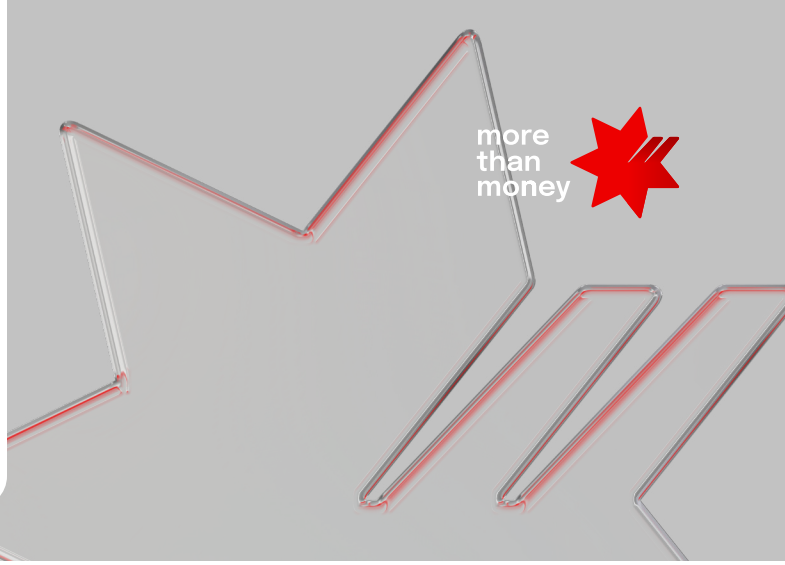
Digital ID
Design Sprint



Executive Summary

NAB hosted a two-day Digital ID Design Sprint with the goal of bringing together leading thinkers in the field of Digital ID.

The Sprint identified and articulated the key elements of a well-functioning Digital ID ecosystem, the barriers we currently face and recommendations on how Australia may overcome these challenges as it implements Digital ID. This paper summarises the activities and discussions from the Design Sprint.

Central to the conversation were four key themes: adoption, data minimisation, interoperability, and inclusion.

Encouragingly, none of the barriers or challenges identified by the group were considered to be insurmountable, with many of the calls to action focusing on the need for attitudinal and cultural change within organisations and Government, and the need for education more broadly on Digital ID to build trust.

The importance of co-creation between industry and Government, and participation across all parts of civic society was also emphasised, as Australia builds Digital ID infrastructure, which will likely become a critical tool for minimising Australia's cyber risks and encouraging productivity in our economy.

Our calls to action following the Design Sprint are as follows:

1. Banks and other trusted Digital ID providers need to act with a sense of urgency in order to provide options for consumers and citizens and each play their part to build trust and resilience in Australia's Digital ID infrastructure.

2. Government policy needs to recognise that a singular focus on public sector Digital ID solutions will not be the panacea in Australia. To respect an individual's agency and right to choose, Government policy and actions need to encourage and enable trusted private sector and community-led Digital ID providers to exist alongside Government Digital ID offerings.

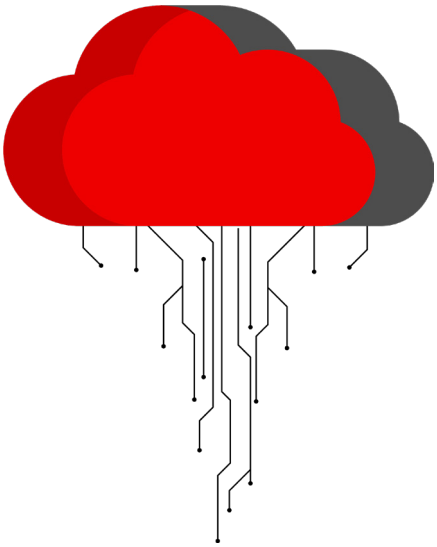
3. For adoption of Digital ID solutions, policies and Digital ID solutions need to be underpinned by user choice and convenience. By listening and implementing a community centred design approach (as one example a First Nations' Australians led approach) precise needs will be surfaced, enabling trust, and facilitating adoption.

