sezoo

DigiGov 2023

“The Verifiable Credentials of Trustworthy Government and their role in all our futures”

Why would this sentence (from the OECD draft recommendations on governance for digital identity) **trigger me?**

"Access to essential services across the public and private sectors and trust between individuals, businesses, and governments rely on being able to prove one's identity."

sezoo

Here’s my aim for this talk

I want to give a different perspective on **digital trust.**

One that is thought provoking and emphasises the critical role of government in digital trust.

[This means you]

sezoo

What might we mean by “digital trust”?

“Digital trust is individuals’ expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders’ interests and uphold societal expectations and values.” - World Economic Forum

"The confidence that individuals and businesses have in the security, privacy, and reliability of digital transactions and interactions." - Mapsted

“...a confident relationship in the unknown” - Rachel Botsman

Notes:

1. There is always some degree of “unknown”, if everything is known and certain, we don’t need trust
2. A decision to trust has many inputs, including: experience, context and choice
3. Trust is dynamic, it changes over time as we demonstrate trustworthiness (or a lack of it)

sezoo

Trust is essential to all human socio-economic interactions

The level of trust we need in any particular situation is shaped by context: our prior experience, the perceived risk and reward, available choice etc.

Everytime we choose to do, or not to do, something, trust is playing a part in the decision and is impacted by the remembered outcome.

sezoo

Four mistakes made too often in the context of digital trust

1) Over focusing on identity
2) Forgetting that trust is mutual
3) Assuming that people can and should always represent themselves online
4) Confusing digital presentation with verifiable presentation

sezoo

Mistake 1:
Over focusing on identity

In most cases the credentials that a person or organisation has are more important than their identity.

It is important that I am the legitimate holder of a valid driving licence when I drive a car. It isn't important that I am John Phillips.

It is important that my gas leak is fixed by a qualified, insured, plumber, not that her name is Jackie.

It's not **who** we are, but **what** we can do, our rights and capabilities, that are important.

Trustworthy digital identities are essential, but not always necessary, and we need more than one.

sezoo

Mistake 2: Forgetting that trust is mutual

Trust needs to be **mutual** to be **meaningful**

Remember you're a customer too, ask yourself why don't organisations (and government's) prove who they are in their interactions with you?

By not authenticating themselves, organisations condition people to behave badly ("trust me, I'm your bank/government…").

Organisations should authenticate themselves to the same level they demand of their customers.

sezoo

Mistake 3:
Assuming that people can and should always represent themselves online

We humans share the same story arc:

- We all start our lives as children dependent on others
- We become independent adults and some become carers for dependents (children and their parents)
- We become cared for and dependent on others
- We die [and are survived and our “estates” managed]

At any one time, a significant proportion of the population is dependent on others, and yet our online systems make little or no concession to this shared reality.

The solutions for this need to go way beyond WCAG: we need trustworthy digital ways for carers to prove their rights and duties for their dependents online (and in person) whenever and to whoever they need to prove this.

sezoo

Mistake 4:
Confusing digital presentation with verifiable presentation

Early “digitization” efforts took existing physical credentials and “digitized” them by making digital versions presentable on the screens of devices.

But no matter how fancy your hologram and active your animation, all visual trickery is too easy to fake in the era of GenAI.

And forcing a “call home” (to check the details with the issuer) to address this weakness creates a privacy issue.

Put simply, presenting (“showing”) a digital artefact to someone physically proves virtually nothing.

We need to use smarter cryptographic approaches to protect and verify digital artefacts in a privacy preserving way, **we can’t see cryptography.**

sezoo

How to avoid these mistakes with new trust models

sezoo

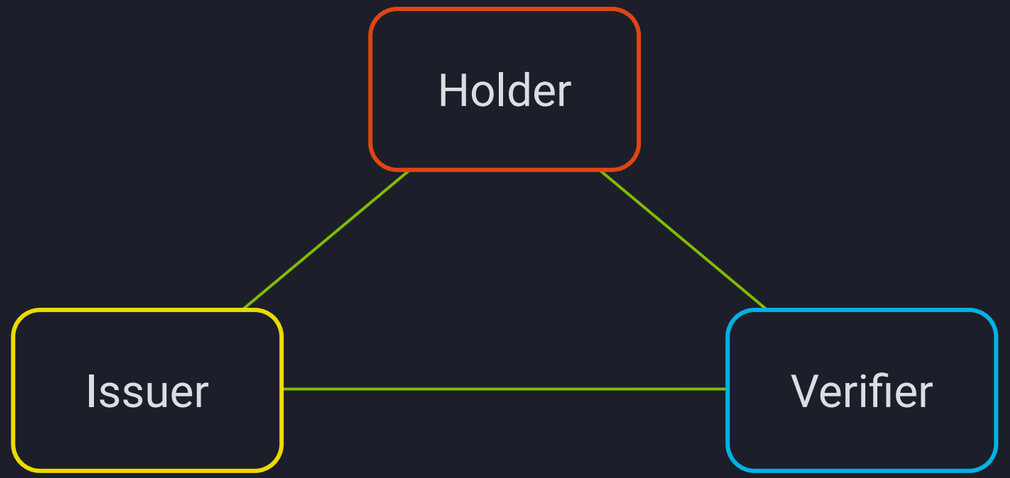
New trust models allow us to focus on **what**, not **who**

New models of trust, using technology like “verifiable credentials”, allow us to selectively prove things about ourselves that are relevant to a transaction: I am over 18, I have a driving licence, I am a qualified teacher, **without having to prove who we are** (unless that is critical to the transaction).

