

Unlocking the potential of trusted digital identity in Australia

A white paper from
Australian Payments Plus
and Deloitte Australia

May 2023



Preface

This paper focuses on the benefits that may be realised in Australia from new investments being made in digital identity and the design considerations necessary to achieve these benefits. Our observations add to a growing body of research on digital identity and hope to inform the future discourse in Australia specifically. The paper draws primarily on the experience of the ConnectID® team at Australian Payments Plus who are responsible for building a digital identity network for Australia, the Digital Trust team at Deloitte Australia, and insights gathered from our customers, partners and advisors. We also draw on the insights of other observers and thankfully acknowledge their direct and indirect contributions.

ConnectID is an initiative of Australian Payments Plus (AP+). AP+ brings together eftpos, BPAY and NPP Australia as one organisation to shape the future of payment experiences.

Authors

Australian Payments Plus

Andrew Black, Managing Director, ConnectID

Dima Postnikov, Head of Identity Architecture and Strategy, ConnectID

Rick Iversen, Head of Product and Scheme, ConnectID

Siobhan Richardson, Commercial Business Manager

Deloitte Australia

John Jones, Partner Digital Trust

Natalie Reed, Director Digital Trust

May 2023



Deloitte.



Unlocking the potential of trusted digital identity in Australia

According to recent statistics, Australians are spending the same amount of time online as they do at work – roughly 40 hours a week.¹

As more and more of our daily lives are managed and transacted digitally, and high-profile data breaches are experienced by an expanding list of well-known and trusted Australian businesses, designing solutions which allow us to do this safely and securely are becoming a top priority. Under this lens, investments in Australia to enable and scale digital identity (digital ID) platforms or services which allow a user to digitally verify they are who they say they are to a receiving party are gaining traction. When designed well, digital ID not only increases resilience against

cyber-attacks and data breaches for individuals and companies but can support the broader development of a country's digital economy.

The following paper examines the potential benefits of digital ID for Australia and the design elements which can help to maximise this potential. In doing so, we first look at what digital ID is, the purpose it serves and how it can benefit individuals, businesses and organisations, and the economy. We then outline the current state of play in Australia and the design considerations which will help it move from this position to fully realise the benefits of digital ID.



So, what is digital ID and what does it do?

Before framing out the potential benefits of investments in digital ID for Australia, we should first define what it means and the purpose it serves. For this discussion, we will lean on the Commonwealth of Australia's Trusted Digital Identity Framework's (TDIF) definition:

“Digital identity is an electronic representation of an entity (person or other entity such as a business) and it allows people and other entities to be recognised online. A person’s digital identity is an amalgamation of personal attributes and information in electronic form that can be bound to that physical person.”²

Digital ID in the above form allows an individual or entity to verify their identity to a receiving or relying party (RP) online rather than manually so that they can receive goods or services and participate in a digital economy.³ In layman's terms, it allows a person to digitally prove, either in person or online, something about themselves to someone else.

1. Norquay, J. 2. Commonwealth of Australia (Digital Transformation Agency) 3. Commonwealth of Australia (Digital Transformation Agency)

What are the benefits of digital ID?

When successfully adopted across a population, the benefits of digital ID extend from those who use the technology to identify themselves (end users / identity owners), to the businesses and organisations who rely on this verification (RPs) and the broader economy.

End users or identity owners

Digital ID can provide users with convenient access to a broad range of digital products and services which previously may have required significant time and effort to avail of manually. For example, giving an individual the ability to digitally verify their identity quickly and safely to open a new digital account and access critical government services.

It also allows for effective and inclusive remote identification where in-person services can be limited and therefore where people may have, historically, also been excluded from participating in the economy.

This is particularly beneficial to countries with widely dispersed and remote populations, such as in Australia. Since the COVID pandemic, this has broader relevance where in-person identification may be undesirable or even impossible at times (e.g., for health and safety reasons). Taken together, digital ID promotes greater inclusion and convenience, improved productivity and increased confidence in digital services.

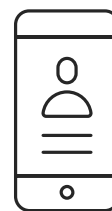
Relying parties (RPs)

For businesses and organisations receiving digital ID verifications, the benefits are even greater. Digital ID can significantly improve the customer and user experience. It does this by streamlining customer onboarding and reducing e-commerce cart abandonment or drop-offs during this process as evidenced by countries such as Sweden and Norway where faster onboarding processes were found to correspond with particularly high digital ID adoption rates (91% and 81% respectively).⁴

Digital ID can also dramatically reduce operating costs whilst improving risk outcomes when compared to manual identification methods. For example, by providing better privacy compliance, fraud detection, automation and less reliance on third party verifiers, digital ID can help banks cut down the cost of onboarding and regulatory compliance by up to 70%.⁵ Effective use of digital ID also allows a business or organisation to minimise its data consumption and reduce data exposure risk by allowing for identification through an assertion rather than collecting and retaining personal information (PI).



