages

Authentication
Broker

SAML API

Attributes
Database

SAML API

SP

SAML API

SP

SAML API

SP

Plenty of solid architectures have been developed for federated identity. But time and time again, federation proves harder than it looks.

ect

Unknown unknowns



Internet Industry Assoc.

IIA 2FA Pilot Blueprint

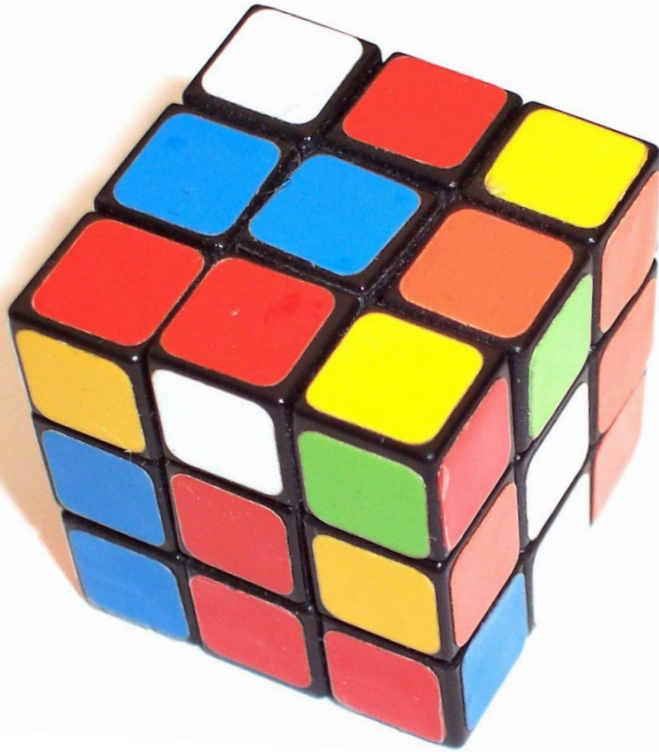
11 August 2005

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

IdP/RP Counsel

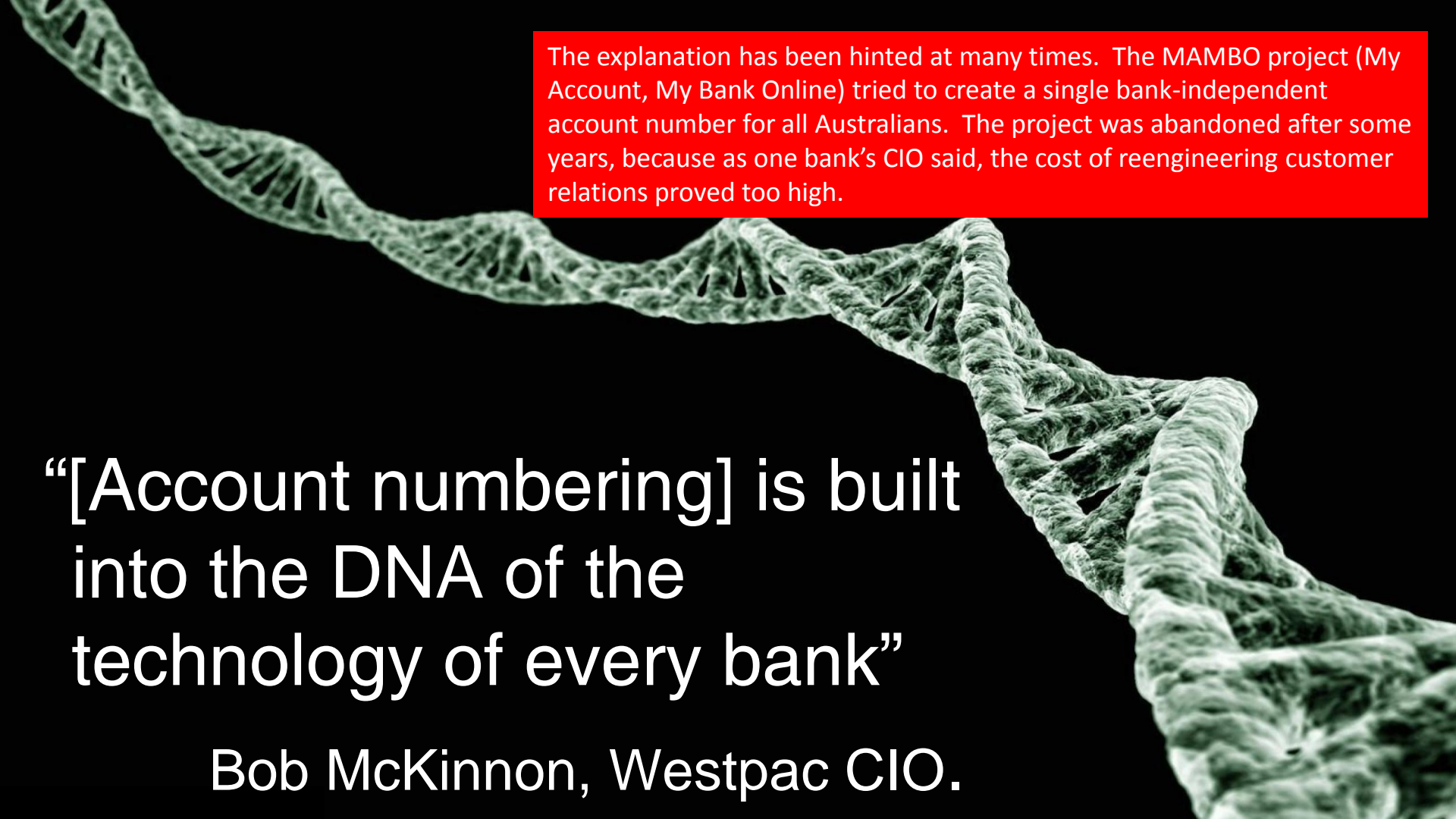
The Australian Internet Industry Association went a long way towards building a shared 2FA hub, including well written template agreements between the hub and participating IdPs and RPs. But lawyers for the participants didn’t know how to deal with the contracts. The legal novelty creates a risk management situation that cannot be planned