Let’s explore how…

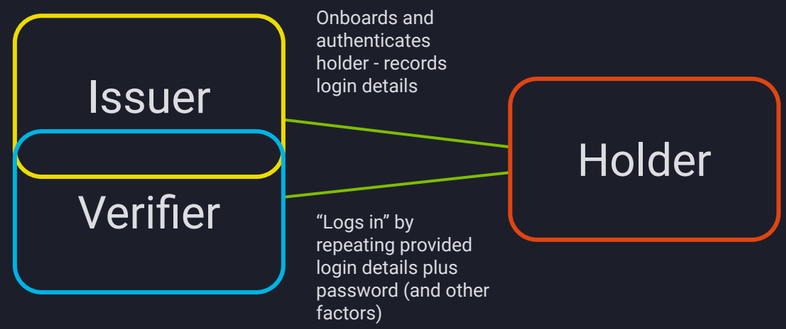
sezoo

Let’s use a simple framework of issuer, holder and verifier to explore the past, present, and future



sezoo

Traditional: Centralised



Same organisation is both issuer and verifier.

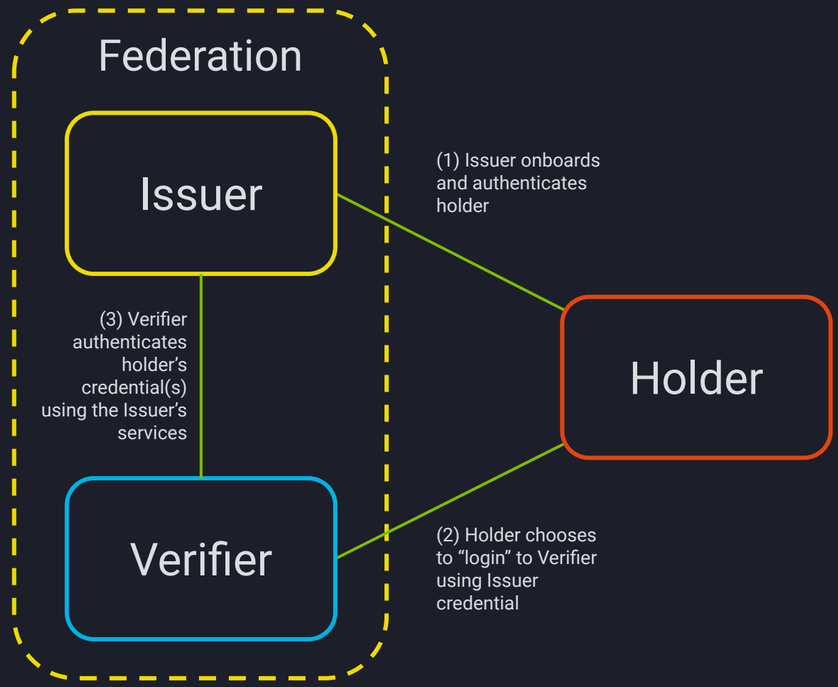
One organisation “holds” all the data about (and for) the holder. The holder accesses data about them by echoing back the authentication credential(s) given to them by the issuer (username/password etc.).

Most current IDAM systems work like this.

sezoo

Current and fading: Federated

["fading" is deliberately provocative, happy to discuss]



