The Digital Transformation Agency

Digital Identity Legislation Position Paper – Phase 2 Consultation

13 July 2021

Re: Have your say – Digital Identity Legislation

To whom it may concern,

Thank you for the opportunity to provide comments to the Australian Government's Digital Identity Legislation Position Paper, that is aimed at expanding the Digital Identity system in Australia. Our submission is provided in good faith as a measure to strengthen the proposed digital identity bill through enhanced privacy, data protection and security measures. We believe these proposed amendments will provide a more inclusive, safer, trustworthy, and dignified experience for Australians who will engage with the digital identity system.

The Trust Alliance is a group of non-profit, academic and technology organisations came together with a common purpose – to develop an identity ecosystem that would:

- Give people better access to help when they need it;
- Enable genuine civic, social and economic participation for all;
- Create greater self-agency and control for those who are vulnerable;
- Provide voice to marginalised communities, and;
- Document the undocumented.

The Trust Alliance focuses on producing the organisational governance and technical guidelines for how decentralised credentials should be implemented. Drawing upon a combination of open source tools and standards, anchored in real world use cases being led by member organisations.

In our submission below, we have mapped key issues for consideration and 32 specific comments or recommendations on the position paper for the Government's consideration. Should you wish to discuss any of the matters below further, please do not hesitate to contact me at louise.gray@care.org.au

Louise Gray

Chair, Trust Alliance

The Trust Alliance submission to the Australian Government's Digital Identity Legislation Position Paper

Introduction

The Trust Alliance welcomes the opportunity to provide feedback on the Government's Digital Identity Legislation – Position Paper.

We broadly support the three tenets of the proposed digital identity scheme: to establish robust governance, strengthen data and consumer protections, and allow other bodies to apply for TDIF accreditation.

In sum, we are supportive of the intent of the digital identity system – to make government services simpler and easier to access for all Australians.

We recognise the potential benefits of a federated digital identity system for Australian citizens, such as improved access to services, particularly for people who cannot attend a physical shopfront to prove their identity. However, we note that a digital identity could create a permanent identifiable record for a person, and that their data could be breached or shared with third parties without informed consent. Such a sensitive system must be properly designed and implemented, lest it result in significant harm to individuals, intended or otherwise.

Digital inclusion: The roll out of a new digital identity scheme should be accompanied with a digital inclusion strategy to ensure that the legislation and technology solution does not exacerbate the existing digital divide. The growing use of technology-based solutions for access to public services, including Centrelink, Medicare and My Aged Care, poses significant challenges for 1 in 10 Australians who live in households without fixed internet connection, including people aged 65 and over, Australians with low levels of income, education and employment, people living outside of metropolitan centres and those from non-English speaking backgrounds.

Digital ability: There is also a wide disparity in digital ability levels across Australia. While the COVID-19 pandemic has made the benefits of digital technologies more obvious (such as QR code scanning, online grocery deliveries, etc.), many Australians are anxious about using digital tools due to their (real or perceived) lack of ability. We recommend a digital ability strategy to boost the digital literacy for these cohorts of Australians to ensure they have the requisite skills to participate and thrive in the digital age[1].

Integration: We are concerned about the proliferation of digital identity schemes across governments, both federal and State/Territory, industry, and not-for-profit organisations. This uncoordinated effort places significant burden on the user to manage multiple identities across multiple tiers of government, and engagements with the private sector. This leads to a fragmented digital identity system, with individuals' data stored across multiple databases and susceptible to data breaches, poor integration, and a poor user experience. This could lead to digital disengagement from citizens; individuals with lower levels of digital skills are the most likely to drop out from the digital ecosystem, further exacerbating the digital divide. Common downstream impacts of digital disengagement for this cohort of citizens are: less access to government services, education, economic opportunities, social and community activities. This is particularly acute, given that in most domains of modern life, the digital version of a service or product is the primary version,

[1] https://digitalinclusionindex.org.au/wp-content/uploads/2020/10/TLS_ADII_Report-2020_WebU.pdf

with physical being the secondary (i.e., emails over physical mail; video-conferencing over a community hall meeting; advertising on social media over a physical newspaper)[2].