Harder than it looks



- IIA 2FA Scheme
- Trust Centre
- MAMBO
- Sxipper
- CardSpace

Federated Identity is very appealing and attracts strong support, in the early days of promising projects and start-ups. But the repeated failure demands explanation



The explanation has been hinted at many times. The MAMBO project (My Account, My Bank Online) tried to create a single bank-independent account number for all Australians. The project was abandoned after some years, because as one bank's CIO said, the cost of reengineering customer relations proved too high.

“[Account numbering] is built into the DNA of the technology of every bank”

Bob McKinnon, Westpac CIO.



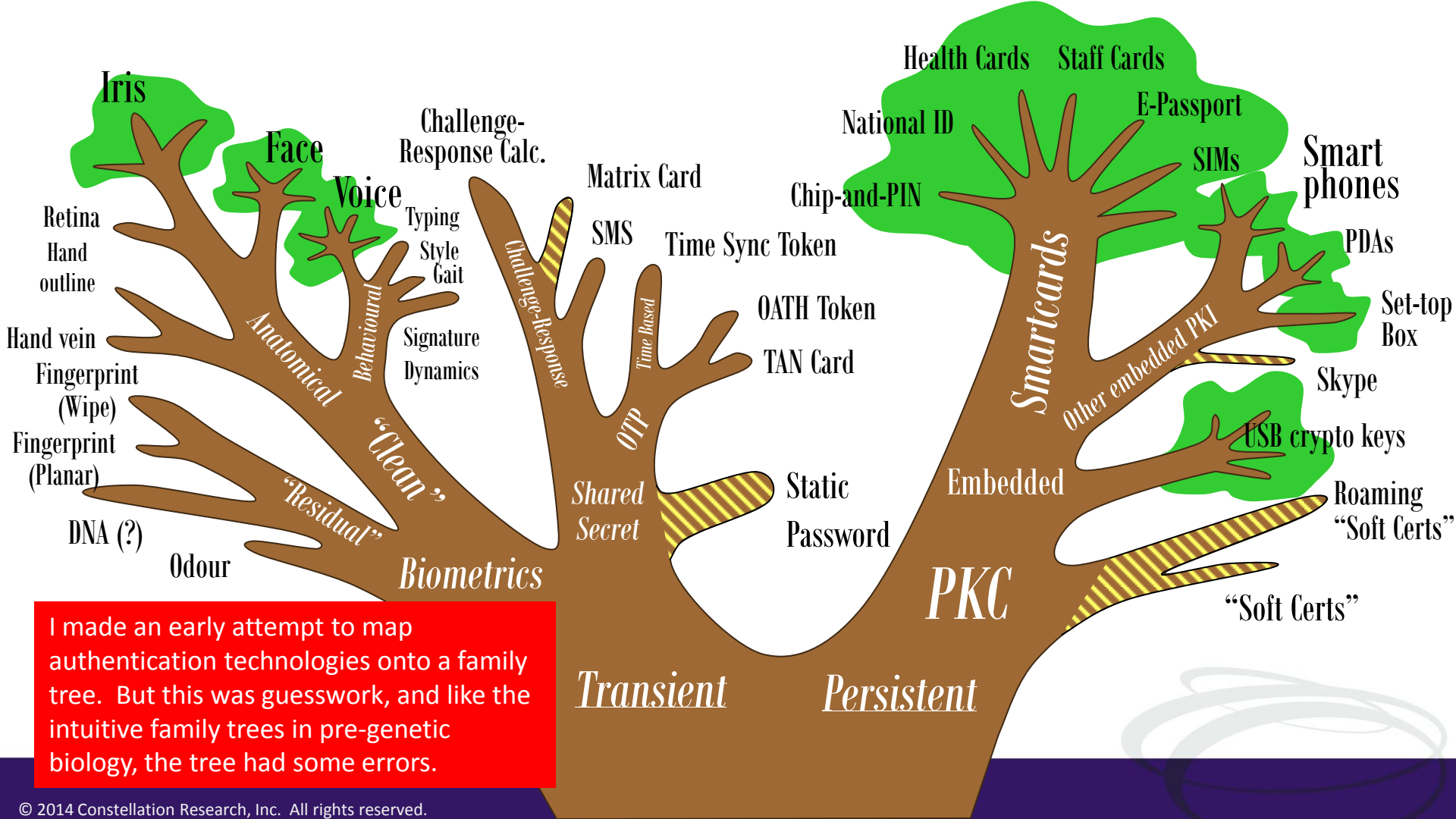
THE RECEIVED WISDOM:

A Digital Identity is a set of claims made about a digital subject.

And Digital Identities are highly contextual.

THE MISSING LINK:

So, Digital Identities have evolved



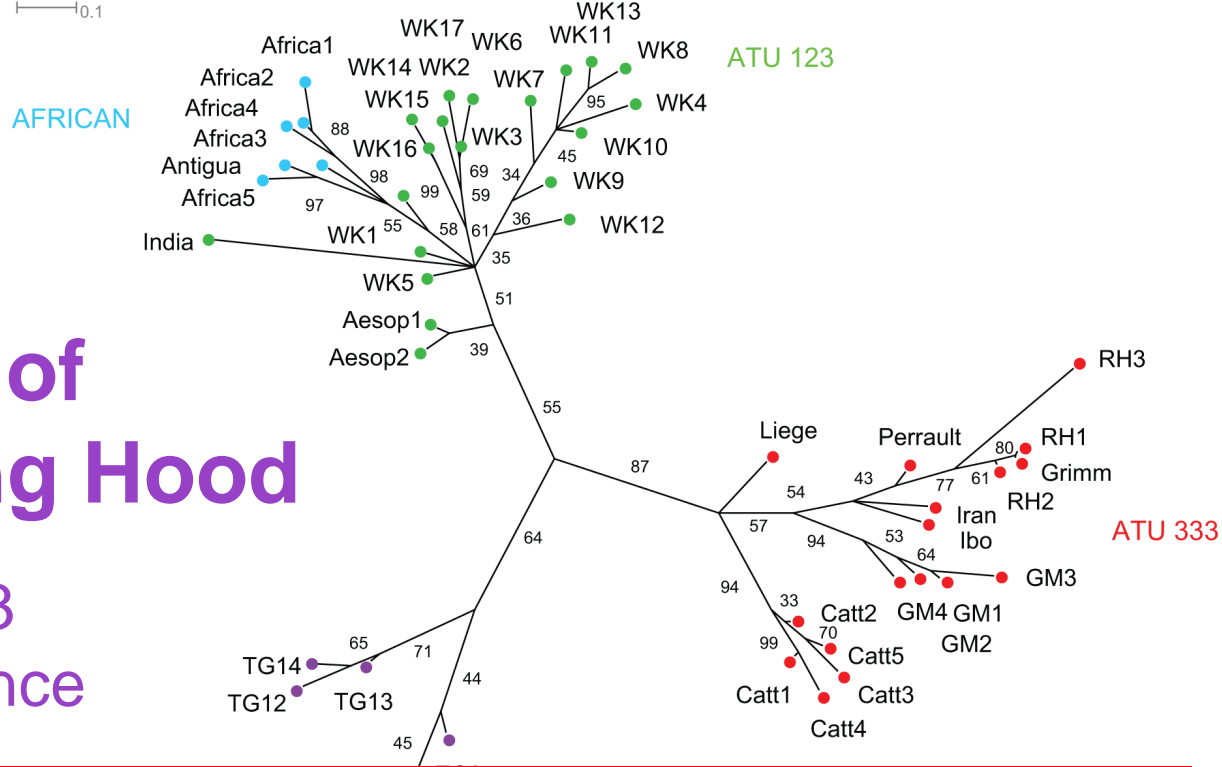
I made an early attempt to map authentication technologies onto a family tree. But this was guesswork, and like the intuitive family trees in pre-genetic biology, the tree had some errors.