Countries with higher digital ID adoption rates have faster onboarding processes.



70%

The amount onboarding and regulatory compliance costs can drop for banks through using digital ID.

4. Biometric Update 5. Tesfaye, M



Avoiding the cost of data breaches

Digital ID can minimise data consumption by allowing RPs to rely on assertions to complete an identity verification rather than collecting and retaining people's data. In doing so, digital ID can also help to avoid the costs associated with data breaches which are felt by citizens, businesses and the economy:

For citizens, this cost comes in the form of exposure of personal identity documents such as driver licenses and Medicare card details. In the latter half of 2022 alone, Australia had five instances of data breaches where information was compromised for 1-10 million people.⁶

For businesses, the average cost of a data breach in Australia in 2022 was estimated at \$2.92 USD million.⁷ This estimate, however, does not include potential fines of up to \$50 AUD million which can now be incurred if they are found to have inadequately protected people's data, following legislation introduced in 2022.⁸

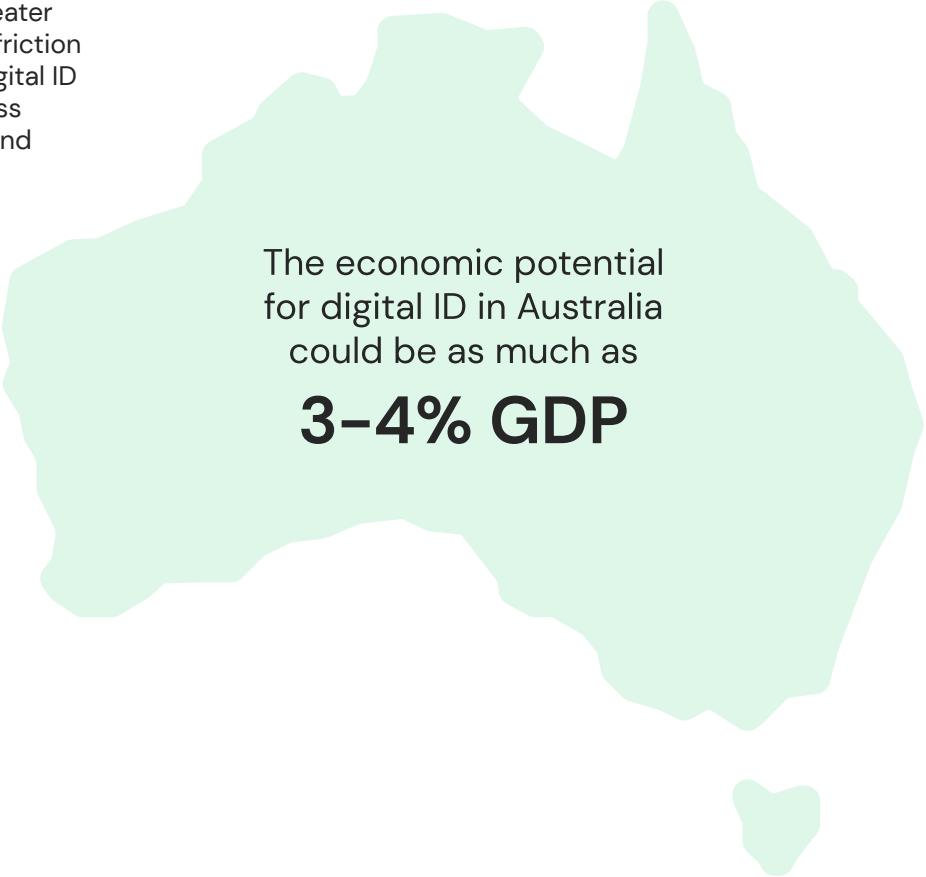
When looking at the broader economy, the cost to the federal government to keep citizens and businesses safe from data breaches and cyber-attacks more generally has skyrocketed to \$1.67 billion.⁹

All of these costs can be tackled through the enablement of a well-designed digital ID solution.

Economy

For governments, digital ID enables greater trust in the digital economy, reducing friction and accelerating economic growth. Digital ID also supports digital enablement across the economy, regulatory compliance and fraud reduction.

For Australia specifically, digital ID supports upcoming Consumer Data Right reforms as well as potential privacy and security policy initiatives which are likely to evolve. Together, the direct Australian consumer and commercial benefit of digital ID has been estimated at approximately \$11 billion¹⁰ per annum and may be as much as 3-4% of GDP¹¹ if the economy-wide benefits follow in the same vein as other developed economies such as the UK or US.