Transition: We note that a number of vulnerable communities have difficulty in attaining an identity record, barring their access to community and social services.

There is a great opportunity to support these cohorts towards using a digital identity in safe and trustworthy ways. Two cohorts that could benefit from a digital identity are: people exiting the criminal justice system (ex-prisoners) and children and young people in out of home care (OOHC). These cohorts would benefit from additional government support to migrate to using a digital identity, which they could easily carry with them for life.

Support should be provided during key transition phases - such as when a prisoner exits the criminal justice system or a child exits the OOHC system. This would ensure these vulnerable cohorts enter or re-enter community life with a digital identity, thereby providing them with the best possible chance of thriving in the community.

Child use: We note the minimum age for participation in this scheme is 15 years old. We have a range of concerns around children participating in the digital ecosystem system. These are centered around ensuring young people are educated about the complexities of creating and managing a digital identity and protecting them from harm.

Best practice: The Trust Alliance has developed the Trust Alliance Credential Framework which outlines a best practice approach to developing a digital identity system. As demonstrated in the framework, a strong identity credential should be practically useful, linked to a real-world identity, consistent with the W3C verifiable claim standard, and stored safely[3]. Our efforts have been informed by extensive global efforts to develop ethical and useful digital identities. Specifically, we have been guided by the identity principles laid out in the id2020 manifesto[4]. These are: ensuring equitable access to identity; recognition that identity is a key enabler of social and economic participation for individuals; identity should be controlled by individuals; and identity credentials should be designed using secure, cryptographic identity systems where possible. Our work aligns with the Principles for Digital Development (Appendix 3).

---

[2] https://economictimes.indiatimes.com/tech/information-tech/the-pandemic-has-made-everything-digital-first-balaji-srinivasan-says/articleshow/81096138.cms

[3] W3C standards consider aspects of accessibility, privacy, security, and internationalization. Further information is available at: https://www.w3.org/standards/about.html

[4] https://id2020.org/manifesto

Specific feedback on the proposed digital identity scheme

Structure of the legislation

1. We **request** that the Bill explicitly provide for a mechanism through which the public can lodge submissions on any proposed future amendments.

Scope of the legislation and interoperability with other systems

2. We **recommend** the inclusion of a customer service standard, set out by the responsible Minister. This should ideally outline key principles of the digital identity solution to maximise the benefit for the public and minimise harm.

Several key guiding principles are laid out below, for consideration:

- **Co-designed** to ensure it is fit for purpose: the design and experience of the solution should be co-created with the community;
- **Integrity**: set out rules outlining what data will and will not be collected, how data will be stored and shared with third parties.
- **Consent** and autonomy: ensure individuals can choose to opt in and opt out at any time; use parts of the services proposed; and can use the id solution across different types of devices.
- **Review and Resolutions** – ensure clear processes are laid out (including timelines) if an individual would like to appeal a decision with respect to their digital identity.

Automated decision-making

3. We **do not support** the use of automated processes in decision-making, as set out in the Bill's position paper.
4. We **request** further information regarding the types of decisions (deemed 'non-discretionary') this would apply to.
5. We **note** the Australian Human Rights Commission's (AHRC) recommendation that "the Australian Government should not make administrative decision, including through the use of automation or artificial intelligence, if the decision maker cannot generate reasons or a technical explanation for an affected person.

Governance

6. We **support** the Office of the Oversight Authority being a statutory officeholder, and for the Information Commissioner to ensure the scheme complies with biometrics safeguards, limits data profiling and enforces the retention and destruction of information.
7. We **recommend** that the Oversight Authority and the Information Commissioner table an annual report to Parliament with respect to the scheme's performance.

Advisory Board(s)

8. We **recommend** that the Board is comprised of a broad range of representatives across society. This may include representatives from industry, academia, regulators, and civil society. This cross-sectoral representation will ensure that decision makers will have a holistic understanding of how the digital identity solution impacts the community, including marginalised and vulnerable groups. It will ensure the Minister and the Government has real-time advice on:
    - the community impact of the digital identity solution;
    - whether the solution is fit for purpose, accessible and appropriate;
    - the changing nature of technologies.

