



Digital Identities through a Techno-Legal Lens

Joseph Hilsberg¹, Hayton Lam¹, Minghao Cai¹, Sushmita Ruj¹, Helen Paik¹, Asif Gill², Susanne Lloyd-Jones²

¹ University of New South Wales ² University of Technology Sydney



ABSTRACT

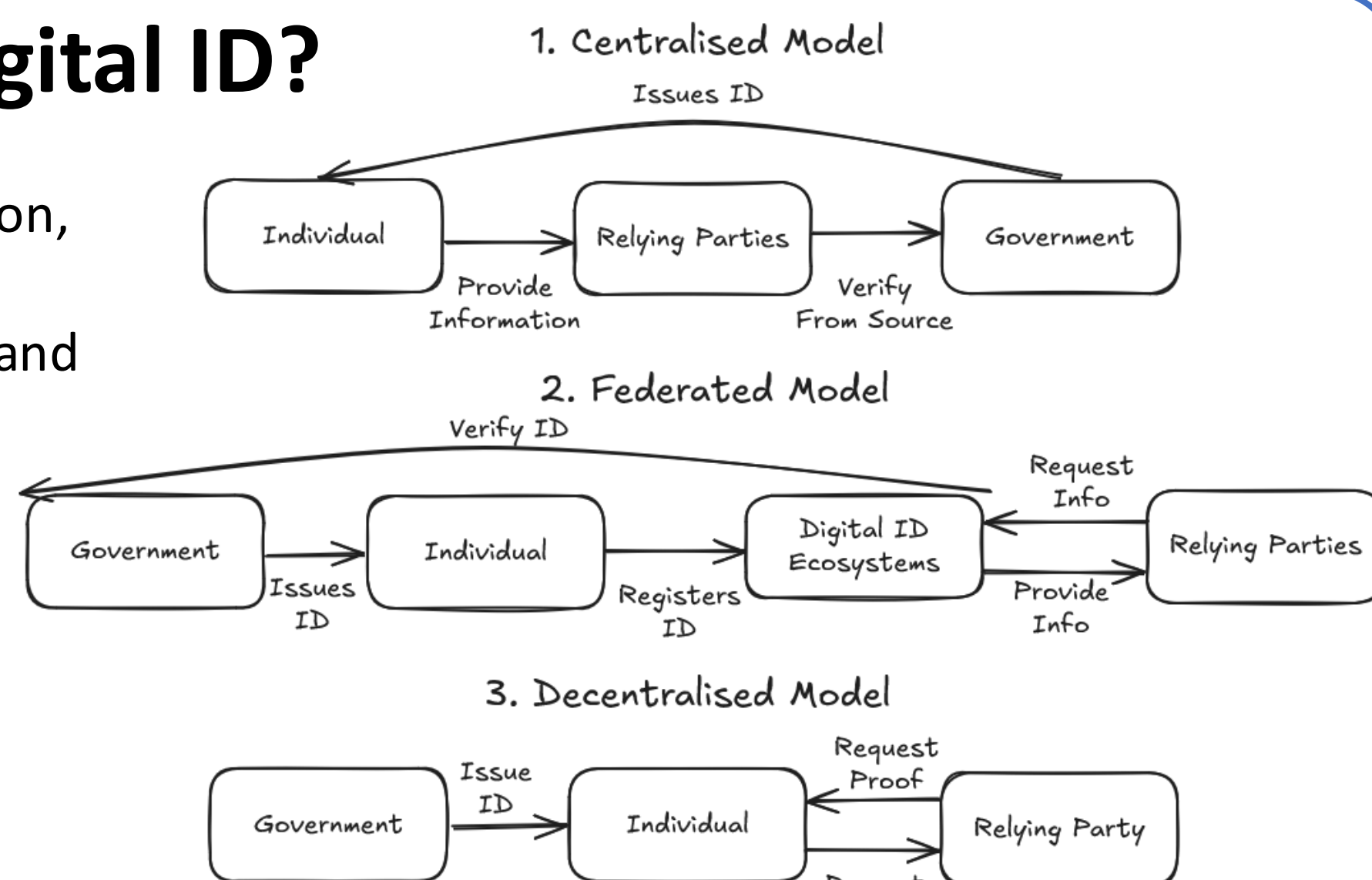
In 2024, Australia passed the Digital ID Act. But what is a digital identity and why is it important? This research explores the concept of digital identities, the tools and techniques to construct digital identities and legal requirements. It discusses various digital identity frameworks around the world and their relationship with the Australian Digital ID framework. It concludes with the road ahead in this space

OVERVIEW OF DIGITAL ID

What is Digital ID?

The digital representation of an individual, organisation, or entity (e.g. AI agents) in the online world, encompassing a collection of attributes, credentials, and data that uniquely identifies them across digital platforms/services.

Digital identity systems can be categorized into three primary models based on how data is managed, controlled, and shared. Each has distinct advantages, drawbacks, and use cases.



