Provision IT Pty Ltd

Submission:

The Proposed Australian Digital ID Legislation and the Arguments for a Decentralised Self-Sovereign Digital ID Regime

Date: 8/10/2023

Key details

[redacted]

Contact details

[redacted]

Website	http://provisionit.com.au/

Executive Summary

The Internet was built without a way of knowing who and what is connecting to one another. Decentralised Self-Sovereign Digital ID is the best identity and access management system for the digital ecosystem, providing ownership, control and agency over a Peer’s verifiable credentials. The federated identity regime put forward in the Federal Government’s proposed Digital ID legislation is not in the best interests of the Australian public and should not be passed and implemented by the Australian Parliament. Rather than “top-down” decision-making by the Federal Government and other “vested” interests, only honest and genuine public-private consultation can deliver a decentralised identity-based infrastructure required for the emerging hyper-connected digital ecosystem of the 21st Century and beyond.

What is a Decentralised Self-Sovereign Digital ID Technology?

1. Safely managing digital identities online is a technical challenge – identity is not really about "identity" per se, but how to manage verifiable credentials (or decentralised identifiers) pertaining to identity in the digital realm.

2. Digital identity is the data available online about a peer, while Decentralised Digital Identity ("DDI") is identity management that allows people to control their own digital identity, without reference to a specific identity service provider.

3. Self-Sovereign Identity ("SSI") is an approach to DDI providing for ownership, control and agency over all identity data at the edges of digital networks, comprising private / public-key technology, general-purpose digital wallets / agents that are accessed via private keys, digital verifiable credentials and digital connections (without the need for an intermediate service provider or proprietary network) – SSI is the Internet for Identity, which allows for autonomous and independent self-determination.

4. With the proliferation of digital services and an expansion of the creative digital economy in Australia, centralised (or account-based identity, "lent" to the user, via a username and password) or federated (via identity service providers and "single sign-on") models for digital identity management are inefficient and vulnerable to cyber-attacks, thereby being unsuitable for the emerging hyper-connected digital ecosystem, where not only people and other legal entities need to prove who they are, but so too billions of Internet-connected devices.

5. SSI allows peers to collect verified credentials about themselves in a portable digital wallet (such as passports and driver's licences), where the peer controls what verifiable credentials are shared from that digital wallet to many requesting third parties via the "trust triangle" of Issuer, Holder and Verifier – peers only allow access to those credentials required to close-out particular transactions across multiple identity management systems using a single set of access credentials.

6. "Blockchain" technology (or distributed ledger technology associated with Web3 development) and / or decentralised verifiable data registries will be used to store the verifiable credentials that are referred to by verifiers.

7. Provision IT Pty Ltd ("Provision IT") has commenced development of a prototype trust-based technology (the SSI stack) and associated SSI governance framework, enabling peers of digital systems greater control over their verifiable credentials – Provision IT's approach to digital identity will be simple, secure and mobile, with potential to bind the identity holder to verifiable credentials via biometric templates stored in a peer's digital ID. Provision IT aims to integrate this technology with the company's decentralised finance technology.

8. Preventing the widespread adoption of SSI is the disparate digital ID schemes established by national Governments around the world.

The Business Case for Decentralised Self-Sovereign Digital ID Technology

9. Decentralised SSI digital ID technology has no single point of failure, as connections are P2P and do not rely upon centralised systems, which generally track "user" interactions.

10. The key benefits of SSI are as follows:

Peer Control: Peers control access to their verifiable credentials, determining what verifiable credentials are shared, with whom, and for what purpose.

Convenience: Decentralisation simplifies on-boarding, resulting in cost savings and efficiencies from Digital Transformation.

Mobility: Peers can share their digital identities across different platforms, services, and organisations without being tied to a specific identity provider.

Security and privacy: SSI has strong cyber-security measures and privacy-focused technologies, such as encryption and decentralised storage, to protect personal data, so that verifiable credentials are with the peer, not in the cloud, or stored in a data centre.

Fraud reduction: Decentralised digital identification does not rely on usernames and passwords that can be hacked (no government or corporate "honeypots" of personal data) - the peer creates an online identity in the form of a mobile self-sovereign digital wallet that is verified in real time against authoritative sources, such as government databases and other anti-fraud checks.

Interoperability: SSI protocols enable interoperability between different identity systems, which are not "purpose-built", promoting compatibility and adoption.

11. The Business Case for SSI is superior to centralised or federated models because through providing peers ownership and control over their digital identities, SSI offers the potential for increased privacy, reduced reliance on centralised databases, minimised identity theft risks, and improved peer experiences in digital interactions.

The Proposed Australian Digital ID Legislation and Decentralised Self-Sovereign Digital ID

12. The proposed Australian Digital ID legislation seeks to implement strong privacy safeguards for people who use digital IDs provided by a voluntary "accredited" Digital ID provider, noting that the Federal Government will manage the Accreditation Scheme, setting technical standards and enforcement mechanisms, while the ACCC will be the "independent regulator", managing and regulating "trustmark". The Australian Digital ID legislation will also enable an expansion of a government-controlled digital ID system, that is, it will encourage expansion of a centralised digital ID system.

13. A centralised or federated approach to digital ID is not in the best interests of the Australian people – rather than "top-down" decision-making from the Federal Government and other vested interests, why not honest consultation and communication with the Australian public, via genuine private-public collaboration for the building of decentralised identity-based infrastructure (a "bottom-up" approach)?

14. Historically, the Australian public do not trust centralised identification schemes, for example, the Hawke Labor Government's failed attempt to introduce an Australia Card in the 1980s – the draft legislation might be regarded as a "digital" approach to same, using government-managed identity service providers, noting that the Australian public are wary of government corruption and ideological conformity, wanting less interference from government in their daily lives.

15. The Australian public should be provided with ample opportunity to become objectively informed of the different types of identity management systems available in the market for such systems, including decentralised self-sovereign digital ID, as a great deal has changed since the National ID project was launched by the Federal Government – some localities in Canada (Ontario) and Switzerland (Zug) now use SSI and so too should Australia adopt this technology for its own comprehensive digital ID system, as SSI provides the same capability as centralised or federated systems, but without coaxing the public into using government-managed Identity Providers through the veneer of an “Accreditation Scheme”.

16. The International Association of Privacy Professionals (“IAPP”) conclude in their White Paper titled “Self-sovereign identity as future privacy by design solution in digital identity?” (2022) that while digital identity is complex, SSI technology has the potential for better privacy protection of digital identities, as it supports peer control of their own identifiers and allows for their selective disclosure, thereby aligning with the principles of data minimisation and purpose limitation.

17. Civil society groups, such as the Internet Identity Workshop recognise the potential of digital identity under SSI through the use of distributed ledger technology, as SSI distributed ledger technology allows for a permission-free, interoperable and decentralised digital identity framework for genuine peer control of identity credentials, thereby building public “trust” in identity management systems.

18. In 2020, the Federal Government released the National Blockchain Roadmap, which did mention “identity” and “trusted credentials”, but not SSI specifically - a SSI system based on distributed ledger technology provides a viable digital identity management framework for Australia, as long as the technology aligns with the data and privacy protections afforded under the Australian Privacy Principles, vis-à-vis the Australian Privacy Act.

19. In a civil society, the Australian public would control their own verifiable identity credentials as peers, which means SSI puts the interests of an autonomous and powerful public in this third system ahead of the Federal government and corporations.

20. The current digital ID legislation will not close the “trust gap” and is not in the best interests of the Australian public – the proposed legislation should not be put to the Australian Parliament accordingly.