Meme (n): a replicable unit of cultural transmission.

Basic features are shared between digital identities and are selectively passed down from one generation to the next – such as form factors, algorithms, identification rules, key lengths, and user interfaces. These features represent “memes” in the technical sense of the word.

The phylogeny of Little Red Riding Hood

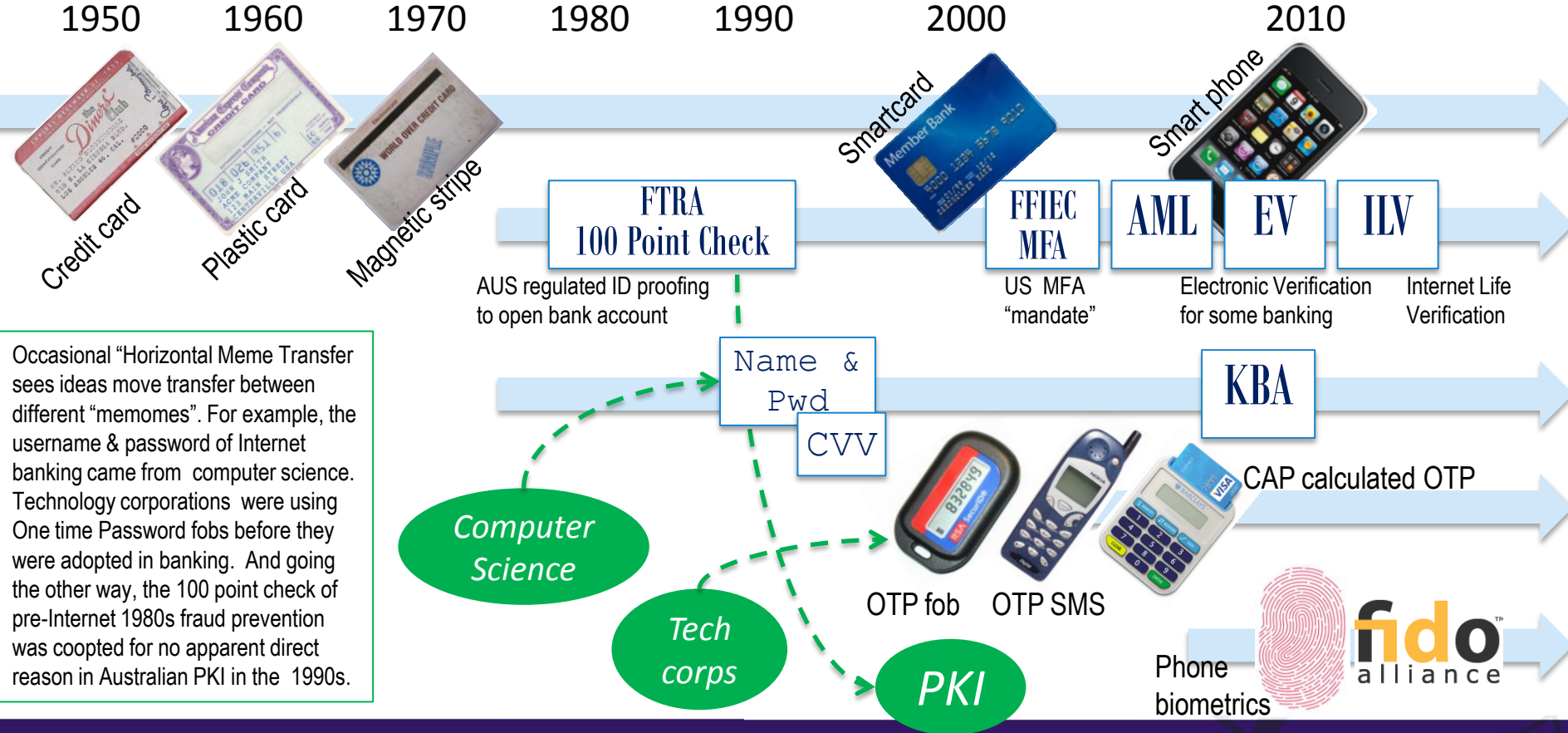
Jamshid Tehrani 2013
Public Library of Science