The Trust Alliance, being across sectors and focused on use of digital credentials to minimise harm and maximise inclusion, is well placed to support this and would welcome the opportunity to engage further.

Information Commissioner: Privacy regulatory functions

9. We **request** further detail around the biometric safeguards being proposed; what 'data profiling' will entail; and the retention and destruction rules around handling information.
10. We **note** the Review of the Privacy Act by the Commonwealth Government with a focus on:
    - Efficient and effective service delivery, done in a responsible way, that protects fundamental consumer rights in the process;
    - Empowering consumers, protects consumers, serves the economy;
    - Enhancing individuals' control over information, require greater focus on building in privacy by design;
    - Building community trust and confidence around data handling.
11. We **request** the Digital Transformation Agency to provide information about how the Bill and the Digital Identity will incorporate future changes to the Privacy Act; and the level of consultation undertaken with the Attorney-General's department on this matter.
12. Pseudonymity: we **recommend** the digital identity solution supports the creation and maintenance of pseudonymous digital identities; the Bill could play a greater role in facilitating pseudonymous identities, as a data protection mechanism. Appropriate safeguards could be implemented to ensure credentials are issued to a real person, with unique identifying documents but the credential itself could be detached to the individual to whom the credential is issued, thereby severing a potential data linkage in the future. This would serve as an additional safeguard for vulnerable people, in the event of a data breach.

Functions of the Oversight Authority

13. We **recommend** that any data held by the Oversight Authority, such as lists and registers be done in a safe way to ensure citizens' data is protected.

    Data sharing with third parties should only be done when there is clear consent from the individual. The individual (citizen) should be informed of where and how their identity data is being used, even when this is for law enforcement purposes.

14. With respect to gaining informed consent, we **recommend** that people be provided with easy-to-understand information in a variety of formats to support people with barriers to access - including disability, lack of on-line accessibility and literacy barriers - in their first language on the digital identity as well as their rights and protections in relation to it, to ensure consent is informed.

Review rights

15. We **note** the proposed internal and external review rights.
16. We **note** the AHRC's recommendation in its recent Technology and Human Rights report that "The Australian Government should introduce legislation to create or ensure a right to merits review, generally before an independent tribunal such as the Administrative Appeals Tribunal (AAT), for any AI-informed administrative decision. We agree with this policy recommendation and we **recommend** such a merits review process be applicable to all decisions with respect to the granting, suspension or cancellation of a digital identity.
17. We **recommend** that the Oversight Authority provide financial support to the individual or party during the review so that they can pursue the matter with the AAT.

Privacy and consumer safeguards

18. We strongly **support** the limitations of using biometric matching in the system to one-to-one matching.
19. We **support** the voluntary nature of the digital identity scheme. Participants should have the choice to opt in and opt out at any time.
20. We **propose** that the alternative channels should be easily accessible – on par with using a digital identity – to ensure the individual is not punished for choosing to use a non-digital channel.
21. We **note** additional privacy impact assessments (PIAs) will be undertaken as the system expands to ensure privacy requirements are upheld.
22. We **recommend** these PIAs to be undertaken by independent security consultants, and for the results to be published to the public in a timely manner. This effort will ensure transparency and result in greater community trust.
23. We **note** that the Paper states that "the Digital Identity system has undergone end-to-end cyber security and risk assessments." We **request** further detail on these assessments, such as which entity conducted the assessment and their results.
24. We **note** anyone aged 15 years and over can create and manage their Digital Identity. We **seek** further information with respect to the safeguards to protect children from harm, as a result of the digital identity system. This may include children-specific review and appeal rights, a children-specific digital access and inclusion strategy, and accounting for situations where young people may have complex guardianship and parental responsibility arrangements.

Restrictions on data profiling

25. We **support** the limitations on the collection, use and disclosure about a User's behaviour on the system. However, we are concerned about information being passed to a law enforcement agency without an individual's consent.
26. We **recommend** that an individuals' information should only be shared with a third party after consent from the individual has been granted, on a case-by-case basis. The consent should be sought from the individual in real-time.