4. Government, industry and the community need to work together to co-create a Digital ID framework that best meets the needs of the nation. We should learn from the successes of other jurisdictions and create a role for a Digital ID co-ordination and implementation body in Australia, leveraging the most favourable aspects of such bodies as the Digital Identity and Authentication Council of Canada ('DIACC') and the UK's Open Banking Implementation Entity Body ('OBIE').

Whilst these calls to action do not reflect the individual views of any one participant in the Design Sprint (and noting that there may be disparate views regarding the journey to Australia's ultimate Digital ID ecosystem), we note the observation that there was broad consensus around the vision for the ecosystem and actions in the interests of the Australian Digital ID ecosystem generally.

NAB would like to sincerely thank all of the experts who generously shared their knowledge and time across two full days). Without each of your insights and contributions, the creation of this work would not be possible.

NAB will continue to champion a Digital ID ecosystem, which is designed with users at the centre, with world leading qualities which embrace the lived experience and uniqueness of all parts of our community. Next year we will convene further initiatives on Digital ID, including broadening our focus to cross-border issues and corporate ID challenges and opportunities.



Introduction

There is growing urgency around implementing a well-functioning Digital ID ecosystem in Australia to help combat the rising fraud and scams epidemic by minimising the amount of personal data being unnecessarily collected and stored and to also support increased productivity in the Australian economy.

In support of this, NAB has launched a number of initiatives in relation to Digital ID. One such initiative was a Digital ID roundtable with leading thinkers in the field, focussing on privacy, security, and customer centricity, plurality of digital identification systems and access and inclusion, convened earlier in the year. Arising out of the roundtable was a recommendation from Government for NAB to initiate a Design Sprint on Digital ID.

The Design Sprint was held over two days at NAB's Melbourne and Sydney offices and brought together participants from industry, academia, consultants, consumer advocates, regulators, and Government. Day one comprised use-case focussed workshops, whereas on Day two participants directed their attention to policy challenges and recommendations. The purpose of this paper is to document and summarise key recommendations from the group as they relate to the necessary ingredients for Australia to establish a successful digital ID framework.

As the sessions were held under Chatham House Rule, comments are unattributed. Please note that the opinions expressed herein are the personal views of the participants and do not necessarily reflect the official views of the organisations represented, including NAB.

[1] A summary of the Roundtable discussion can be found here: Experts discuss the future of digital identity - NAB News.

Thematic overview of the Digital ID Design Sprint

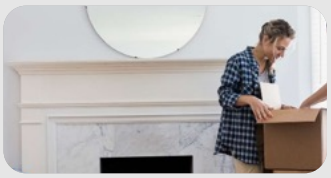
Day one of the Design Sprint focussed on five priority use cases, where Digital ID solutions could assist in minimising privacy risks and enhancing productivity, namely:

- Residential rental applications;
- Proof of age for alcohol delivery;
- Employee onboarding;
- Social media/online personas & e-commerce; and
- Government payments in emergencies.

Through the lens of user stories (a snapshot of which can be found below) participants directed their attention to the status quo and the way in which identification or attribute verification is currently conducted in each of the use cases. Working in teams, participants engaged in design thinking methodologies to identify key problems across each of the use cases. For the second half of the day, participants focussed on how digital ID solutions may address some of these common issues.

Rental Applications

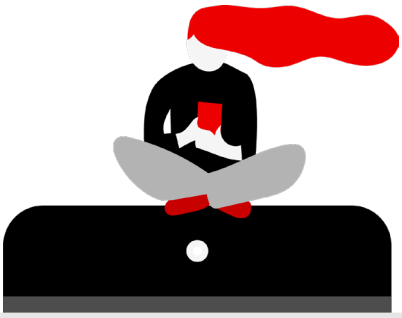
User story
Olivia



Olivia is a 37-year-old mother of two young boys. She lives in a rental property in the eastern suburbs of Melbourne. Her tenancy agreement is shortly coming to an end, and she is currently in the process of applying for a new residential lease.

"There are so many hoops to jump through just to secure a roof over our heads."

"I'm time poor and need a solution that is safe and trustworthy."