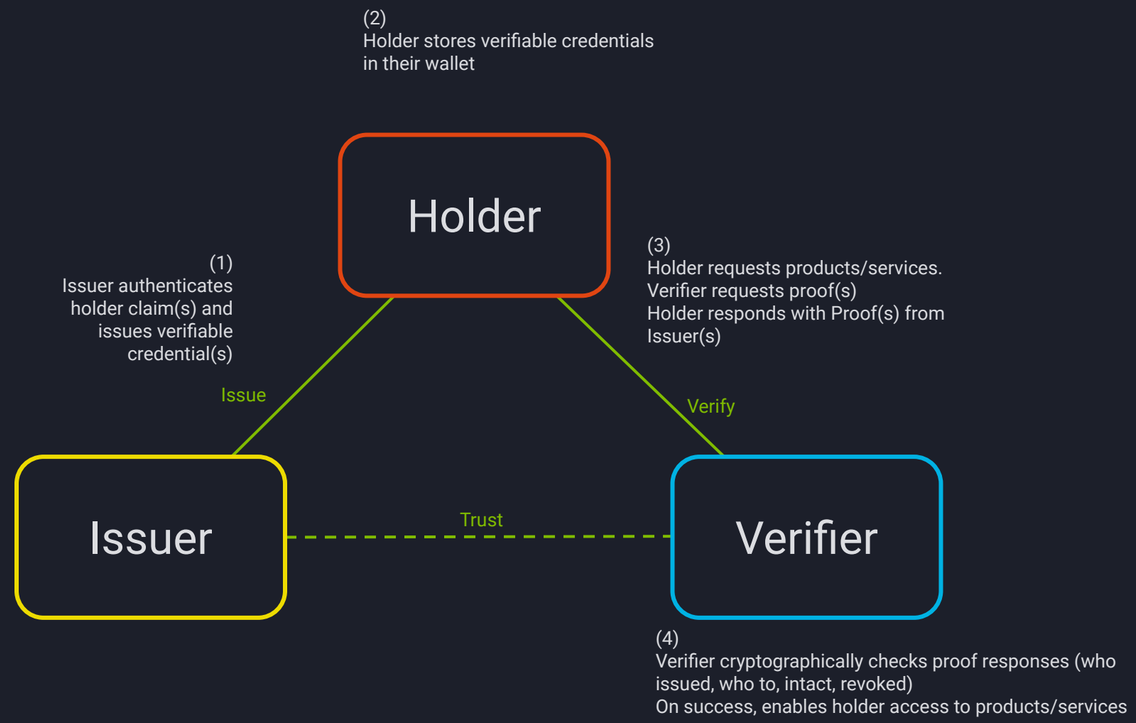
Issuer and Verifier are different organisations and part of the same federated framework. The Verifier 'trusts' the Issuer's identification and authentication services.

Verifier holds application specific data about the holder. Issuer holds "identity" (authentication) specific information about the holder.

The current TDIF architecture is like this but includes parties like "exchanges".

sezoo

Current and Emerging: **Decentralised**



Actually many centres of authority (trusted issuers) and “holder initiated decentralised verification” would be more accurate, but wordy.
Also **“decentralisation” ≠ “blockchain”** in this context - unless your implementation needs one.

No direct communication between verifier and issuer.

The Holder can have many credentials from many issuers and interact with many verifiers.

Credentials support any verifiable data, not just assertions of identifier(s).

sezoo

Trust depends not just on trustworthy data, but on trustworthy issuers (institutions)

We can use cryptography to prove who issued something, and whether it has been tampered with since being issued.

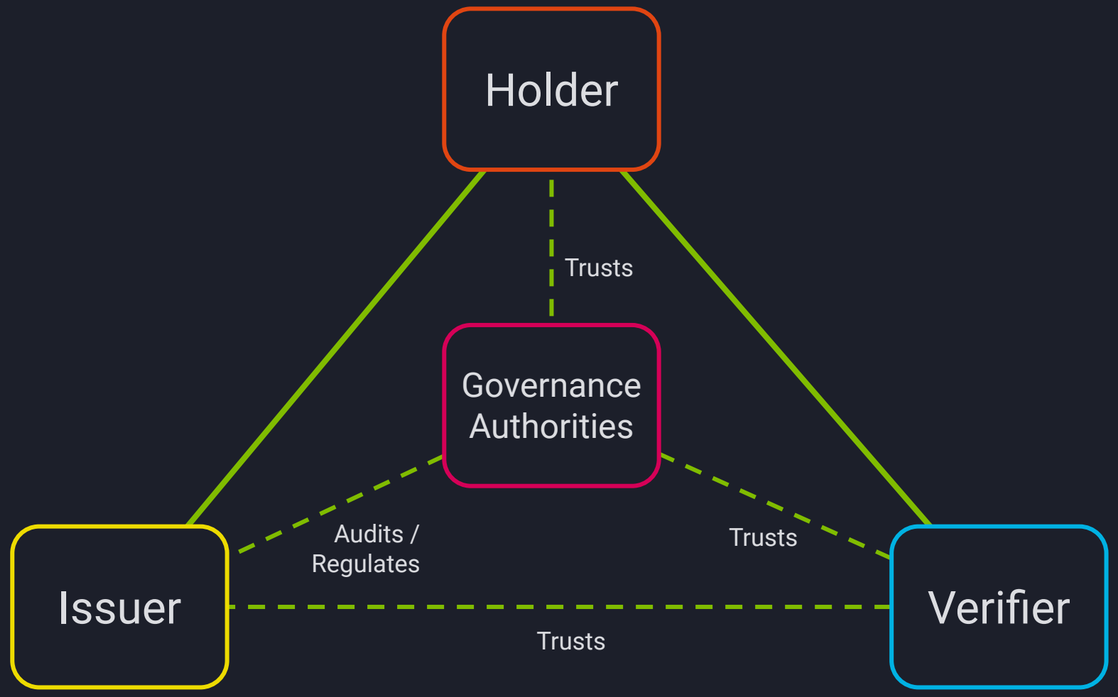
So we can trust that the data is what the data is, and that the issuer issued it, but whether we trust what the issuer issues depends on other factors.