The economic potential for digital ID in Australia could be as much as

3-4% GDP

6. Office of the Australian Information Commissioner 7. IBM 8. Federal Register of Legislation 9. Department of Home Affairs 10. Australia Post 11. McKinsey Global Institute



What is the current state of play in Australia?

Australia has a well-developed digital economy, with the previous federal government focused on a strategy to make it into the top 10 digital economies by 2030.¹² Important investment in infrastructure and network access has helped achieve national digital inclusion and ability rates of 71.1% and 64.4% in 2021 but it is worth noting that progress has not been equally distributed across the population with inclusion rates dropping to 57.4% and 47.4% for those aged 65–74 years and 75+ years old respectively.¹³

Despite this divide, digital capabilities across public and private sectors have become more sophisticated. Having recognised the opportunity presented by digital ID some time ago, both government and private sector stakeholders have already invested in initiatives to advance digital ID in Australia, with the government's total investment from 2015 to 2022 amounting to more than \$600 million.¹⁴

Federal

At the federal level, this investment has included the creation of myGovID for identity verification to access government agency services and the Digital Transformation Agency's development of the Trusted Digital Identity Framework (TDIF), an accreditation scheme for digital identity services.

State

At the state level we have seen various initiatives to digitise identification documents and other credentials. For example, Service NSW and Service SA have both launched digital driver licenses, with Victoria and Queensland expecting to rollout similar programs in 2023 and 2024.

More broadly, the Queensland government released a Request for Proposal in December 2022 to develop a digital ID strategy and roadmap while Service NSW recently announced the selection of Mattr as its technology partner for a whole-of-government digital ID platform.¹⁵

Private

We have also seen solutions developed by the private sector, such as ID by Mastercard, Australia Post's Digital ID and a digital wallet from MEECO for storing verified credentials. There are also more traditional identity verification services for regulated know-your-customer use cases, but these can be costly and generally offer end users limited transparency into how their PI is being used.

While initiatives to date have been helpful in advancing digital ID in Australia, they have created a fragmented landscape which limits the realisation of the benefits listed above. Public sector digital ID platforms can generally only be used for government services or within state-based boundaries, while private sector solutions have targeted specific use cases and therefore have had limited adoption across the population. With the current federal government set to invest an additional \$26.9 million in 2023–24 to further expand the country's digital ID capabilities,¹⁶ and leveraging this investment to support its ambition of making Australia the most cyber secure nation in the world by 2030,¹⁷ we must focus on initiatives which address this fragmentation.



12. Department of Prime Minister and Cabinet 13. Australian Digital Inclusion Index 14. Shah, R 15. Saarinen, J 16. Commonwealth of Australia 17. Department of Finance



How can we realise our full potential?

To move Australia from its current state of play and unlock its full potential, building solutions which solve for fragmentation through a variety of use cases while keeping Australians' data secure will be crucial. We identify some common design characteristics which any such solution should consider to support this future success in Australia:

Coverage



For any digital ID system or service to be relevant, it must be able to cover a large majority of people needing to identify themselves. Rather than a single, monolithic approach to digital ID, a better approach to ensure broad coverage is to create an ecosystem of diverse identity providers (IDPs) which brings together trusted institutions (e.g., banks, telcos and government identity issuers) to provide identity services.

Re-usable ID and secure authentication



A service that requires an individual to create a new digital ID through a registration or verification process can limit uptake. An alternative is to draw on and reuse existing, verified identity data stores held by trusted institutions such as banks and government agencies. By designing a solution that also relies on the authentication mechanism of these trusted institutions (e.g., using a bank log in to authenticate a user for completing their identity verification), the solution can leverage their significant investment in cyber security while providing customers with a trusted and familiar experience.

Choice and interoperability



To maximise relevance and usage, a digital ID system ideally provides both choice and interoperability. End users should have a choice of IDPs to maximise coverage but also to allow individual choice at a transaction level (a person may be comfortable using a government agency to verify their ID for access to a new government service but not renting a property). An ecosystem that provides interoperability with a variety of IDPs gives greater consumer choice.

