Australian Government
Digital Transformation Agency

dta

Digital Identity Legislation

A legislative framework for establishing permanent governance structures and privacy protections for the Digital Identity system

Background Paper

Digital Transformation Agency

Version: 18

1. Background

In 2014, the Australian Government's Financial System Inquiry highlighted a fragmented approach to identity verification in Australia, resulting in significant costs to individuals, businesses, and the Australian economy.[1] The Inquiry recommended a national identity strategy that would improve efficiency and security across the digital economy.

Since 2015, the Australian Government has been developing a Digital Identity system that will provide individuals with a simpler, safer and more secure way to verify their identity online.

As of October 2020, the Digital Identity system is used by over 1.7 million Australians and 1.2 million businesses to access over 70 government services.

The purpose of the Legislation is to establish permanent oversight and governance structures for the system, as well as enshrine in law a range of privacy and consumer protections, enabling the Digital Identity system to be used confidently across federal, state and territory governments as well as the private sector.

The purpose of this Background Paper is to provide general information about the Digital Identity system, as context for those reading the Digital Identity Legislation Consultation Paper.

2. What is a Digital Identity?

A Digital Identity is a simple, safe and secure way for Australians to prove who they are online. It only needs to be created once, by completing the digital equivalent of a 100-point ID check at a government shopfront or Post Office, to allow the ability for people to access and receive a range of services wholly online.

Australians can reuse their Digital Identity to securely access connected services, for faster, cheaper and easier transactions. Individuals save time and money. Small and medium enterprises have more time to manage and grow their business.

1 The Australian Government the Treasury, 2014. Financial System Inquiry Final Report, The Australian Government the Treasury, Canberra, https://treasury.gov.au/publication/c2014-fsi-final-report

3. What a Digital Identity is not

A Digital Identity is not a single, universal or mandatory number, or an online profile. User information remains private and protected. Users are asked for consent before any of their personal details are shared with the service they are trying to access.

Creating a Digital Identity is voluntary. It is not a replacement for physical documents such as a birth certificate, visa, driver's licence or passport. Australians who cannot or do not want to use a Digital Identity can continue to access government services over the phone or face-to-face at government shopfronts.

4. Benefits of the Digital Identity system

The Digital Identity system is designed to make accessing government and private sector services easier, faster and more convenient for Australian people and businesses.

It will safeguard privacy by sharing only relevant details (compared with handing over an identity document in person). It will strengthen the security of digital services and help prevent fraud and identity theft when Australians interact online.

As the Digital Identity system evolves, it will save time and money for more and more individuals, including:

- students who need access to education records and government assistance
- apprentices who have started work and training
- business owners and people who are starting a new business
- job seekers accessing government support
- families who need access to government payments and services.

For businesses, using a Digital Identity will:

- allow them to access participating government online services
- give them control over who can work on behalf of their business online
- save them time, with fewer identity verification processes
- protect identity and business information and prevent unauthorised access.

As demonstrated throughout the COVID-19 pandemic, technology plays a critical role in enabling people and businesses to deliver and receive trusted services in times of crisis.

Proving identity online is critical for digital services. Expanding Australia's Digital Identity capability will improve efficiency, reduce the costs associated with delivering and accessing services, and contribute to economic recovery.

The following case studies describe how a Digital Identity could be used to access government services in a range of different circumstances.

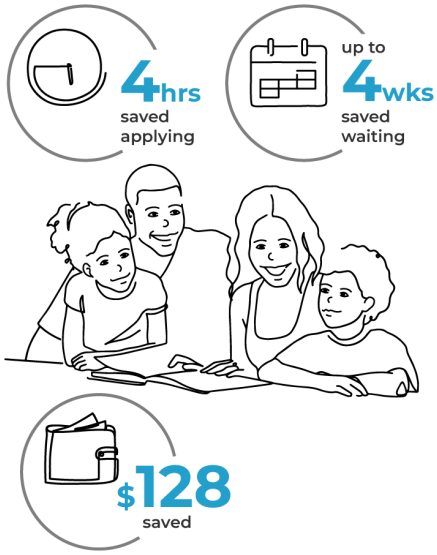
Case study: Regional families affected by natural disaster

In the future, Digital Identity will help families affected by natural disaster to save time and money.

Henry is a farmer who has been reluctant to use online government services in the past, preferring to make an hour-long drive to visit a Services Australia service centre or an Australia Post shopfront instead.

After battling extreme drought, Henry decides it is time to use government services online and creates his Digital Identity so he can quickly set up new online accounts. He can no longer afford to spend hours on the road when he needs to be on the farm.

When a bushfire tears through the family property and destroys his family's birth certificates and passports, Henry realises the value of his Digital Identity. With his Digital Identity, he doesn't need to wait for replacement documents and he can still access all of the government services he needs.