Here we need additional sources of trust. We might ask, for example:

“how is the issuing organisation governed, under what regulations, and by who?”
(aka “can I trust them?”)

sezoo

Trustworthy systems require trustworthy, transparent governance



sezoo

Let’s get real:
Two world class
Australian government programs

sezoo

1) NSW DIVC Program

sezoo

NSW's world leading "Digital Identity **and** Verifiable Credentials" program

The distinction between "digital identity" and "verifiable credentials" is deliberate, functional **and** technical.

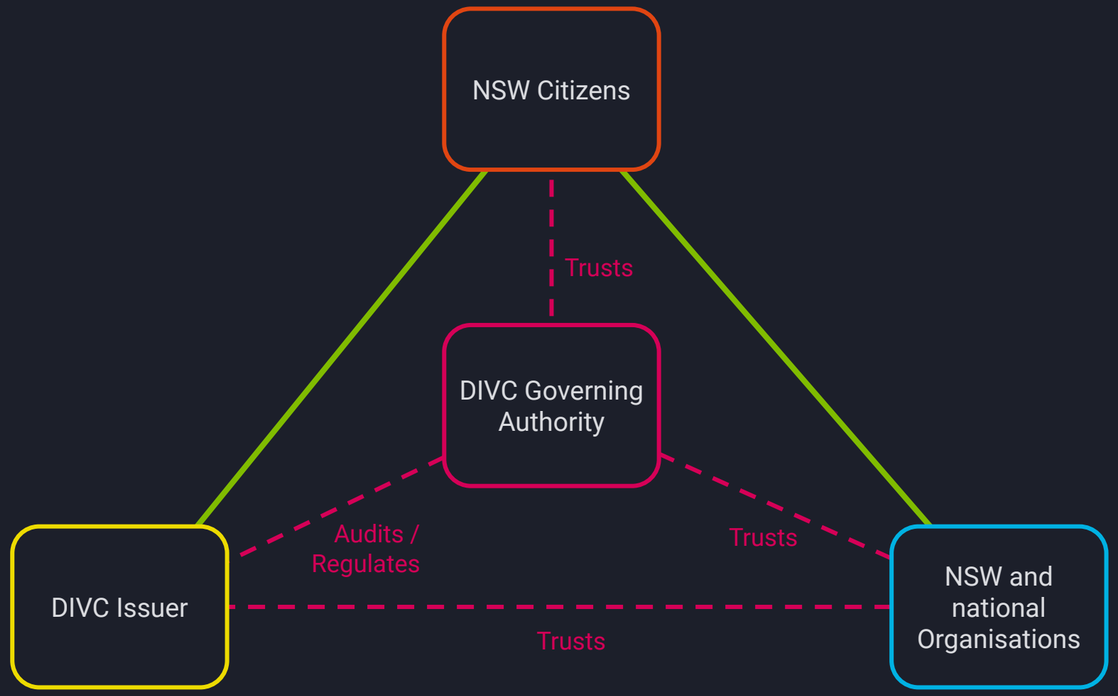
There are some specific established technical solutions for "digital identity" that the program seeks to leverage (such as NSW.ID and TDIF)

"Verifiable credentials" (credentials that we can cryptographical authenticate and check integrity) can be used to prove many (many) things from education, health, licences, employment, memberships etc. They can also be used to provide verifiable credentials about identity.

What the name recognises is the distinction between the process/function of "identification" (who), and the proof of the credentials that someone holds (what).

sezoo

In DIVC, NSW is an issuer, a governing authority, and a Verifiers



sezoo

A self-contained system makes for an easier (but not trivial) initial business case