Privacy



As the recent high-profile data breaches in Australia have shown, protection of PI and privacy is vital. There are several considerations for a successful digital ID system here:

a) Data minimisation

To minimise the amount of PI data captured by a RP, a well-designed digital ID platform can provide a digital attestation (also known as an assertion or zero knowledge proofs) from an IDP to the RP that a particular identity attribute matches a given condition. For example, it can allow a RP to store an 'over 18' flag rather than a customer's date of birth.

b) No new data silos

PI can also be protected if we avoid the creation of new data repositories. Approaches to digital ID that leverage existing, well-protected stores of data (e.g., bank systems or government ID issuers) avoid new targets for hackers.

c) Consent

Another important aspect of privacy which must be considered for successful digital ID design is visibility and ownership. A user should know what information about them is being shared and with whom. This can be addressed by providing a user with the ability to give explicit consent to share any identity attributes or assertions as part of a verification transaction.

d) Systemic privacy

In addition to the mechanisms above, a modern digital ID system should define overarching rules that govern the use of the system and PI. This is typically done through a set of scheme or network rules that specify privacy protections, liability management and operational processes to support fraud management and ID recovery.

Flexibility



Finally, to be successful in today's rapidly moving digital landscape, digital ID systems must have the flexibility to evolve. Technical 'futureproofing' can be supported through open approaches with minimal proprietary customisation that support domestic and global interoperability. Transparent and inclusive governance mechanisms are also important to provide the appropriate feedback loops required for ongoing innovation and evolution.

There are other insights and success factors which should be considered in the design of an effective, economy-wide approach to digital ID. For example, the need to address the current digital divide in Australia and ensure vulnerable groups are appropriately educated and not excluded from use, alongside the harmonisation/evolution of digital ID-related regulation and legislation. However, the characteristics listed above will best help us to realise the full potential for digital ID in Australia.

Where to from here?



Australia has made inroads towards enabling digital ID across the economy. However, as outlined above, current investment has only moved the needle so far. For digital ID to be truly successful in Australia, we must focus on economy-wide solutions which make it relevant and useful to a broad population, while prioritising security and privacy to deliver the trust and confidence required by end users and relying parties.

This cannot depend on any one organisation or the design of their solution. Given the complexity and ubiquity of identification requirements across the entire economy, collaboration across public and private sector is a must. Doing so with urgency is necessary to prevent further nation-wide cybersecurity fallout. If achieved, we may then see the trusted digital ID infrastructure that Australia deserves.



References

Australian Digital Inclusion Index, Key Findings and Next Steps, 2021,
<https://www.digitalinclusionindex.org.au/key-findings-and-next-steps/>

Australia Post, A frictionless future for identity management, December 2016,
https://auspost.com.au/content/dam/auspost_corp/media/documents/digital-identity-white-paper.pdf

Biometric Update, Survey suggests digital ID could reduce high onboarding abandonment rates, June 2019,
<https://www.biometricupdate.com/201906/survey-suggests-digital-id-could-reduce-high-onboarding-abandonment-rates>

Commonwealth of Australia, Growing the economy: Modernising our economy and maximizing our strengths, May 2023,
<https://budget.gov.au/content/O3-economy.htm>

Commonwealth of Australia (Digital Transformation Agency), Trusted Digital Identity Framework (TDIF): O2 – Overview, 2023,
https://www.digitalidentity.gov.au/sites/default/files/2023-03/tdif_o2_overview_-_release_4.8.pdf

Department of Finance, Data and Digital Ministers meeting Communique , November 2022,
<https://www.finance.gov.au/sites/default/files/2022-11/data-and-digital-ministers-meeting-communique-41122.pdf>

Department of Home Affairs, Australia's Cyber Security Strategy 2020, Last updated February 2023,
<https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020>

Department of Prime Minister and Cabinet, Digital Economy Strategy 2022 update, March 2022,
<https://www.pmc.gov.au/news/digital-economy-strategy-2022-update-released>

Federal Register of Legislation, Privacy Act 1988, December 2022,
<https://www.legislation.gov.au/Details/C2022C00361>

IBM, Cost of a Data Breach Report 2022, July 2022,
<https://www.ibm.com/downloads/cas/3R8N1DZJ>

McKinsey Global Institute, Digital Identification: A key to inclusive growth, April 2019,
<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>

Norquay, J., Australian Internet Statistics 2023, Prosperity Media, January 2023,
<https://prosperitymedia.com.au/australian-internet-statistics/>