Proof of age

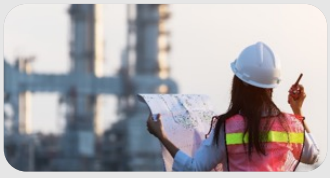
User story
Tania

Tania and her partner are ordering some takeout and alcohol from an online delivery service. The delivery driver cannot leave the alcohol without proof of Tania's age and requires a photo of her drivers' licence to be scanned to his phone.

"I'm worried that a photo of my drivers' licence is being scanned via a delivery driver's phone."

Employee Onboarding

User story
John and the Hiring Manager



John is a new migrant to Australia, with 10+ years' experience and receives a job offer at a mining site in Qld. He's required to undergo a rigorous probity process which the mining company undertakes via a third party, requiring health information and criminal checks. This process is also time consuming as his credentials are not immediately recognised because they don't match the standard Australian format.

"I really want this job, so I don't have any choice other than to provide all of the information they're asking me for."

"We're so short staffed at the site – we can't afford to wait another week for the onboarding process."

Online Personas/ e-commerce/Social Media

User story
Jan and Peter

Jan and Peter are celebrating their wedding anniversary and decide to take a trip to far north Queensland. They find a gorgeous rental online with a number of positive reviews. When they arrive, it doesn't look anything like the photos. Cyber-criminals have been creating fake property rental listings, using fictious profiles and data scraped from the web. Utilising AI, they can 'chat' with potential customers making it hard to detect that the listing is actually fake. Once they receive payment, they often delete the listing and repeat the scam again and again.

"Everything about the online listing made it feel so real. We never suspected it was fake."

Online Personas/ e-commerce/Social Media

User story
Harry and his dad

Harry is 10 years old and loves playing games online, especially, 'Minetopia,' which allows him to chat with his friends whilst they're playing. At school pick up Harry's dad hears one of the other parents talking about Minetopia and reports of fake accounts being created by bad actors who trawl social media for photos of children and create fictious user profiles.

"How do I protect my child online?"

Government payments in emergencies

User story
Alannah and the Government Agency

Alannah's home in Victoria has been severely damaged by floods and the Victorian Government has officially declared the region in which she lives a disaster area. She's staying in emergency accommodation and may be able to access financial support to help recover. She needs to provide a suite of information and proof in order to get access to support. If Alannah is eligible, she will also need to provide her bank account details for the payment.

"We need this process to be secure and simple so that we're supporting the community quickly and safely"

Throughout the day, we heard some core cross cutting themes which were of critical importance to address in relation to Australia's Digital ID ecosystem. These were:

- Adoption
- Data Minimisation
- Interoperability
- Inclusion

On Day two of the Sprint, participants drilled down in relation to these core themes, by asking:

- What are the enablers of adoption; data minimisation; interoperability and inclusion within Australia's Digital ID ecosystem?
- What are the barriers to achieving these core ingredients of a well-functioning Digital ID?

From these discussions participants distilled recommendations addressing each core theme. The next sections of the paper set out the challenges and recommendations as they relate to each theme in turn.

Core themes

(A) Adoption

What are some of the current barriers we face in Australia to adoption Digital ID services?

Addressing this question, the following key issues were put forward:

- For businesses, there are commercial hurdles to adopting Digital ID solutions. It was noted that business leaders need to be 'decision ready' given there is likely to be a long-term investment in infrastructure, including for example costs to digitally transform and migrate to new technologies. Participants spoke of the requirements in respect of digitising legacy industries and services, which may have or 'no' tech solutions for customer onboarding.
- From an individual's perspective a key issue is that of trust. Many citizens and consumers have concerns regarding the privacy and security of their data. They may also be apprehensive regarding the potential for digital identification schemes to be used as tools of surveillance. These concerns may arise from a number of factors, including mistrust in prior proposed Government-identification schemes, opacity regarding data governance practices of participants and a perceived lack of redress options if things go wrong.
- Excessively fragmented Digital ID solutions with poor interoperability was also noted as a key a challenge to adoption as participants voiced their views that it would lead to friction in adopting, integrating, and onboarding for users. It was noted that fragmentation would lead to poor utility (particularly of Government issued credentials), poor reliability and ultimately barriers to choice, which would lead to confusion within the community as to which solutions should/could be used.
- Finally, participants called out the legal and regulatory landscape and posed an open question as to whether the law is permissive of adoption of Digital ID. Although no comprehensive overview of the legal and regulatory landscape emerged from the discussion, participants were comfortable to state that there may be aspects of the law that were 'blockers' and some that are 'enablers.'