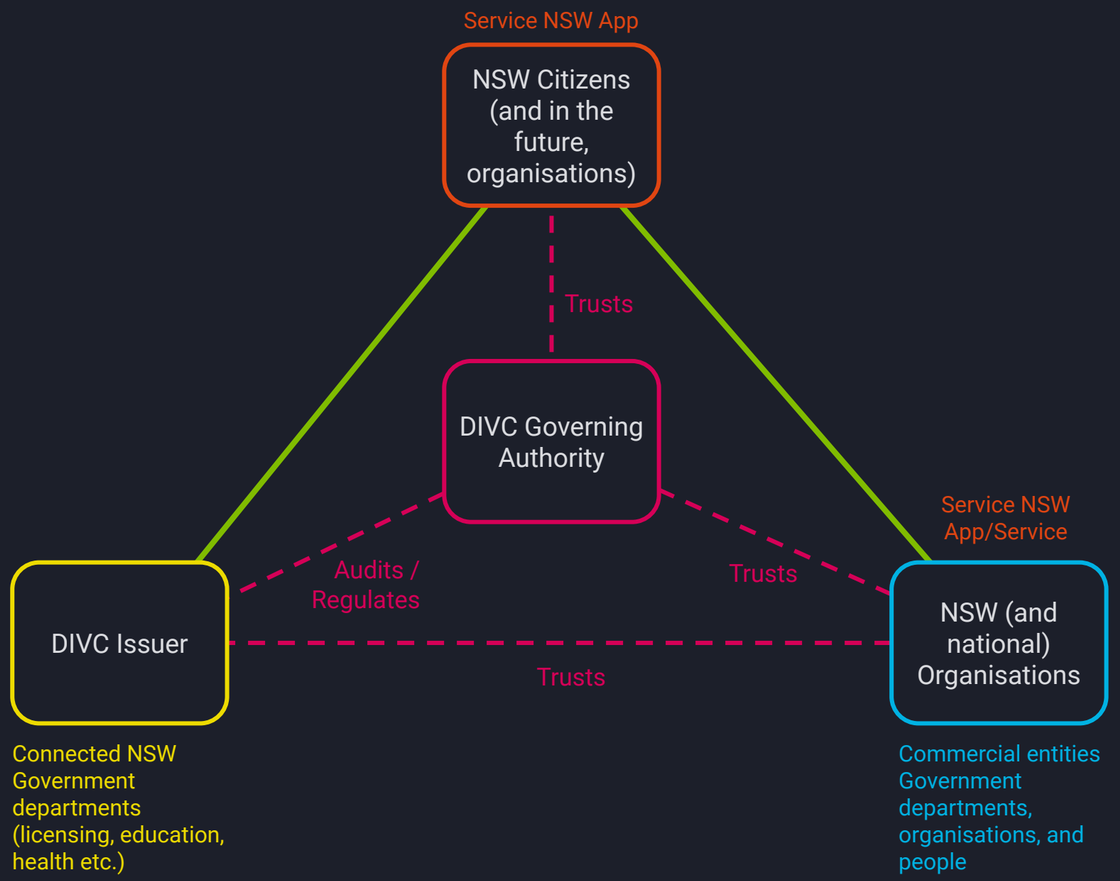
The DIVC business case includes benefits such as improved service access and efficiency (online accessibility and time saved), as well as improved security and privacy.

There are benefits identified for citizens and organisations, as well as cost savings for government.

And the expectation is that the platform will enable additional offerings and benefits beyond existing government services.

sezoo

The DIVC program creates a **digital trust framework** for people and organisations in NSW



sezoo

A few of the key points of the DIVC program

1. Benefits for customers, government and business
2. Creates a digital identity system for NSW citizens designed to allow future interoperability with Federal systems
3. Enables existing government authorities (health, education, sport, transport etc) to issue verifiable credentials through Service NSW according to their existing governance frameworks
4. Builds on existing (positive) NSW user experience of the Service NSW App by adding digital wallet capability.
5. Uses open-standards for verifiable credential data issuance, storage, presentation and verification (OIDC, DIDWeb, W3C VC etc.)
6. Could support other standards (e.g. ISO mDL)

sezoo

2) The National Digital Birth Certificate Program

sezoo

The Australian national digital birth certificate program

A national program, run by the NSW Department of Customer Services, is entering initial trials in NSW of a **digital birth certificate**.

With successful trials, and with agreements with other states, people born in Australia (and parents of people born in Australia) will be able to use a digital birth certificate for themselves and their dependents.

This will be genuinely transformational!

Why would I say that?

sezoo

A birth certificate is a foundational document

Birth certificates are proof of the civil registration of a person. They enable individuals to participate in family, cultural, social, and economic activities and confirm their right to access government services and benefits.

Birth Certificates have recognised legal significance unlike synthetic “digital IDs”

sezoo

Physical birth certificates have limitations and risks

- Perishable
- Easily lost
- Hard to share (certified copy process)
- Hard to verify (just because you have a birth certificate in your possession, doesn’t mean you are the subject of the birth certificate)
- Can be fought over and access can be denied to vulnerable people.