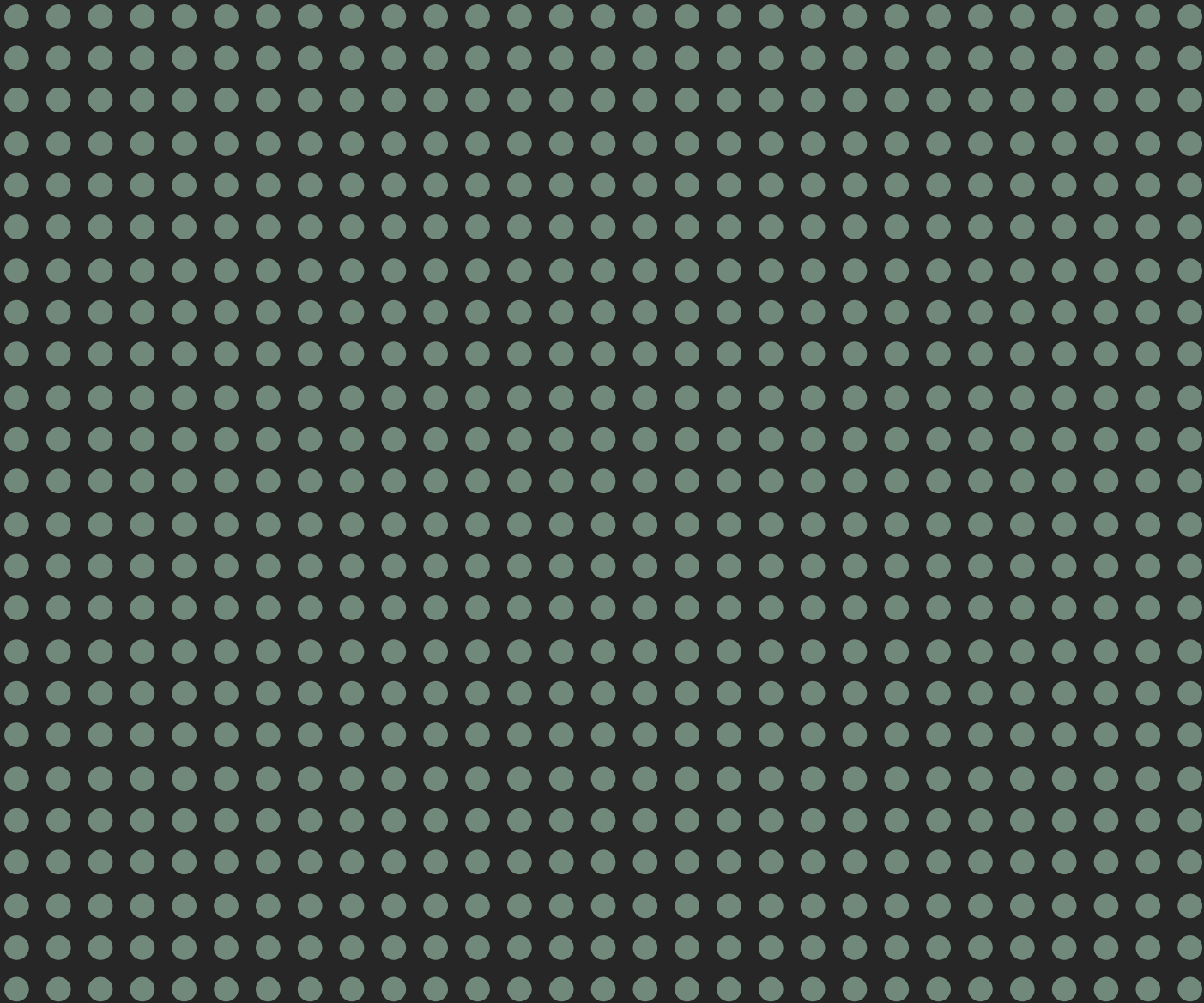
Office of the Australian Information Commissioner, Notifiable Data Breaches Report: July to December 2022, March 2023,
https://www.oaic.gov.au/__data/assets/pdf_file/0026/39068/OAIC-Notifiable-data-breaches-report-July-December-2022.pdf

Saarinen, J, NSW govt appoints MATTR as technology partner for Digital ID, CRN Australia, April 2023,
<https://www.crn.com.au/news/nsw-govt-appoints-mattr-as-technology-partner-for-digital-id-592922>

Shah, R, The Future of Digital Identity in Australia, Australian Strategic Policy Institute, November 2022,
<https://www.aspi.org.au/report/future-digital-identity-australia>

Tesfaye, M, Digital Identity and the future of banking: How digital identity can slash the costs of onboarding and regulatory compliance by up to 70% for banks, February 2020,
<https://www.businessinsider.in/finance/news/digital-identity-and-the-future-of-banking-how-digital-identity-can-slash-the-costs-of-onboarding-and-regulatory-compliance-by-up-to-70-for-banks/articleshow/74336913.cms>





For more information:

✉ hello@connectid.com.au

🌐 connectid.com.au

©ConnectID is a registered trademark of eftpos Digital Identity Pty Ltd 80 648 970 101
©2023 Australian Payments Plus. ABN: 19 649 744 203. All rights reserved