# Why Isn’t Identity Easy?


## Stephen Wilson

**Founder & Managing Director, Lockstep Technologies**

**swilson@lockstep.com.au**

**lockstep.com.au**


Identiverse 2021 SWILSON Why Isnt Identity Easy (1.1) HANDOUTS.pptx

**JUNE 2021** | **#identiverse**

identiverse®

# “Digital Identity is easier done than said”

## UK Government lead on Identity Assurance, 2012.

*Around ten years ago, the U.K. government (amongst others) was ramping up efforts to cultivate a public-private digital identity ecosystem. Senior figures adopted an optimistic mantra, announcing the time had come, digital identity would be relatively easy and suggesting there was such pent-up demand that commercially sustainable identity supply was imminent.*

*At around the same time, I wrote a paper that critically reflected on the very opposite experience. Over 2000-2010 we had seen several large scale well-backed federated identity projects unexpectedly fail, including Cardspace, OpenID, Identrus and the Australian banks' Trust Centre. Verify GOV.UK too eventually sank despite its leaders' optimism. So why has digital identity been so difficult?*

# Identities Evolve

## Why federated identity is easier said than done

Stephen Wilson
Lockstep Consulting Pty Ltd, Australia
swilson@lockstep.com.au

*AusCERT 2011 Conference: "Overexposed" May 2011, Gold Coast, Australia*

### Abstract

Why does digital identity turn out to be such a hard problem? People are social animals with deep seated intuitions and conventions around identity, but exercising our identities online has been hugely problematic. In response to cyber fraud and the password plague, there has been a near universal acceptance of the idea of Federated Identity. All federated identity models start with the intuitively appealing premise that if an individual has already been identified by one service provider, then that identification should be made available to other services, to save time, streamline registration, reduce costs, and open up new business channels. It's a potent mix of supposed benefits, and yet strangely unachievable. True, we can now enjoy the convenience of logging onto multiple blogs and social networks with an unverified Twitter account, but higher risk services like banking, e-health and e-government have steadfastly resisted federation, maintaining their own identifiers and sovereign registration processes.

*While identity has been slow going, mobile technologies have turned out to be a rich platform for carrying and presenting secure copies (tokens) of payment accounts, boarding passes and even virtual hotel room keys. So why is this type of innovation relatively easy?*