Memetics has been a controversial pursuit, but is undergoing something of a resurgence. I am applying phylogenetic modelling in an attempt to demonstrate the evolved interrelatedness of digital identities. The tree shown here is of a famous fairy story, and shows the strength of memetics in diverse fields of study.

TG10 Huang TG1

Authentication evolves



The Authentication Memome

Character	Values
Token Form Factor	Mag card / Prox card / Smartcard / Smart phone
Token activation	None / Password / PIN / Biometric / Continuous Auth
ID Proofing	FTRA 100 points / AML / HIPAA / PIV / ECD / ISO 29003
Enrolment channel	OTC / Remote / Automatic / Refereed
Second Factor	None / Time OTP fob / Event OTP fob / OTP SMS / C-R fob / CAP
Biometric	None / Fingerprint* / Face* / Voice* / Vascular Hand / ECG
Signature Algorithm	RSA / ECDSA
Sig Key Length	2048 / 4096 / 160 / 224 / 256 / 384 / 512
OTHERS	WORK IN PROGRESS

So what?

- Explanatory power

The memetic/ecological frame may shed light on why federated identity is harder than it looks

- We're getting rid of LOAs right?

Earlier in the Cloud Identity Summit, the new NSTIC CIO floated the idea of getting rid of Levels of Assurance. It's a great idea. To make it work, we need fresh understanding of how authentication solutions respond to real risks.

- Help drive the *Attributes Push*

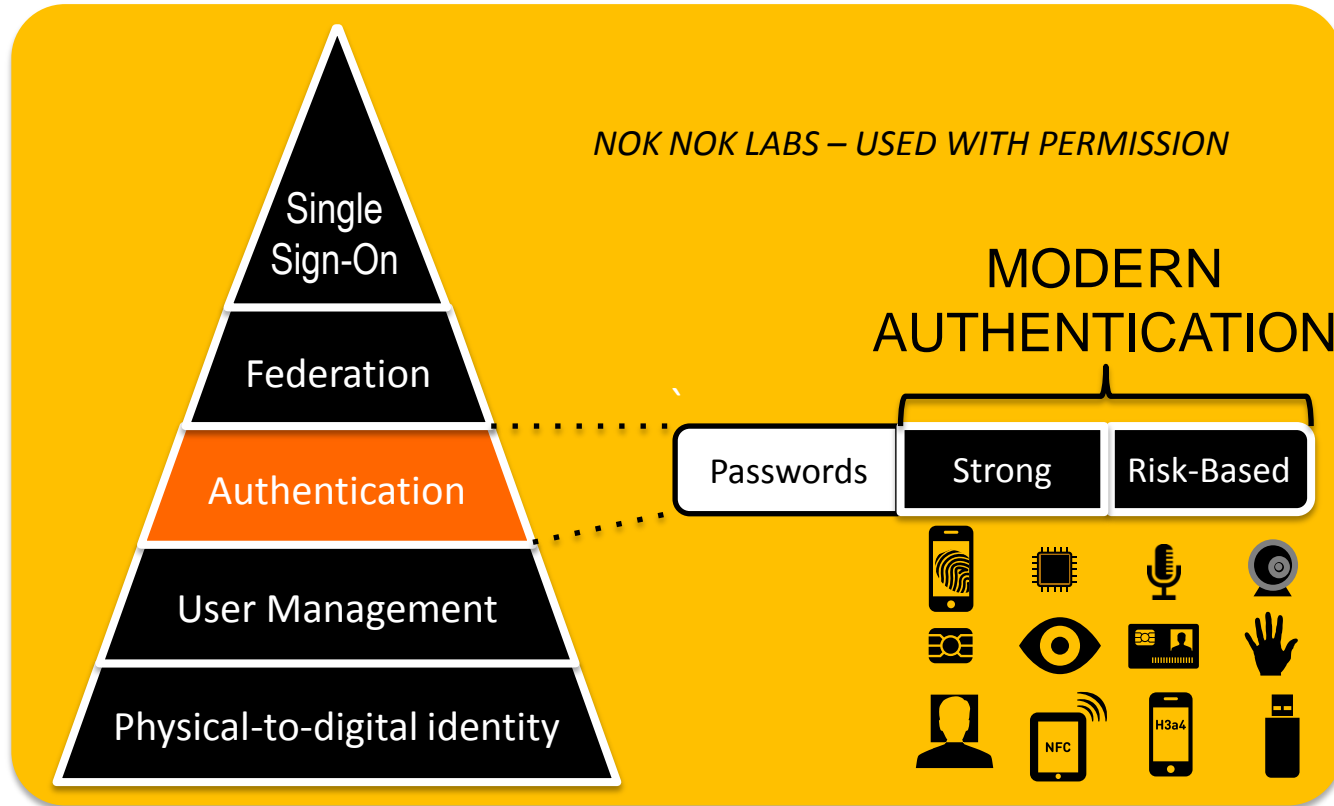
Interest in Attributes is gaining strength, with the AXN, and in the strategies espoused by FIDO. The ecological/memetic frame emphasises attributes and provides a robust intellectual framework.

