14 August 2026

Department of Finance
One Canberra Avenue
FORREST ACT 2603
AUSTRALIA

Re: Digital ID Act Statutory Review Consultation

Dear Sir/Madam

The Australian Digital Trust Community Group (ADT CG) under the OpenID Foundation (OIDF) welcomes the opportunity to comment on the Digital ID Act Statutory Review. Please see our general recommendations and responses to specific questions raised in the Digital ID Act consultation document.

On a general note, the ADT CG encourages the Department to continue to focus on interoperability as part of evolving the Australian Government Digital ID System. OIDF standards like OpenID for Verifiable Presentation, OpenID for Verifiable Credential issuance, OpenID Connect, FAPI 2.0, OpenID Federation, Shared Signals are likely to underpin or play a role in AGDIS.

We encourage the Australian community to use the freely available open source tests for implementers to prove out their deployments meet the security, privacy, interoperability and scale properties inherent in the specifications. Should the Australian government establish an accreditation or conformance scheme that includes (but may not be limited to) OIDF specifications, the government should consider leveraging the low-cost self-certification program (https://openid.net/certification/) or the future accreditation program launching in Q2 2026 (https://openid.net/oidf-announces-new-investment-to-expand-conformance-services/). Both services are available to ecosystems, with a goal of ensuring ecosystem partners can achieve their objectives.

As a global open standards body, we welcome the opportunity to support the Australian community. As per OIDF's practice of being transparent and open, we intend to share our response to this request for comments in a blog post on openid.net in the near future.

We welcome the opportunity to discuss our comments or other related matters. Contact john.scullen@aaf.edu.au regarding any follow-up to this response.

Sincerely

John Scullen
on behalf of the Australian Digital Trust Community Group co-chairs

Executive Summary

The Australian Digital Trust Community Group (ADT CG) welcomes the opportunity to contribute to the statutory review of the *Digital ID Act 2024*.

The Act has established an important foundation for digital identity in Australia and created a framework upon which broader digital trust services can be developed. As digital identity adoption matures, this review presents an opportunity to consider how the framework can evolve to support economy-wide participation, innovation and long-term public value.

Our feedback is informed by a broad range of participants across government, industry, technology, higher education, research and standards communities. While our recommendations focus on digital identity, many of the same observations apply more broadly to Australia's digital trust infrastructure, including adjacent initiatives such as Consumer Data Right and emerging trusted digital credential ecosystems.

At a strategic level, we encourage the Government to consider digital trust as a national capability supported by four interconnected pillars:

1. Commonwealth Government;
2. State and Territory Governments;
3. The Private Sector; and
4. International Interoperability.

Figure 1 illustrates a simplified common trust framework with a range of different schemes operated by various stakeholder groups.

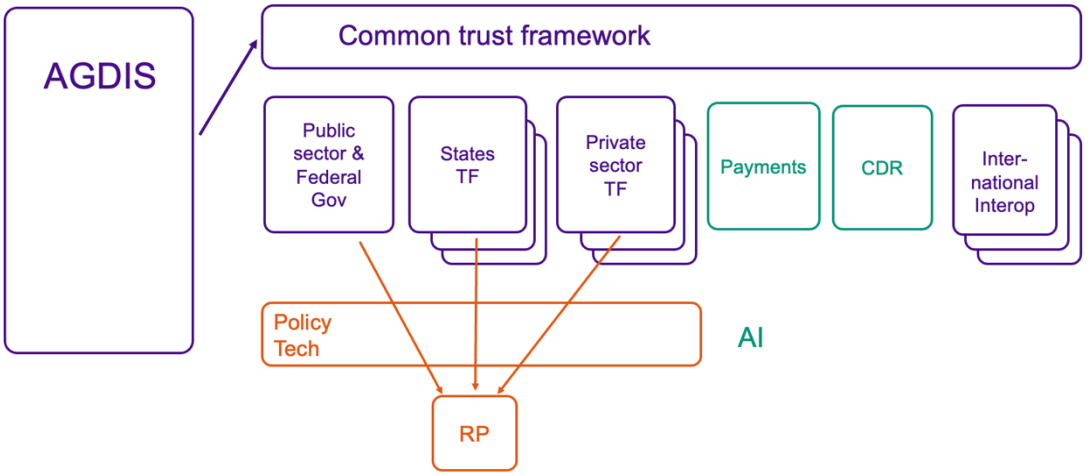

Figure 1: Trust framework concept

Long-term success will depend not only on the effectiveness of any one pillar, but on how well they operate together to create a coherent and trusted ecosystem for Australians and Australian organisations.

Against this backdrop, our submission centres on three key themes.

1. Design AGDIS for economy-wide outcomes

The current framework has provided an important starting point for Australia's digital identity ecosystem. However, future policy settings should place greater emphasis on the outcomes Australia is seeking to achieve rather than implying specific architectural models or implementation approaches.

We encourage a **principles-based approach** that enables multiple sectors and trust frameworks to participate while maintaining strong security, privacy and interoperability outcomes. Utah's State Endorsed Digital Identity is one example of a principles-based approach. In our view, adoption challenges are increasingly economic and organisational in nature, involving incentives, network effects and coordination across participants. These concepts are explored in greater detail in *The Impact of Digital ID Ecosystem Design on Welfare* (ADT CG, 2026)[1]. Success should be measured through transparent outcome-based metrics that reflect public value, uptake and impact, rather than activity measures such as transaction volumes or accreditation counts alone.