# Digital Identity

Australia Card 1985-87

AU National Authn Authority 1998

*Identrus* 1998-2002

*Infocard* 2006-11

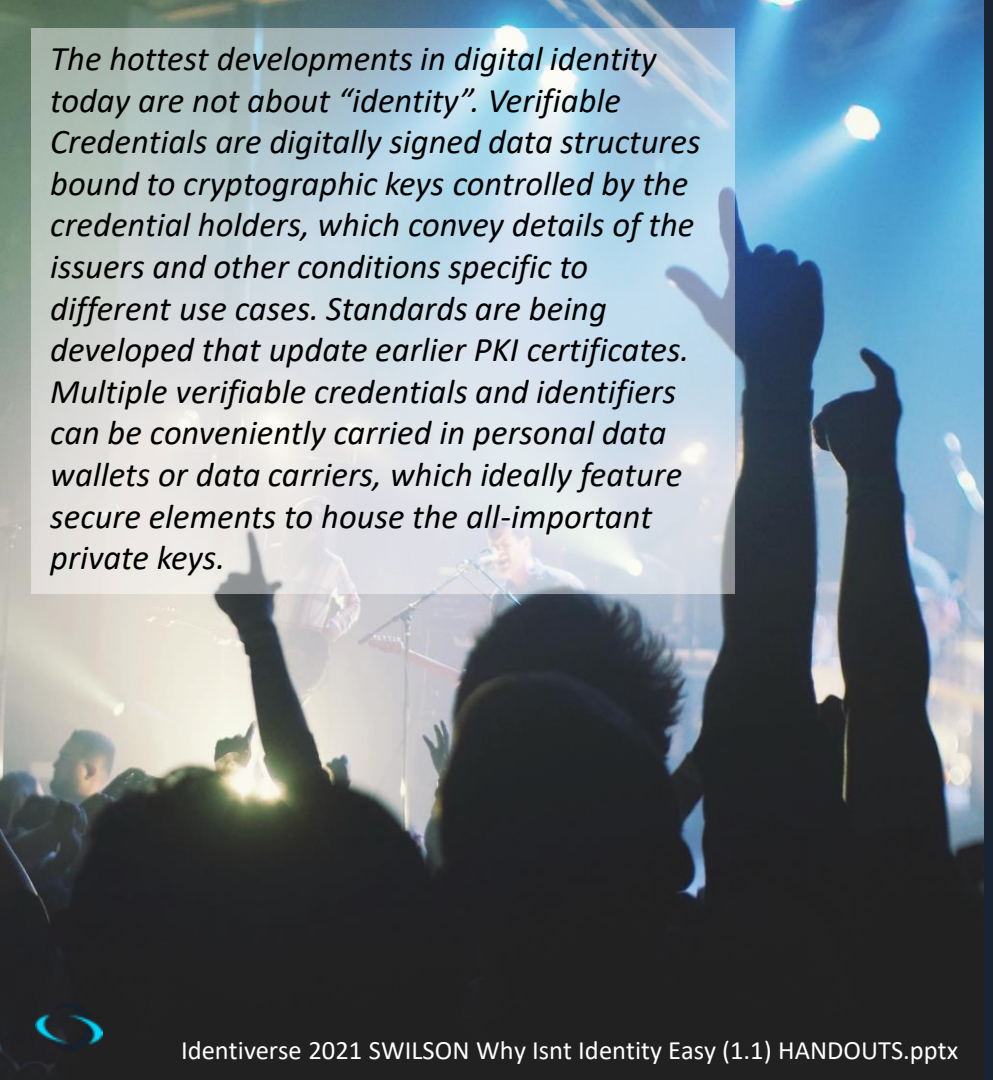
UK National ID 2006-10

US NSTIC 2009-16

UK Verify 2011-18

AU *TrustID*, TDIF 2014-??

*From the beginning of e-commerce, we have tended to complicate digital identity. Its relationship with "real" identity has never been clear and loosely defined metaphorical efforts like "electronic passports" have never fixed liability. The Anglophone (Five Eyes) countries have no tradition of National ID; occasional proposals have been roundly rejected by the public, which has poisoned most of the discourse of identity capability building. Private sector initiatives in banking and technology sectors (e.g. Identrus and Infocard) came and went. British and American efforts at grand public-private federations attracted very few Relying Parties (despite the urgency of better identity) and spawned no commercially sustainable identity businesses. Scandinavia and the Baltics have seemed successful with multi-purpose digital IDs but these are backed by specific legislation. A few free market identity frameworks remain in development in Australia and Canada. Progress has been disappointing and their futures remain uncertain.*



*The hottest developments in digital identity today are not about "identity". Verifiable Credentials are digitally signed data structures bound to cryptographic keys controlled by the credential holders, which convey details of the issuers and other conditions specific to different use cases. Standards are being developed that update earlier PKI certificates. Multiple verifiable credentials and identifiers can be conveniently carried in personal data wallets or data carriers, which ideally feature secure elements to house the all-important private keys.*

# What's hot?

- Verifiable Credentials
- Decentralised IDENTIFIERS
- Wallets (data carriers).

# “There’s no artifact called an ‘identity’ in SSI.”

Phil Windley, Founder & Chair,
Sovrin Foundation.