In the future, by using Digital Identity, a family affected by a natural disaster can save $128 in avoided costs and four hours applying to replace identity documents and driving into town to apply for assistance. They save up to an additional four weeks by not having to wait for new identity documents to be created and sent before they can apply for assistance.

Before Digital Identity, Henry had to:

01 Replace primary identity document
120 mins

02 Lodge application for disaster assistance
30 mins

03 Replace secondary identity document
120 mins

04 Provide supporting documents for claim
60 mins

Total 330 mins

But with Digital Identity, Henry can:

01 Lodge application for disaster assistance
30 mins

02 Provide supporting documents for claim
60 mins

Total 90 mins

Potential time saved is four hours. Save up to an additional four weeks by not having to wait for new identity documents to be created and sent before applying for assistance.

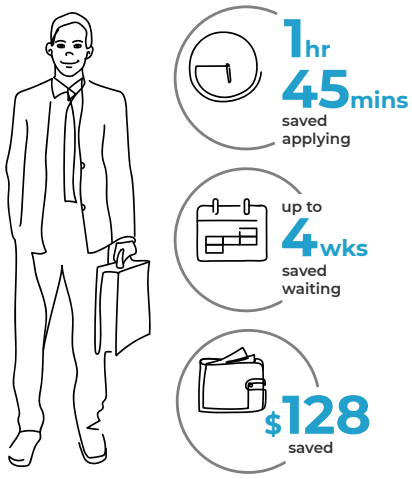
Case study: Starting a new business

In the future, using Digital Identity will help new business owners to save time and money.

Alex is an IT specialist who decides to fulfill his long-term ambition of starting his own small business. He wants to get his new business off the ground as quickly as possible, particularly because he is the primary earner in his family.

Alex has a number of steps to complete, including applying for an Australian business number (ABN) and registering his business name.

A former colleague urges Alex to use Digital Identity. Alex finds the process takes a quarter of the time it otherwise would have. He also saves $128 in avoided costs.



In the future, by using Digital Identity, a new business owner can save $128 in avoided costs, and one hour and 45 minutes by not having to post certified documents to the Australian Business Register for review and processing. An additional four weeks is saved by not having to wait for identity documents to be manually reviewed and processed.

Before Digital Identity, Alex had to:

01 Register online to:
- create new ABN
- register for GST
- register for PAYG
- register business name

15 mins

02 Post certified documents to Australian Business Register for review and processing

105 mins

03 Login to online business profile and manage who is authorised to access account

15 mins

Total 135 mins

But with Digital Identity, Alex can:

01 Register online to:
- create new ABN
- register for GST
- register for PAYG
- register business name

15 mins

02 Login to online business profile and manage who is authorised to access account

15 mins

Total 30 mins

Potential time saved is one hour and 45 minutes. Save up to an additional four weeks by not having to wait for identity documents to be manually reviewed and processed.

5. How is the Digital Identity system being used in Australia?

Over 1.7 million Australians and 1.2 million businesses already use Digital Identity to access over 70 government services.

While initially focused on Federal Government services, we are working towards Digital Identity being a whole-of-economy solution. This will connect state and territory and private sector services, making things easier for everyday Australians and businesses.

The Government's bushfire and COVID-19 responses highlight the importance of Australians being able to prove who they are online. Using Digital Identity, Australian businesses have been able to use myGovID to apply for JobKeeper online.

A number of Digital Identity providers already operate in Australia. This includes Australia Post's Digital iD service, which provides digital verification services for a range of public and private sector organisations including Airtasker, banks and foreign exchange services. The passage of Digital Identity Legislation will make it easier for these types of relying parties and Digital Identity providers to participate in the Digital Identity system.

6. The Trusted Digital Identity Framework

The Trusted Digital Identity Framework (TDIF) provides the tools, rules and accreditation criteria to protect the Digital Identity system. The TDIF specifies the minimum standards entities must meet to become a part of the system. This includes security, privacy, accessibility, usability, service operations and technical integration matters.

The TDIF also creates the technical framework within which the Digital Identity system operates.

The TDIF applies strict standards to the way the Digital Identity system works, by:

- defining requirements for the proper operation of the system
- defining the roles and operating responsibilities of system Participants
- providing assurance regarding usability, privacy, security and interoperability of its processes and data.

The TDIF has been developed, and is continuously iterated, in collaboration with key stakeholders including government agencies, peak industry bodies, privacy commissioners, state and territory governments and the wider public. It is also consistent with international standards such as ISO standards, OpenID Connect, Security Assertion Markup Language (SAML), FIDO Biometrics Framework and the NIST Digital Identity and Authentication standards.

To date, there have been more than 5,500 contributions from stakeholders in the development of the TDIF from across the technology, privacy and consumer sectors.