- Attributes Exchange Network (AXN)

- FIDO Alliance



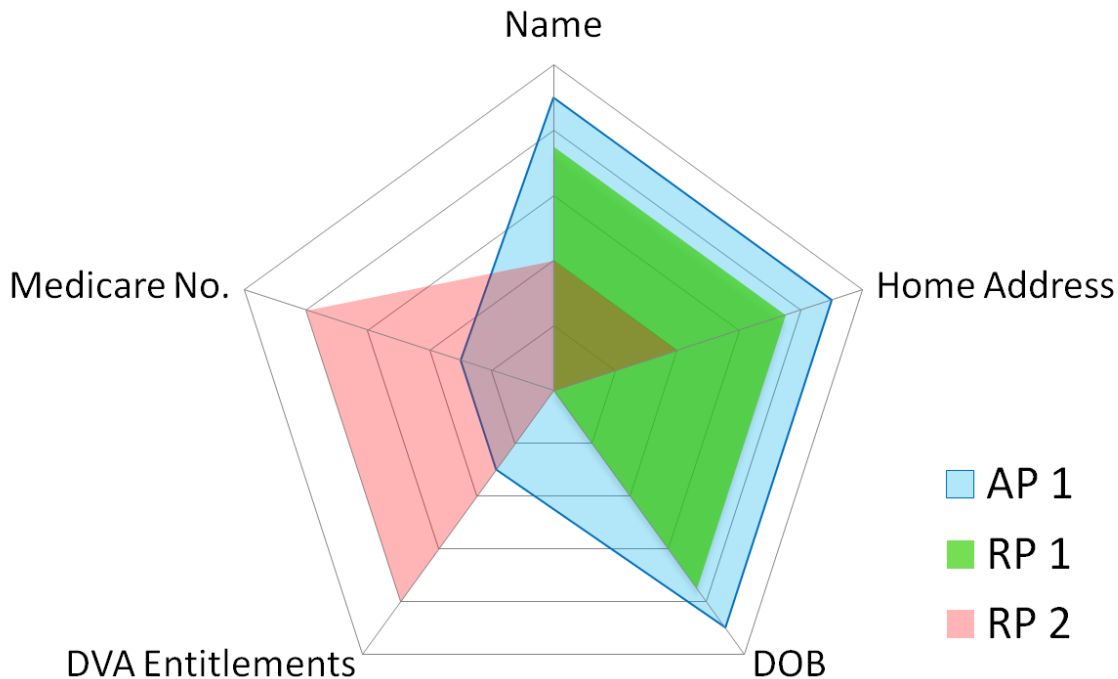
FIDO Identity & Authentication



The FIDO Alliance is sticking to its convictions and focusing strictly on the authentication level of the “Digital Identity Stack”. The realisation that identity can (and should) be separated from authentication resonates with my thesis that Digital Identities are evolved ensembles of attributes selected to manage particular risks.

Federated Attributes

A practical upshot of this new theoretical framework could be schemes that federate concrete attributes instead of abstract identities. The diagram shows how a basket of attributes furnished by one Attribute Provider can be mapped against the needs of different Relying Parties. “Identity” is multi-dimensional, and not one-dimensional as implied by the LOA model.



Why are things the way they are?
Because they got that way.



Thank you



Steve Wilson

+61 (0)414 488 851

steve@ConstellationR.com

Twitter: @steve_lockstep

<http://lockstep.com.au/blog>

www.ConstellationR.com