Why Use Digital ID?

Efficiency: Streamlined services can cut errors and save costs.

Government Leadership: In 2025, governments lead with mobile solutions like EU's EUDI, empowering citizens through standardized, accessible systems.

Integratable: Seamless integration into apps for effortless banking, healthcare, e-gov access etc.

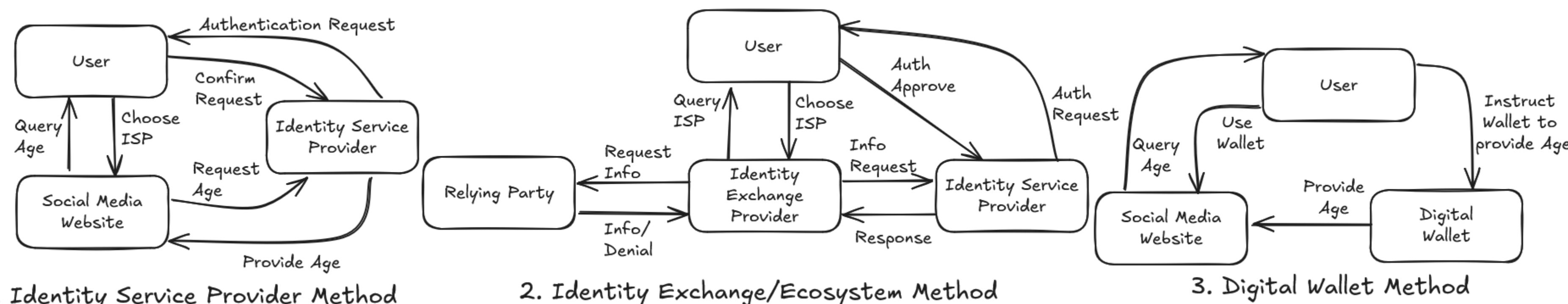
Secure: Leverage biometrics, encryption, and zero-knowledge proofs to combat fraud, deepfakes, and breaches effectively.

Example Use Case: Verifying Individual's Age

One commonly explored use case for Digital ID is the verification of an individual's age. This can be in many virtual and physical contexts:

- Entering bars
- Verifying age for restricted content or transactions

The figures to the right illustrate 3 forms of Digital ID interactions in the context of visiting a social media website for 16+ individuals only.



DIGITAL ID AS A FRAMEWORK

Entities & Desirable Properties

Issuers – Issuers create credentials by making verified claims about subjects and cryptographically signing those claims.

Holders – Holders possess credentials and control their presentation.

Verifiers – Verifiers receive presentations and validate them to make trust decisions

Correctness – Ensures the system functions accurately

Unforgeability – Prevents unauthorized creation or alteration of credentials

Unlinkability – Protects user privacy by preventing the linking of multiple credential presentations to the same individual across different contexts.