More detailed information on the framework and specific policy documents is available at www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework/framework-documents

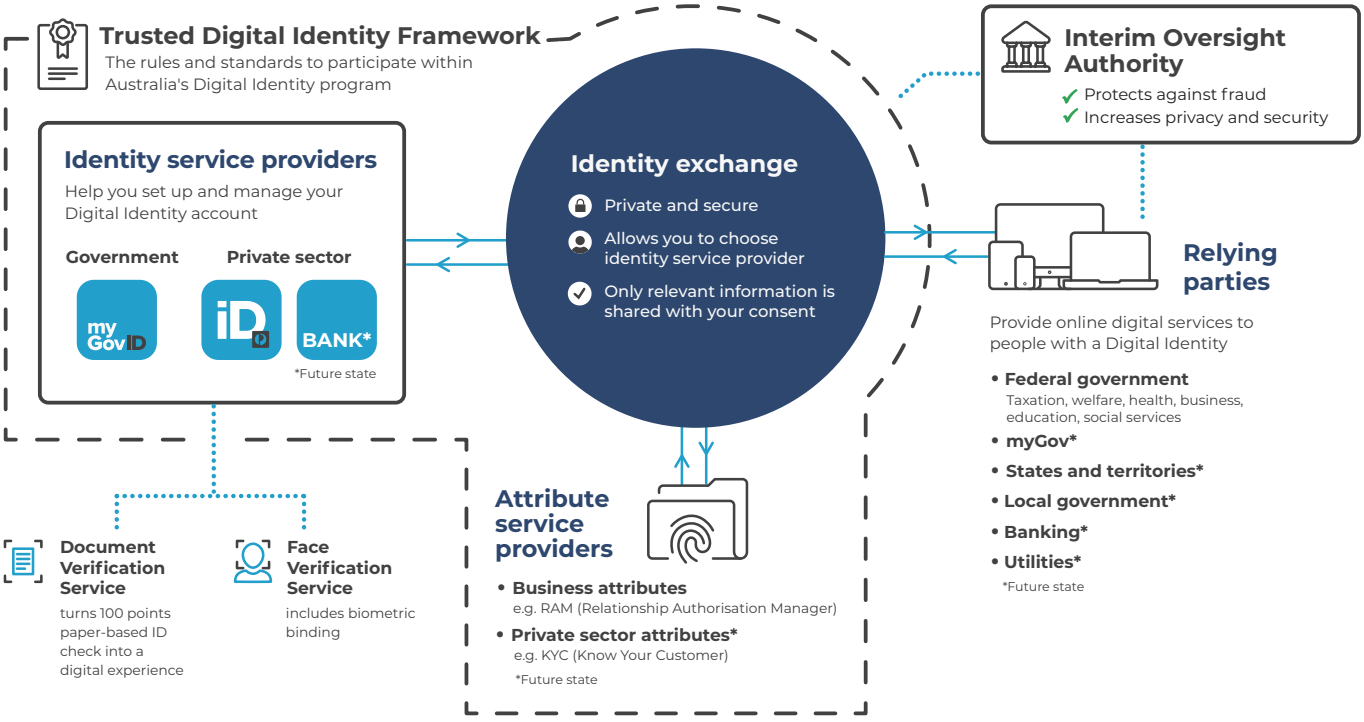
7. Participants within the Digital Identity system

The Digital Identity system is comprised of four types of Accredited Participants:

1. **Identity providers** – identity providers help you set up and manage your Digital Identity account. If you choose to create and use a Digital Identity, your identity provider will be your gateway into the Digital Identity system. Examples of identity providers are myGovID and Australia Post's Digital iD service.
2. **Attribute service providers** – to access certain kinds of services, you may be required or wish to provide more detailed identity information (such as the fact that you have a degree or qualification). Attribute service providers are entities such as professional bodies or universities that can provide, with your consent, this kind of authoritative information.
3. **Credential service providers** – credential service providers play a critical role in keeping the system secure and safe. They take care of all credentials (that is, passwords and other forms of access restrictions) used in the system.
4. **An identity exchange** – an identity exchange facilitates interactions between Accredited Participants to occur in a way which is secure and respects your privacy. The identity exchange acts like a switchboard: transferring information, with your consent, between relying parties, identity service providers and attribute service providers. The identity exchange only passes on the specific information which you consent to be shared – nothing more, nothing less. In this way, the identity exchange incorporates privacy by design and helps protect your personal information.

In addition to the four types of Accredited Participants in the system, *relying parties* are approved services that provide online digital services to people with a Digital Identity. This can include government or private sector services. Relying parties rely on the verification services provided by the other Participants within the system.