sezoo

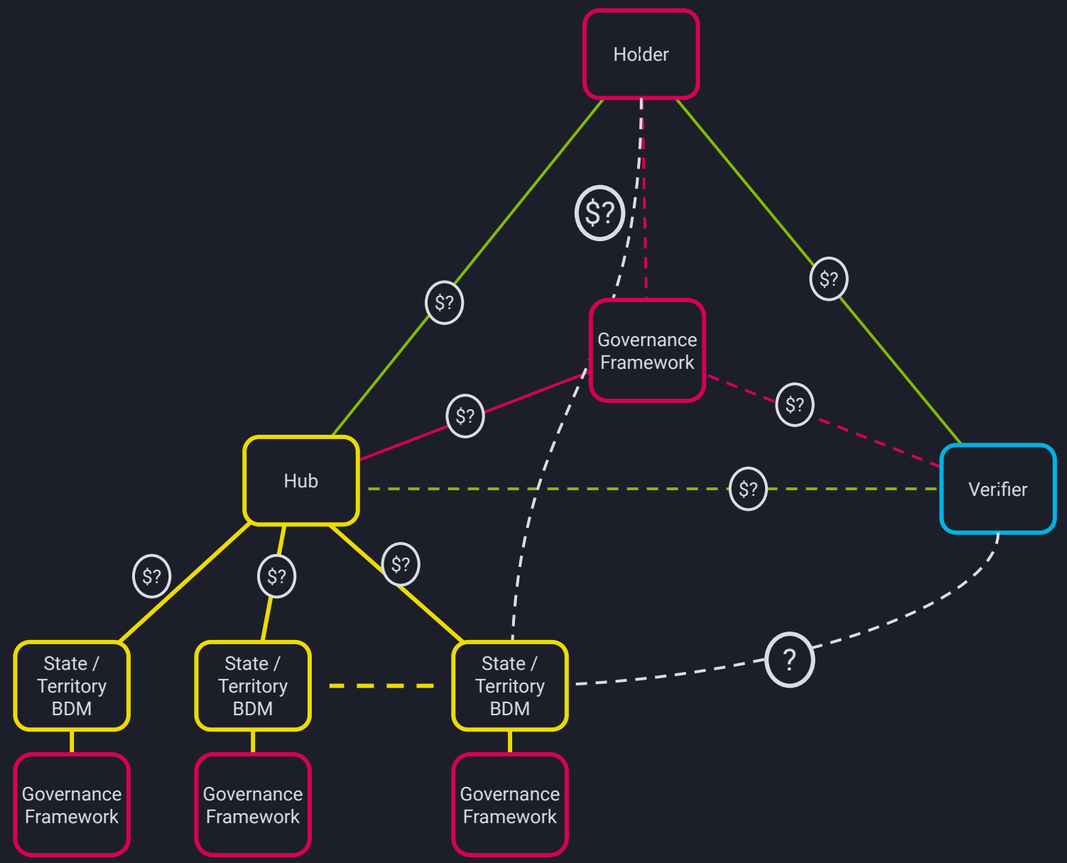
[Verifiable] Digital Birth Certificates will be game changing

The first trials will use digitally (PKI) signed PDF versions of birth certificates, next comes Verifiable Credential versions. This means that…

- Holders can use selective disclosure (parts of the certificate), the whole certificate, or that they have a certificate (zero knowledge proof).
- Verifiers can ask for just the data they need (not the whole thing) and cryptographically check the responses they receive.
- Issuers (Registrars) can reduce distribution costs and build new value models.
- The digital birth certificate **itself** is verifiable, we don’t need to verify it and produce another (synthetic) identifier - potentially disruptive.

sezoo

National Digital Birth Certificates will require a multi-party, multi-jurisdiction, multi-governance system



sezoo

Making this work means that we have to consider new challenges

- How does governance work for the new hub entity that orchestrates authentication of people and issuance of digital birth certificates? How do we tell if people have the right to access birth certificates other than their own?
- How do we recognise the accountability and responsibility of the State and Territory Registrars (who create the records), and the shared “Hub”?
- How do we govern the commercial and legal relationships between each of the parties?
- What is the appropriate cost/fee model amongst registrars?
- What should the commercial model be for all participants (issuers, holders and verifiers)?

sezoo

A few closing thoughts

sezoo

Towards Mutual Verifiable Credential Recognition

(Mutual Recognition, Credit for Prior Learning, Registered Occupations, Professional Qualifications etc.)

If someone can prove that a (trusted) authority has issued them a credential (as a teacher say), then other authorities can choose to allow verifiers (schools in our example) in their jurisdiction to recognise these credentials.

However, “mutual recognition” requires more than just data verification and alignment, it requires cross-jurisdictional recognition of the meaning and value of credentials. It requires registered occupation rule alignment and/or gap identification.

Technology such as Verifiable Credentials with published schema, and executable (code) rules, can make things possible, but Governments need to work to make interoperability work.

sezoo

Towards Antifragile systems

Our cyber threats mean that we can't **just** focus on making things robust, that can make us fragile to what happens **when** things fail…

What if a critical institution (such as a government body or a bank) were to be unavailable for several days during which its customers needed support? How do they prove to other providers that they are customers?

We can't rely upon any system that requires an unavailable entity to authenticate its customers (centralised and federated won't work)

System and service **resilience** can be developed by allowing credentials to be verified and used **decentrally**, even if the issuer isn't available

Governments (and their citizens) need antifragile systems.

sezoo

Towards Guardianship

At the beginning of this presentation I referred to the gap in our current digital designs where people who care for others, or who represent others (people or organisations) **cannot** prove their rights and duties online.

We see verifiable “Guardianship Credentials” as a way of proving that someone has been duly recognised by an authority and issued a credential stating their duties and responsibilities to another (their child, parent, family member or other dependent).

Government authorised institutions define the regulations and issuing authorities for guardianship. Guardianship credentials can be an “and” to existing paper processes.

sezoo

Towards Verifiable Organisations and their Verifiable Delegates

GLEIF (the Global Legal Entity Identity Foundation) governs the issuance of LEIs (Legal Entity Identifiers) and recently released a “verifiable Legal Entity Identifier”, a vLEI.

vLEIs are verifiable credentials that enable organisations to prove who they are in their interactions with other organisations, and who their authorised officials are (and their roles).