Issuer Hiding – Conceals the identity of the credential issuer from verifiers

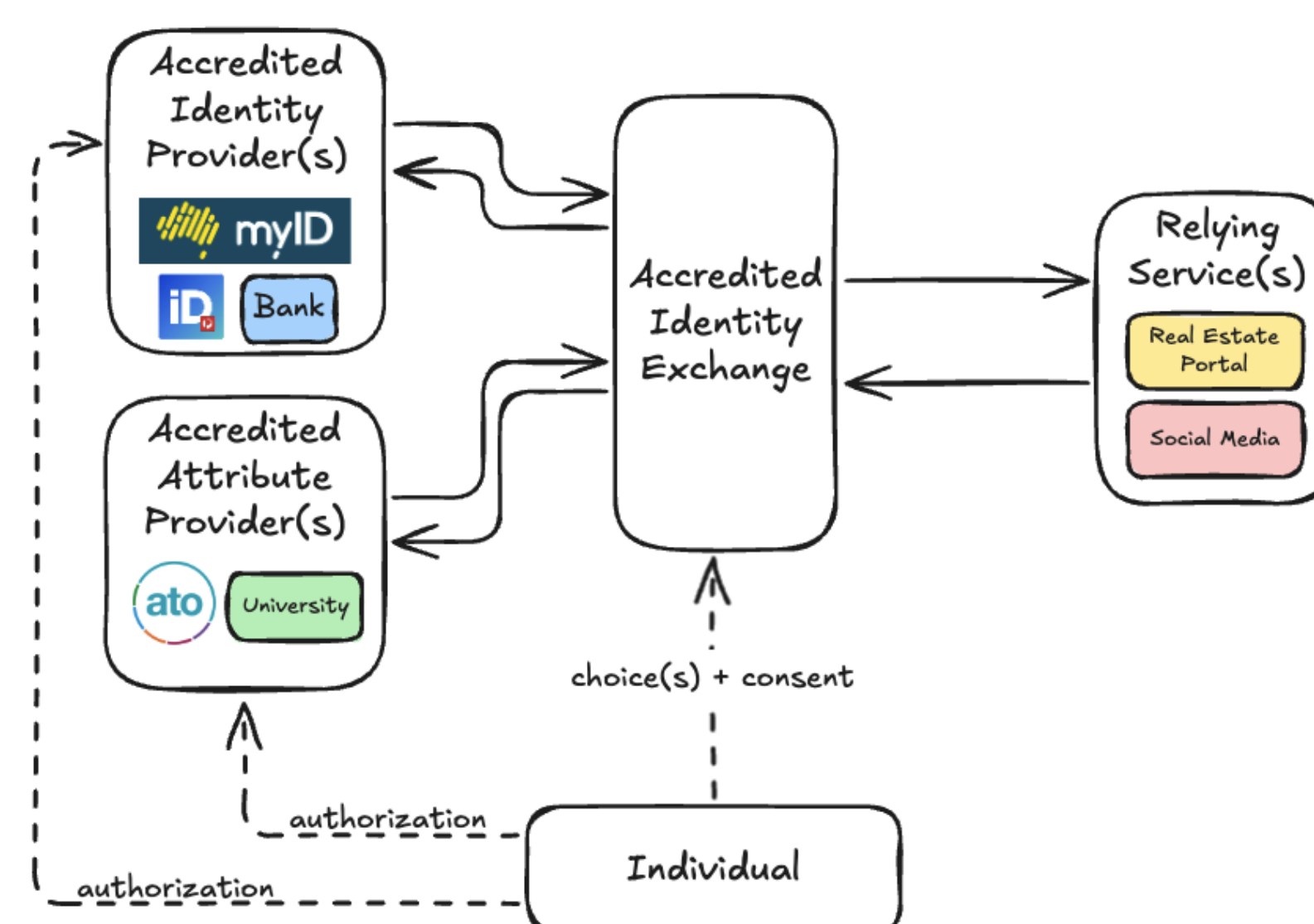
Selective Disclosure – Allows users to reveal only specific attributes from a credential without exposing the entire set of information

Revocation – Enables the invalidation of credentials when necessary

Australia's Digital ID Framework

In AGDIS/TDIF, authentication and presentation flow involves 2 separate instances of the OpenID Connect (OIDC) protocol:

- Relying Party to Identity Exchange
- Identity Exchange to ID/Attribute Provider(s)



Tools and Techniques

The construction of digital signatures relies on public-key cryptography, where a private key is used for signing and a corresponding public key for verification. Widely deployed constructions include **RSA Signatures**, **ECDSA** and **EdDSA**.

"Anonymous Credentials" are capable of being formed by utilising ZKP based systems like **CL-signatures** and **BBS/BBS+**. Major drawbacks include limited flexibility and facing deployment barriers (Cryptography support from on-device Secure Element Hardware).

Increasingly popular user-centric DID systems leverage existing credentials for enhanced privacy via ZKPs (**zkSNARKs**, **zkSTARKs**), featuring **Groth16** (succinct), **PLONK** (universal), and Google's **Ligero** (hash-based in Longfellow-ZK).

Comparisons Around the World

Country/Region	Digital ID Framework Type	Key Features
Australia	Federated	Australia's <i>Digital ID</i> regime is a federated system, encouraging multiple digital identity ecosystems to co-exist and interoperable interact with each other. Any participant of the regime must meet certain accreditation requirements for operational and cyber security, alongside any other system rules implemented by the identity exchange provider administering a system.
European Union	Federated-Decentralised	The new eIDAS 2.0 regulation now mandates that all member States should create digital ID systems which are primarily decentralised, with digital wallets permitting maximum citizen control over credentials. However, the EU 'digital ID regime' itself is considered federated, as each Member State is permitted to create their own system, provided it meets general data security and other technical standards.
India	Centralised	Aadhaar is a digital identification system that focuses on a 12-digit number issued to every individual. It is tied in with demographic information, biometrics (irises and fingerprints) and requires OTP verification from a mobile device (where biometrics is not available).
Estonia	Centralised-Decentralised	Estonia is in an odd position - while it should be taxonomically be centralised, as its system revolves around an 11-digit personal number issued to every system, and is the basis for their digital ID, it utilises a decentralised storage system, where different databases store different relevant information, and required information is accessed via a blockchain-based data exchange layer known as 'X-road'.
Denmark, Finland, Norway, Sweden	Centralised-Federated	These countries have a semi-federated system whereby banks are providers of identity services, which are often then tied-back to a central management or exchange network operated by the government.

Conclusion

Australia's digital identity regime is primarily enforced by regulatory safeguards. Other decentralized frameworks such as the EU have focused on digital wallet approaches which promote greater self-sovereignty. This research will continue explore the following questions as it progresses:

- Should one framework type be preferred over another?
- How can global and unique framework types become interoperable? Is there need for international standards or an overarching framework?
- What are the limitations of Australia's Digital Identity System, and how can we overcome these?