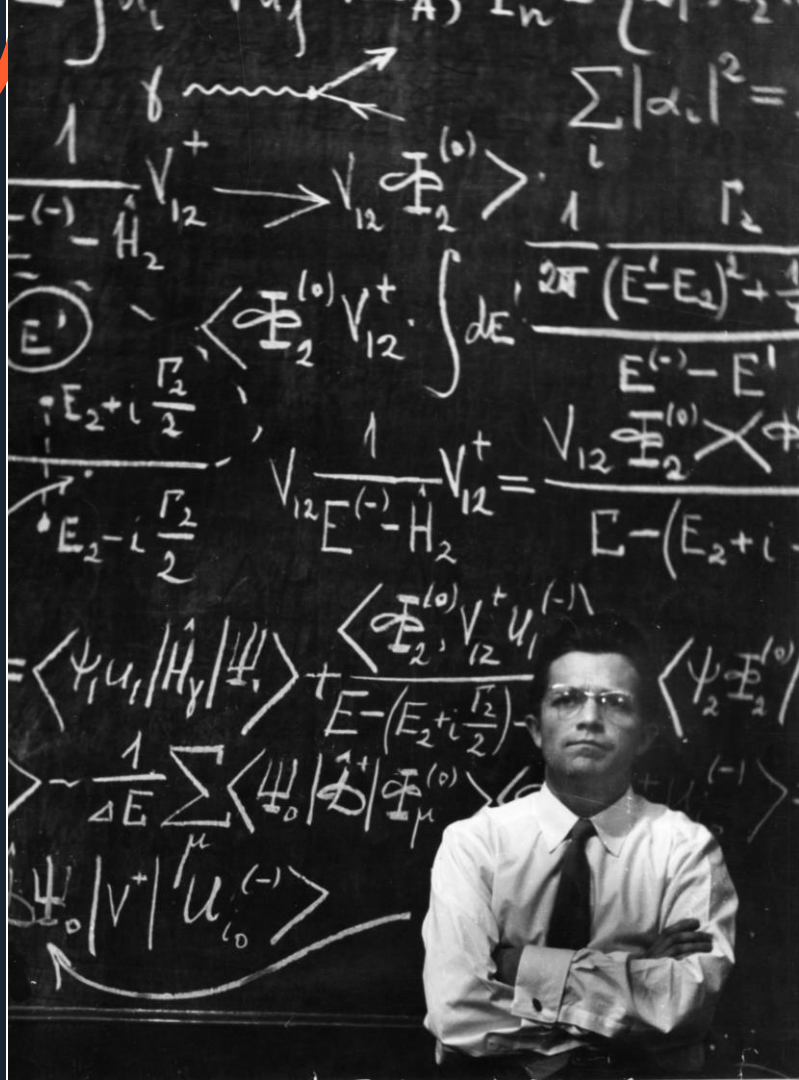
*The Self Sovereign Identity (SSI) movement has dominated the industry for several years, with a call to action to reclaim “ownership” of one’s identity in the face of mounting online exploitation and surveillance. It’s an understandable desire but can’t be literally true. SSI has cooled a little, with the language morphing towards better control of personal data flows. The focus now is on relationships and credentials, with new Verifiable Credential protocols that acknowledge the interests of issuing authorities and Relying Parties.*

*So what if we forgot about "identity" as such? We know from experience it's just too subjective. What if we focused instead on verifying objective pieces of information which are specific to each relationship or transaction?*

What do you need to know?

Where will you get the data?

How will you know if it's true?



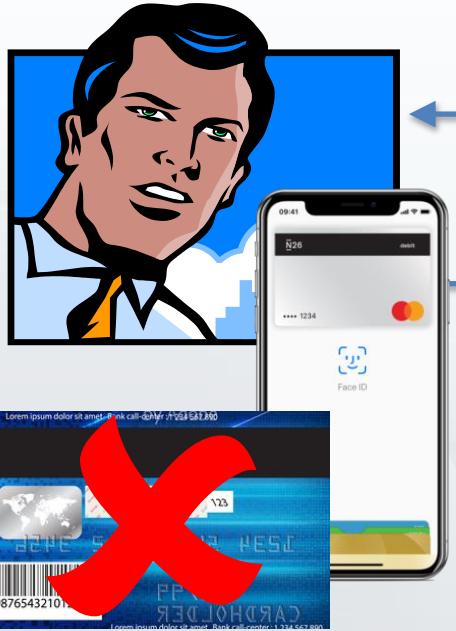
# What do you need to know?