Further, vLEIs (and VCs in general) will also enable improved provenance and trust for things like supply chains and cross border trade (see UN/CEFACT whitepaper)

Government has a significant role to play in the governance of these systems. They are the originating issuers of business registrations upon which LEIs and vLEIs rely.

sezoo

Towards Verifiable Content in the age of GenAI

One of the problems exercising many minds at the moment is how we will tell truth from untruth or “alternative truth” in a future with generative AI able to create vast volumes of deeply believable content.

One of the answers is building on the work of organisations like Content Provenance and Authenticity (C2PA). Using technology like Verifiable Credentials, we enable producers of content to sign their content and hence enable verification of who created the content and that it hasn’t been tampered with. Doesn’t mean it’s true, does mean that we know who created it.

Not all online content can or should be signed (think whistleblowers and autocratic regime opposers), but we can choose whether we trust unsigned content or not.

Protecting citizens from misinformation is increasingly important for all governments.

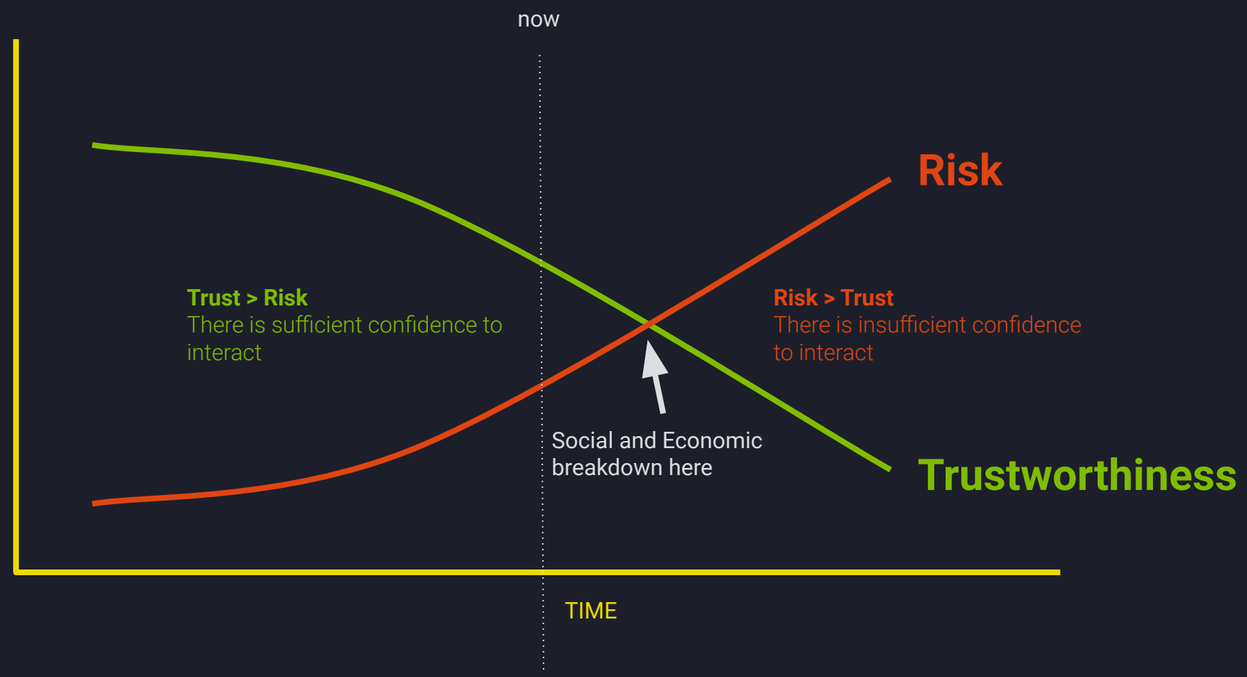
sezoo

Sanity Check: Technology on its own is never the solution, there is always real human work to do

- Trust is a universal, human, need: we need “humanity centred” and ethically based thinking
- Interoperability demands that we build with current standards, and that we expect them to evolve and change (W3C, ISO, OIDC, DIF, IETF)
- We need verifiable data **and** verifiable governance
- We need wallet standards for multiple data and presentation formats, Europe’s EIDAS large scale pilots may help here. [We’re wary of the emerging “wallet wars” and the global digital deities dictating choices]
- We expect State based “Service Apps” to be augmented under the covers with wallet capabilities
- We need to think about now **and** long next (years and decades, not weeks and months) - how might my digital driving licence be designed to last 10 years?
- We need to be creative and pragmatic about the new challenges, opportunities and socio-economic models ahead

sezoo

Finally…
IF trust **is** crumbling [1], **and** risks are increasing, **and** both trends are digitally accelerated, **then** we have a clear and present problem…