Data protection

27. In terms of best practice around cyber security and information management, we request the DTA to **clarify** if the digital identity system will meet, or align to, the Australian Cyber Security Centres's (ACSC's) Essential Eight Maturity model's mitigation strategy with respect to cyber security incidents; and the Information Security Manual (ISM).

Record-keeping

28. We **do not support** metadata and activity logs being retained for up to 7 years after a User deactivates their digital identity or their account is deleted for inactivity and would welcome further information as to why this would be considered necessary and appropriate.
29. We **recommend** that in these two circumstances, a user's identity metadata and activity logs be destroyed immediately after use.
30. We **do not support** retention of any identity information once a User has deactivated their digital identity or their account has been deleted for inactivity.

    Destroying identity information at the earliest opportunity will minimise the chance of citizens' data being breached.

Data breaches can lead to serious violations of individuals' privacy and in some cases have resulted in serious harm to vulnerable individuals. For example, in January 2021, the Department of Home Affairs was found to have interfered with the privacy of 9,251 detainees in immigration detention by mistakenly releasing their information. In making this judgement, the Information Commissioner recognised that "a loss of privacy or disclosure of personal information may impact individuals and depending on the circumstances, cause loss or damage.[5]"

Data storage

31. We strongly **recommend** that data retained by the Accredited Participant, the Oversight Authority and any other third party, be held in Australia. This includes ensuring that any cloud storage of citizens' data is not held offshore.

Safeguards on biometric information

32. We **support** the limitation of biometric matching in the system to one-to-one matching. We propose that the image (i.e a selfie image matched to a primary document such as a Passport) provided by the user be destroyed immediately upon completion of the function (the match).
33. We **support** the AHRC's Recommendation (19) that Australia's federal, state and territory governments should introduce legislation that regulates the use of facial recognition and other biometric technology. And for the legislation to:
    a. expressly protect human rights
    b. apply to the use of this technology in decision making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement
    c. be developed through in-depth consultation with the community, industry, and expert bodies such as the AHRC and the OAIC.

Data breaches

34. We strongly **support** the stipulation of the Bill requiring Accredited Participants to notify the individuals, the OAIC and the Oversight Authority when there are reasonable grounds to believe that a data breach has occurred, as per the mandatory data breach notification laws.

Portability and interoperability

35. Given the federated nature of the digital identity scheme and other jurisdictions having launched various digital identity schemes and services (i.e., Service NSW, Service Victoria), we **recommend** that individuals be provided the option to use their federal digital identity for State Government services, and individuals be given the choice to move certain personal data from one service to the other. To facilitate this process, interoperability between services and across national boundaries – either through the TDIF or otherwise – should be encouraged through the life of the scheme.
36. We **recommend** the use of cryptographically secure, decentralised identity systems to provide greater privacy protection for users, while also allowing for portability and verifiability.

[5] https://www.oaic.gov.au/updates/news-and-media/information-commissioner-orders-compensation-payable-by-home-affairs-for-breaching-detainees-privacy/