Recommendations

To address the challenges of adoption, the following recommendations were canvassed.

- For adoption there needs to be trust in the system and to build this, participants recommended education about Digital ID, how it works and what are its benefits.
- Trusted brands utilising Digital ID and offering it to their customers was noted as another means of encouraging adoption. Alongside this, it was noted that Digital ID offerings should engage familiar patters or a 'ceremony of steps' and should be designed ground up with accessibility in mind, having regard to the needs of all users of the system.
- Digital ID needs to make sense commercially for industry to adopt it. Therefore, we need to ensure ease of adoption for parties, including that Digital ID is simple to use (and re-use). An example was given of the rise in adoption of contactless cards, due to their widespread acceptance in supermarkets.
- To get the best outcomes, it was noted that Government and industry should engage in co-creation throughout the legislative journey of Digital ID in Australia. It was agreed that public-private partnerships or pilots could feed into the legislative and governance systems design. To ensure that the regulatory landscape supports the adoption of Digital ID it was further noted that it will be important to understand industry-specific practices and legislation that may currently be a blocker to implementation.
- Cross market use cases which allow the ability to use Digital IDs across multiple countries for e.g., for migration, security for cross-border eCommerce and online chat interactions.
- There should be a consistency and simplicity in the message.

Participants:

- suggested education to an 'agreed level,' highlighting for example, the importance of the role of Digital ID in combatting fraud.
- spoke of the need for alignment in terminology and recommended that Government take a lead role in setting the appropriate language and level at which Digital ID is discussed to aid with consumer education.

(B) Data minimisation

What are some of the current barriers we face in Australia to data minimisation?

Data minimisation is an imperative for a well-functioning Digital ID. Participants considered the barriers to data minimisation in Australia and the following key issues emerged:

- Established behaviours were noted as a barrier to data minimisation. Attitudes such as "we've always asked for it and always kept it" and an overly narrow focus on legal requirements rather than putting your customer or citizen 'hat' on to consider what information is really needed in a given context were all noted as aspects of culture which present blockers to data minimisation.
- For industry, it was noted that there is often a lack of clear guidelines regarding what information they need to keep beyond minimum legal periods and what information, or data should be deleted or disposed of.
- The power imbalance, oftentimes weighted against individuals was also cited as another challenge to data minimisation. Renters in a highly competitive rental market, for example, are often not in a position to oppose collection of their personal data.
- A lack of technical capability or understanding of what data an organisation holds (and where such data is held) and not having adequate governance and a process in place to delete data post retention period and the costs of implementation, were also referenced.
- Finally, it was noted that there may be a lack of interest or a lack of capacity and resources for many small businesses to engage with data minimisation practices given the regulatory limits of federal privacy laws i.e., with some exceptions, not capturing small business operators.

Recommendations

Participants put forward the following recommendations to encourage data minimisation practices:

- Given the practice of over-retaining 'just in case,' industry and regulator engagement was also recommended to help companies better understand minimum document retention requirements for evidentiary and regulatory compliance purposes. With a view also that state and local authorities, Regulators, and industry guilds might all need to revisit the requirements that they currently make for data retention.
- There was also a recommendation to better utilise privacy enhancing technical solutions such as 'zero knowledge proofs' to avoid unnecessary data transfer and retaining evidence of the verification instead of the actual personal information.
- In line with recommendations arising out of the Government's review of the *Privacy Act 1988* (Cth), participants called for an 'audit' of current regulatory requirements, which may mandate organisations to retain records, for example the *Corporations Act 2001* (Cth) to determine whether these are still fit-for-purpose or should be amended to minimise the amount of data organisations currently hold.
- Tougher regulatory consequences for companies that are non-compliant with data deletion requirements was suggested as a means of encouraging greater adherence and preventing over-retention of information by organisations.
- Boldly, a nation-wide 'culture shift' was called for (i.e., 'it's ok to delete') leveraging the unique (and unfavourable) position that Australia holds, having experienced three very large-scale data breaches over the course of 2022 – 2023, which impacted millions of individuals. It was posited that Australia

should ensure that it does not miss the opportunity to learn valuable lessons from these events, chiefly that over-retention of personal information can be a business liability and presents a major cyber risk. A question was also posed as to whether consumer education could help drive cultural change, where individuals are better informed of their rights.