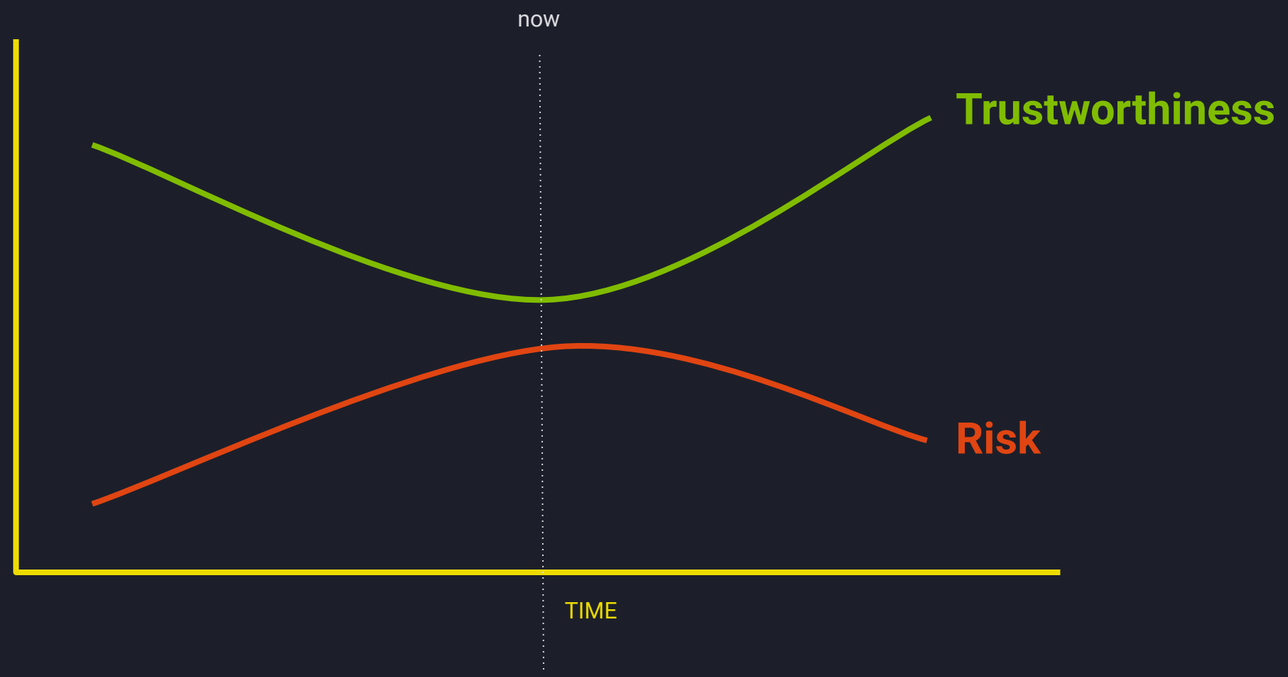


[1] Australian Government re-enters the realm of 'distrust' - Edelman Trust Barometer Report, 2023

sezoo

So we need to reverse this trend.

Government has a critical role in helping create a more trustworthy future.
This means you



sezoo

Thank you.

Questions?

John Phillips
Sezoo Co-Founder

E: john@sezoo.digital
L:
https://www.linkedin.com/in/11dot2/
T: https://twitter.com/11dot2John

sezoo

Some of the sources that influenced this presentation

Kwame Anthony Appiah “The Ethics of Identity” (ISBN 978-0691130286)

Rachel Bostsman “Who Can You Trust?” (ISBN 978-1541773677)

Joe Macleod “Ends” (ISBN 978-9163936445)

Amartya Sen “Identity & Violence” (ISBN 978-0393329292)

Elizabeth M. Renieris “Beyond Data” (ISBN 978-9780262373425)

Shoshana Zuboff “The Age of Surveillance Capitalism” (ISBN 978-1610395694)

World Economic Forum:
- Reimagining Digital ID, Insight Report, June 2023
- Earning Digital Trust: Decision-Making for Trustworthy Technologies
- The Global Risks Report 2023 - 18th Edition

Trust over IP: https://trustoverip.org/

Decentralized Identity Foundation: https://identity.foundation/

Gallup: https://www.gallup.com/394472/indicator-leadership-approval-trust-institutions.aspx

OECD: https://www.oecd.org/governance/trust-in-government/

Edelman Trust Barometer 2023: https://www.edelman.com.au/trust/2023/trust-barometer

GLEIF: https://www.gleif.org/en

UNECE: https://unece.org/sites/default/files/2022-07/WhitePaper_VerifiableCredentials-CBT.pdf

SOVRIN Foundation: https://sovrin.org/a-deeper-understanding-of-implementing-guardianship/

UK Department of Justice: https://mojdigital.blog.gov.uk/2022/05/06/designing-for-a-relationship-not-a-user/

sezoo

sezoo

Sezoo is an independent advisory/consulting practice whose mission is to "radically improve trust in digital interactions for the benefit of all".

Sezoo acknowledges the Traditional Owners of the country throughout Australia and their continuing connection to land, sea and community. We pay our respects to them, their cultures and to Elders past, present and emerging.