APPENDIX 1: ID2020 MANIFESTO

1. The ability to prove one's identity is a fundamental and universal human right.
2. We live in a digital era. Individuals need a trusted, verifiable way to prove who they are, both in the physical world and online.
3. Over 1 billion people worldwide are unable to prove their identity through any recognized means. As such, they are without the protection of law, and are unable to access basic services, participate as a citizen or voter, or transact in the modern economy. Those affected are those most vulnerable to disadvantage and exploitation. Most of those affected are children and adolescents, and many are refugees, forcibly displaced, or stateless persons[6].
4. For some, including refugees, the stateless, and other marginalised groups, reliance on national identification systems isn't possible. This may be due to exclusion, inaccessibility, or risk, or because the credentials they do hold are not broadly recognised. We need to understand and respect that many people flee governments and situations of distrust and are therefore rightfully reluctant to "register" their identity. While we support efforts to expand access to national identity programs, we believe it is imperative to complement such efforts by providing an alternative to individuals lacking safe and reliable access to state-based systems.
5. We believe that individuals must have control over their own digital identities, including how personal data is collected, used, and shared. Everyone should be able to assert their identity across institutional and national borders, and across time. Privacy, portability, and persistence are necessary for digital identity to meaningfully empower and protect individuals. The existing global regulatory and policy framework globally is complex, confusing and ill-suited to identity portability.
6. Digital identity carries significant risk if not thoughtfully designed and carefully implemented. We do not underestimate the risks of data misuse and abuse, particularly when digital identity systems are designed as large, centralized databases.
7. Technical design can mitigate some of the risks of digital identity. Emerging technology — for example, cryptographically secure, decentralised systems — could provide greater privacy protection for users, while also allowing for portability and verifiability. But widespread agreement on principles, technical design patterns, and interoperability standards is needed for decentralized digital identities to be trusted and recognized.
8. This "better" model of digital identity will not emerge spontaneously. In order for digital identities to be broadly trusted and recognized, we need sustained and transparent collaboration aligned around these shared principles, along with supporting regulatory and policy frameworks.
9. ID2020 Alliance partners jointly define functional requirements, influencing the course of technical innovation and providing a route to technical interoperability, and therefore trust and recognition.
10. The ID2020 Alliance recognizes that taking these ideas to scale requires a robust evidence base, which will inform advocacy and policy. As such, ID2020 Alliance-supported pilots are designed around a common monitoring and evaluation framework.

[6] https://preparecenter.org/wp-content/uploads/2021/06/Digital-Identity-Enabling-dignified-access-to-humanitarian-services-in-Migration-Final.pdf

Appendix 2 - The Trust Alliance Framework

The Trust Alliance Credential Framework describes the technical approach surrounding the main functions required by digital credentials.

Registering a credential issuer: For a credential to be practically useful, it must be linked to a real-world identity. When a credential is verified, the relying party must have confidence that it was genuinely issued by the stated authority. We currently use the Trust Registry for this purpose. The Trust Registry is comprised of two registers; the Issuer Register and the Claims Status Register. An issuing entity (Issuer) is created and registered by storing their public-key and entity name on the Issuer Register.

Issuing a credential: Issuing a credential to an individual is consistent with the W3C verifiable claim standard. Credentials are generated using this standard and are cryptographically secured and anchored back to the Trust Registry's identity register via the issuer's identity. Individual privacy is maintained by ensuring only the issuer identity is registered to the Trust Registry and later used for credential verification.

Storing a credential: No individual credential information is stored on the blockchain. Verifying a credential: Credentials are verified by following a three-step process. First the credential is checked to see whether it has been tampered with. This is guaranteed by using the cryptographic signature attached to the credential when it was issued. The second step checks to see whether the credential was issued by the authority stated on the credential which is achieved by checking the cryptographic signature on the credential against the Issuer Register on the Trust Registry. The final step is to check the Claims Status Register to see whether a credential has been revoked.

Appendix 3 - Principles for digital development

Design With the User
User-centered design starts with getting to know the people you are designing for through conversation, observation and co-creation.

Understand the Existing Ecosystem
Well-designed initiatives and digital tools consider the particular structures and needs that exist in each country, region and community.

Design for Scale
Achieving scale requires adoption beyond an initiatives pilot population and often necessitates securing funding or partners that take the initiative to new communities or regions.

Build for Sustainability
Building sustainable programs, platforms and digital tools is essential to maintain user and stakeholder support, as well as to maximize long-term impact.

Be Data Driven
When an initiative is data driven, quality information is available to the right people when they need it, and they are using those data to take action.

Use Open Standards, Open Data, Open Source, and Open Innovation
An open approach to digital development can help to increase collaboration in the digital development community and avoid duplicating work that has already been done.

Reuse and Improve
Reusing and improving is about taking the work of the global development community further than any organization or program can do alone.

Address Privacy & Security
Addressing privacy and security in digital development involves careful consideration of which data are collected and how data are acquired, used, stored and shared.

Be Collaborative
Being collaborative means sharing information, insights, strategies and resources across projects, organizations and sectors, leading to increased efficiency and impact.