8. Digital Identity System



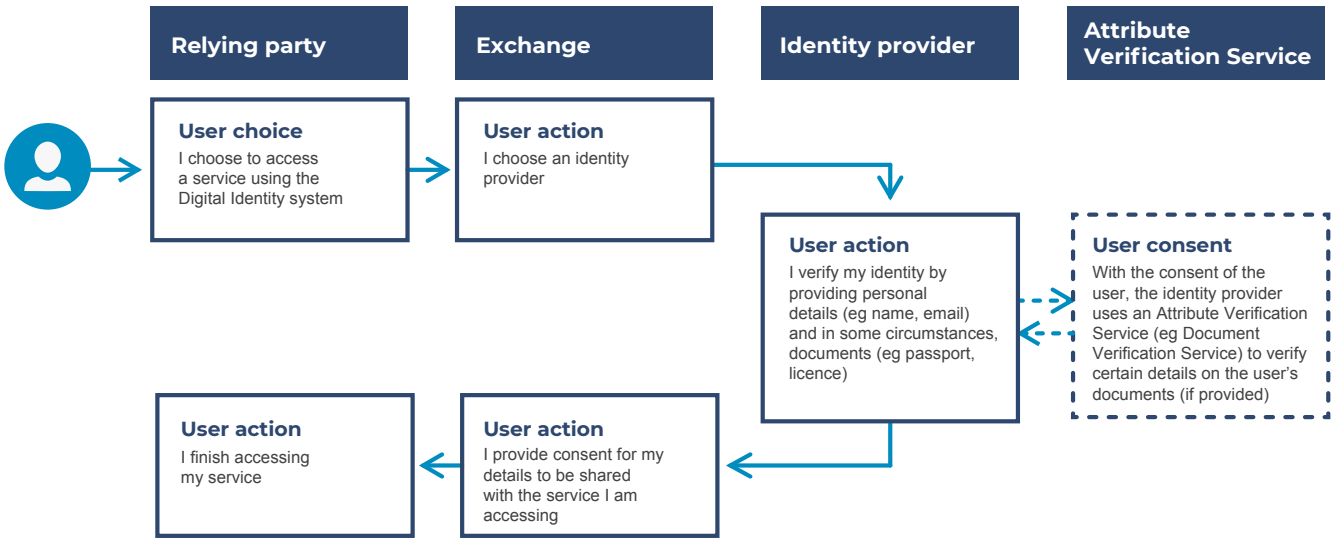
All Participants in the Digital Identity system – apart from relying parties and the Oversight Authority – are accredited against the TDIF, which sets out their ongoing requirements around privacy, fraud protection, security and identity proofing.

To fulfil their identity proofing requirements under the TDIF, identity providers will use existing services to help verify a person's name, date of birth and other details. The Department of Home Affairs' Document Verification Service (DVS) and Face Verification Service (FVS) are the two current attribute verification services that identity providers may choose to use. Although identity providers will use the DVS, FVS and similar services, such services are not part of the Digital Identity system.

The Digital Identity system does not create a central data store for additional identity information. The existing information is accessed at source and shared based on consent. When identity information is verified, the information is used to check a match and then discarded. This very important security and privacy principle ensures the Digital Identity system does not collect additional information that would make it a target of cyber attacks.

A more detailed description of the technical roles and responsibilities of Participants in the system is included in the Consultation Paper.

9. User journey across the system



10. Principles underpinning the Digital Identity system

The Digital Identity system is based on these core principles:

- **Choice** – creating and using a Digital Identity is voluntary. Users will have the option to select from multiple identity providers to verify their identity and access government and private sector services online.
- **Consent** – consent is required at multiple occasions when a person uses the system. A person must consent to set up a Digital Identity with an identity provider. The person's consent must also be obtained by the identity exchange before their Attributes can be passed through to a relying party. Furthermore, Users can withdraw consent for their Digital Identity to be used at any time, and opt out of the system through a process which is easy to understand and access.
- **Privacy** – safeguarding the personal information of Users is the single most important design feature of the Digital Identity system. Privacy-enhancing principles are embedded in its design and architecture, with a focus on:
    - limiting the collection, use and disclosure of personal information to a narrow purpose
    - minimising retention of information and keeping data stores separate
    - giving Users choice of how they verify their identity
    - giving Users control through consent and transparency.
- **Security** – is embedded in the Digital Identity system design. The TDIF includes specific security requirements which Participants must comply with to become and remain accredited. The system is protected by strict security protocols set by the Australian Government and all data is securely encrypted and stored in Australia.

- **Integrity** – the Digital Identity system is governed by an Oversight Authority which has a broad range of duties and powers with respect to the safety, reliability and efficient operation of the system. The Oversight Authority is responsible for operational system assurance for the Digital Identity system.

The passage of the Digital Identity Legislation will enshrine these principles in law. As it expands, the Digital Identity system will continue to:

- change the way online identity verification is achieved
- unlock economic value across the broader economy, and
- transform service delivery across Australia.