We recognise proposed reform of the *Privacy Act 1988* (Cth) which is currently underway and note that certain of the recommendations in respect of data minimisation and inclusion could be supported and enabled through various proposed changes to the *Privacy Act,* which have also been agreed in-principle by the Government.

(C) Interoperability

What are some of the current barriers we face in Australia to interoperability of Digital ID services?

Turning to interoperability, another core theme which was identified as being critical to Australia's Digital ID ecosystem, there were a number of issues that participants drew out as potential barriers.

- Attitudes of participants in the ecosystem was a theme that permeated the discussion, where participants noted that organisations with a narrow focus on commercial interest that prioritises potential competitive advantage likely to stifle interoperability. Alongside this, differing views amongst participants on who needs to change or converge (as the case may be) or participants that are not sufficiently willing to accommodate new players were also highlighted as challenges
- Existing ways of doing things and inertia and silos was noted as another barrier i.e., 'If one or two dominant players emerge, why bother?'
- Restrictive commercial models and high barriers to entry may also prevent interoperability between different solutions.
- Poor uptake or user engagement was referenced where it was unlikely that there would be sound commercial rationale to invest in interoperability where there was low consumer or citizen utility found in Digital ID solutions.
- Notwithstanding the fact that different firms or industries may need different data points, there was a view that parties could make solutions interoperate. However, knowledge gaps and a lack of awareness around common standards and frameworks which could be used was also described as blockers of interoperability.
- Lack of knowledge in dealing with different cultural and social aspects of identity was also considered to be a barrier to interoperability between different Digital ID solutions.

Recommendations

To encourage interoperability between different Digital ID solutions, the following recommendations were made:

Industry collaboration:

- It was noted that industry needs to convalesce around standards and to encourage iterated improvement and capability expansion. We note and acknowledge the efforts and work done by entities such as ConnectID in this regard. It was also suggested that Digital ID providers come together to provide a single integration point for relying parties, in a similar vein to the CDR.
- It was recommended that parties take the learnings from other large industry standards and processes such SuperStream and the Consumer Data Right.
- On collaboration, it was noted that an open co-ordination and implementation body could be established and that there is a need for a neutral "barn" for public and private sector to align on technical and commercial standards.
- It was noted that Government and Industry should come together to agree forms for redress and recourse where Digital ID solutions do not comply with mandated standards or where there is otherwise consumer harm.
- There was a call for proof-of-concept projects or pilots between Government and Industry participants. It was also suggested that industry

should support pilots of the Digital ID taskforce, even if these were intra-government and not involving private sector as there could be learnings for all parties which would ultimately benefit the system as a whole.

- Digital ID providers need to acknowledge that most citizens and consumers are likely to have multiple Digital IDs which they choose to use in different circumstances.
- Governments need to role model interoperability between State, Territory and Federal Digital ID providers.
- Government needs to ensure there is space for private sector Digital ID providers to participate and provide value for their customers.
- All participants will need to work together to ensure within the ecosystem overall there is resilience, monitoring and enforcement of conduct that does not meet regulated standards.
- If the phased approach for roll out of interoperability between private and public sector Digital ID solutions is pursued, Government needs to help provide certainty in the investment landscape for potential private sector Digital ID providers and Government needs to accept and encourage use of private sector Digital IDs to encourage interoperability.
- In relation to regulatory settings for Digital ID, the system needs to be open and contestable with incentives to innovate and differentiate services to provide more utility to users and ensure that there are options for users of Digital ID based on their preferences and the scenario.
- Finally, it was recommended that all parties need to maintain the urgency around their actions to support the implementation of an interoperable Digital ID ecosystem in Australia.

(D) Inclusion

Ensuring that services are inclusive and accessible to all those that may choose to use them is paramount to the success of Digital ID. Participants considered the barriers to inclusive Digital ID services and noted as follows.