*There are comprehensive "infostructures" already in place for verifying specific pieces of data about transacting parties. Some infostructures include hosted technology, relying party hardware and software, personal data carriers, standard contracts and liability arrangements, payment structures and an over-arching network business model that makes data verification sustainable. In Digital Identity these are popularly called "trust frameworks".*

*Consider the credit card system. Fundamentally it exists so that merchants can obtain account details from customers and verify those details to trigger settlement and billing.*

***The only data which the merchant needs to know in this context is the customer's card number.***

# Where will you get the data?



*What's your credit card number?*

4000 1234 5678 9010

***Where will the merchant get the card data?*** *For Card Present payments, it has to be from a genuine branded credit card. In the past, the merchant was expected to examine the card to check the branding and special security features like holograms. The card is a carrier of account data and metadata used to confirm validity. Nowadays, most merchant terminals will read data from a smart chip embedded in the card or in a suitable mobile device (under the covers, the chip and the terminal exchange digital signatures which confirm the data originated from a bank and hasn't been copied our counterfeited). Furthermore, scheme rules can forbid unapproved data carriers; in some markets for example, merchant terminals no longer accept magnetic stripe cards.*

# How will you know if it's true?

*What's your credit card number?*

4000 1234 5678 9010

*Cardholder account information is verified through high availability, high performance card processing infrastructure available worldwide and operated by banks and diverse service providers.*

Issuer

Card Scheme

Acquirer

# How will you know if it's true?

What's your credit card number?

4000 1234 5678 9010

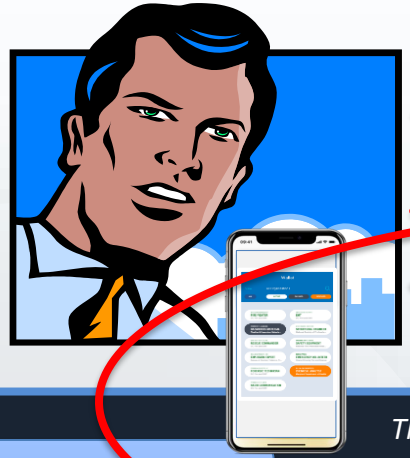
*The card schemes serve a two sided market, delivering cost-benefit to merchants and customers alike, with a sustainable "network business" model where reasonable fees flow to sustain the system.*

Issuer

Acquirer

Card Scheme

# Leverage an established business model

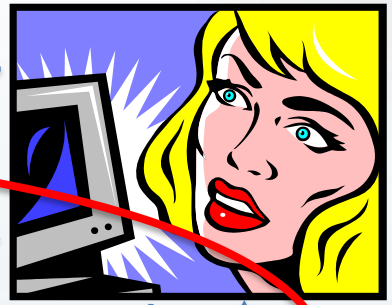


What is your X?

$

42

$



Data Issuers

$

*The holy grail in digital identity has been a business model in which reasonable fees are charged for "provision" and "consumption". Similarly, Open Banking and Open Data frameworks are trying to work out how to make the new markets commercially self-sustaining. Card payment network businesses seem to show the way to a verifiable data business model.*

*Verifiable Data Network Business*

$

Acquirers

# What do you need to show?

- Memberships & licences
- School grades
- Age
- Government IDs
- Health IDs
- Vaccination records …

*In digital life and work, we need to show things about ourselves, typically discrete pieces of important data, backed up by metadata that proves origin, Ts&Cs, regulatory commitments, consent and so on, depending on context. If we generalise from credit cards — including terminal, data carriers, standardised contracts and service providers — we could build truly global infostructure for verifying everything we routinely need to know.*

# Conclusion

We have made digital identity hard by solving for the wrong problem. Personal human identity is always going to be rich and relative and analog but the challenges in the digital domain boil down to trustable data. We know how to solve for data reliability, by blending cryptography and governance. Our industry has been evolving and shifting focus from identity through attributes to arrive now at Verifiable Credentials. Let's keep up the good work, let's be clear about where actual identity problems lie, and use our tools to build infostructure for verifiable data across cyberspace and the digital economy.