2. Prioritise a roadmap for trusted credential issuance

The review provides an opportunity to articulate a clearer vision and roadmap for the development of Australia's digital trust ecosystem. We recommend prioritising the issuance of trusted government credentials that can be reused across government, industry and community sectors. The government's most effective contribution is to cultivate the credential supply side of a digital trust ecosystem.

While identity credentials are an important foundation, proof of qualifications, licences, permits, delegated authority and other forms of verifiable information are the major drivers of improved productivity. These capabilities may also support new interaction models involving automated systems and AI agents acting on behalf of individuals and organisations.

3. Reduce barriers to acceptance and use

Widespread adoption will depend on making trusted digital credentials easier to accept, integrate and use. We encourage the Government to focus on high-volume, high-value use cases that can deliver benefits to the greatest number of participants.

This includes identifying and addressing regulatory and operational barriers that discourage reliance on digital credentials, improving user experience, and providing greater certainty for relying parties. Practical measures that simplify acceptance and reduce implementation friction are likely to have a greater impact on adoption than low-frequency, high-security edge cases.

Our response to specific questions follows. They expand on these themes and identify opportunities to strengthen Australia's digital trust ecosystem while preserving the core objectives of trust, privacy, security and consumer protection that underpin the Act.

[1] OpenID Foundation Australian Digital Trust Community Group (ADT CG) 2026, *The Impact of Digital ID Ecosystem Design on Welfare*, Workshop Summary, June 2026, OpenID Foundation, viewed 7 August 2026, OpenID Foundation Workshop Summary PDF.

Is the Act and supporting legislative framework operating to advance its objects?

The greatest value of a digital identity system is realised when an individual can prove their identity once and then reuse that trusted identity across a wide range of interactions. The system must deliver benefits to all parties while protecting users from commercial coercion, surveillance and unnecessary disclosure of personal information. While the current framework has successfully focused on establishing trust and assurance, adoption and acceptance across the broader economy remain limited. As a result, many individuals and organisations continue to undertake repeated identity verification processes, duplicating effort and cost.

In our view, the next phase of development should prioritise acceptance and reuse. Government-issued and accredited digital identities should be capable of being relied upon as widely as possible across Commonwealth and State government services, regulated industries, and the private sector. Success should not be measured solely by the number of accredited providers or transactions, but by the extent to which digital identity reduces friction, lowers compliance costs, improves user experience, and eliminates the need for repeated identity verification.

Broad acceptance is ultimately an economic challenge as much as a trust challenge. Organisations will adopt digital identity where the benefits outweigh the costs and where regulatory settings provide certainty for relying parties. We therefore encourage a stronger focus on removing barriers to acceptance, clarifying reliance obligations, and creating incentives for widespread reuse of trusted digital credentials across the economy.

Without broader acceptance and commercial viability, the privacy, security and inclusion benefits delivered by the framework will not be fully translated into the economic benefits and productivity gains envisaged by the Act.

Is the legislation supporting the uptake of digital ID and improving service delivery?

Digital ID delivers value when it can be relied upon in the economy. One of the highest value use cases is customer identification by AML/CTF regulated entities. An accredited digital ID carries a higher level of assurance than document-based checks and would materially reduce exposure to certain attack vectors. While the recently revised AML/CTF framework emphasises a risk-based approach, it does not expressly recognise Digital ID. Reporting entities have no certainty that accepting an accredited digital ID satisfies customer due diligence.

To enable reliance, the AML/CTF framework would need recognition (a deemed-compliance or safe harbour pathway) that verification via an accredited digital ID satisfies initial CDD. Consideration should also be given to record-keeping settings, enabling entities to retain the assurance assertion rather than copies of identity documents, consistent with the Digital ID Act's data minimisation rules.

New Zealand has already done this. Its new Identity Verification Code of Practice (in force 1 July 2026) adds a fourth verification pathway: accredited Digital Identity Services Trust Framework providers. Australia should consider adopting the equivalent and the review should recommend that AUSTRAC revises AML/CTF Rules 2025 accordingly.

This will be particularly relevant given planned private sector participation in AGDIS from 30 November 2026 and the Tranche 2 reforms which extend AML/CTF obligations to real estate agents, lawyers, accountants, conveyancers and dealers in precious metals and stones.

Are there options for longer term reform?

The ADT CG supports consideration of longer-term reforms that improve the flexibility, longevity and adaptability of the legislative framework.

Digital identity technologies are undergoing rapid change and legislation should focus on the desired outcomes for Australia rather than prescribing or implying particular technical architectures. While the current framework has successfully established a trusted foundation, it is not always clear that it can readily accommodate emerging models such as verifiable credentials, decentralised trust frameworks, or non-human identities, including AI agents and organisational agents acting under delegated authority. Technical implementation guidance is more appropriately addressed through rules, standards and accreditation requirements, where it can evolve alongside technology and industry practice.

We encourage the review to adopt a more principles-based approach centred on outcomes such as privacy by design, data minimisation, selective disclosure, user control, and the verification of claims or attributes rather than the broad release of personal information. These principles are likely to remain relevant over time, even as the technologies and standards used to achieve them continue to develop.

The review should also consider the extent to which emerging credential models may achieve the policy objectives of the Act through technical means rather than regulatory controls alone. In particular, widespread adoption of verifiable credentials has the potential to significantly enhance privacy by enabling individuals to prove specific attributes or claims without revealing the underlying personal data. This may progressively reduce reliance on some of the more complex privacy controls currently embedded in the framework while continuing to deliver strong privacy, security and consumer protection outcomes.

A future-ready framework should therefore emphasise enduring principles and desired outcomes, while preserving flexibility for new standards, technologies and trust models to emerge.