What are some of the current barriers we face in Australia to inclusive digital ID services?

- Pushing a one size fits all approach is a barrier to the creation of inclusive Digital ID services as parts of the community may mistrust certain institutions and if there are a lack of alternatives this will diminish inclusion. One participant mentioned a specific example of an app intended to increase access to services for homeless youth. Its adoption was low and further research revealed a mistrust of the target audience of the intention of the app, and fear to be pulled into “the system” by Government.
- Where there is an inability to control information flow, it was noted that this would also lead to Digital ID systems being regarded as negatively impacting on an individual’s agency and self-determination.
- The technology itself could be a barrier also, as a number of Digital ID solution require access to a smart phone or authentication with devices using internet connectivity. In the case of remote and underserved communities where there are no alternatives to these kinds of technologies, it was noted that this will also be a barrier to inclusivity and accessibility.

Recommendations

- Participants called for education around Digital ID to ensure that there is a base level of community knowledge and awareness around how Digital ID technologies work and what are the benefits and potential risks. It was also recommended that there be Government ‘trust marks’ for Digital ID solutions that meet required regulatory standards and that safety of any Digital ID solution needs to be demonstrable e.g., 5-star rating.
- Participants emphasised the importance of making use of Digital ID solutions voluntary and not allowing for the mandating of use by industry or Government.
- Ensuring customer and citizen choice was also

recommended a key driver for inclusion (both in terms of choice of a Digital ID provider and choice of whether to use a Digital ID solution at all).

- Participants urged for the need to consider accessibility wholistically and comprising (amongst other factors):
    - Affordability i.e. device access; and
    - Accessibility for people living remotely, for those with a disability, older cohorts, non-English speaking backgrounds
- It was recommended that Government and Industry partner with organisations which could validate attributes beyond date of birth, name and address. In the case of First Nations' individuals, it was noted that people need to have a choice of options they can connect with, for instance connection with land and family. Whereas the current construct and form of identification is 'westernised,' we need to consider other paradigms and ways of thinking of ID where one participant noted that in certain Indigenous cultures privacy may be 'bound into specific environments.'
- Participants also spoke of the need to consider the concept of avatars and anonymity when needed. In certain online environments, the ability to define an avatar that abstracts from the actual person was considered important to provide safety through a lack of judgement and abuse.

  We acknowledge that ConnectID and Hold Access have recently announced a partnership to accelerate the deployment of (WUNA) a digital wallet to be included in the trusted ConnectID network, with the goal of empowering First Nations Australians and those who are digitally excluded to overcome digital accessibility barriers through improved ID verification.

Conclusion and next steps

Digital ID has the potential to minimise privacy risks, build cyber resilience, and encourage productivity in the Australian economy.

Implementing Digital ID in Australia is a collaborative effort between Government, the private sector and community led organisations, each playing an important role in ensuring our Digital ID framework and infrastructure is resilient, meets community needs and is fit for purpose.

We heard some key recommendations and calls to action, which we summarise below:

1. Trust and utility will drive adoption of Digital ID in Australia. Therefore, we need policy settings which will encourage trusted organisations to build Digital ID solutions and support the commercial viability of Digital ID.

2. To drive data minimisation, which is urgent and necessary to combat the prevalence of digital fraud and scams, we need a bold nationwide 'culture shift' to minimise the amount of personal data that is collected and retained. This shift needs to be backed by clear and strong regulation and enforcement.

3. Industry, Government, and civic society need to collaborate on the governance, co-ordination, and implementation of Digital ID. Doing so is essential to the success of Digital ID in Australia and we should consider a role for a body such as Digital Identity and Authentication Council of Canada, or the Open Banking Implementation Entity for Digital ID in Australia.

4. A one size fits all approach will not serve all parts of our community and we have an opportunity to learn from past failures and not repeat those by creating Digital ID frameworks and infrastructure that is accessible and inclusive. This will give us world leading capabilities and unlock Australia's greater potential.

NAB is committed to continuing our efforts on Digital ID and we intend to convene further initiatives on this important topic. NAB's efforts to facilitate the conversation will include broadening our focus to cross-border issues and corporate ID challenges and opportunities.