Using Digital ID for your business

Digital ID changes how businesses and organisations can collect, verify or store personal information. Relying on a Digital ID means you can replace your current processes for verifying a customer's or employee's ID with more streamlined processes that use far less personal information.

By using Digital ID, you may not (depending on your business's requirements under other legislation) need to collect and verify customer or staff identification, reducing the risk that your customer data is lost or stolen. Digital ID can also provide account authentication, allowing returning customers to login more securely to your services or systems.

It can enable you to move more services online, helping to reach new customers, and make accessing those online services more secure. It can also help streamline processes for background checks to make it easier and faster to onboard new employees.

Which businesses can use Digital ID?

You may choose to use digital ID as a **relying party** if you need to identify or confirm certain information about a person before allowing them to access your services or systems.

Common examples of businesses and organisations who can be relying parties include:

- real estate businesses providing services related to buying or renting properties
- telecommunication services
- businesses selling alcohol online and same day alcohol delivery services
- vehicle rental companies
- travel services, including hotels
- employment, recruitment and education providers.

Choosing a Digital ID service

Finding the right Digital ID service for your organisation is important. This short guide is intended to provide you with some information to make a more informed choice.

Accredited Digital ID providers

The Australian Government operates a voluntary accreditation scheme for Digital ID service providers. Accreditation recognises that the Digital ID service meets the privacy, security, fraud control and usability standards set by the Australian Government.

You can recognise accredited services by their use of the Digital ID Accreditation Trustmark which may be displayed on their Digital ID service such as in an app or on a webpage. You can see a list of accredited Digital ID providers in the accredited entities register.

Types of accredited providers

Identity service providers operate Digital ID services that generate, verify, manage and maintain Digital IDs. There are two kinds of identity service providers:

a) **A reusable Digital ID** enables a person to create a digital once and then reuse it again and again.

b) **A one-off Digital ID** provides a one-off verification of a person's ID.

Attribute service providers verify additional information about a person that may not necessarily be included in a Digital ID. This might include a person's:

1. qualifications like a university degree or trade certification
2. licences such as an electrician's licence
3. authorisations such as being able to act on behalf of a business or organisation
4. other verified personal information.

Digital ID exchange provider connect participants in a Digital ID system to each other. A Digital ID system may be made up of multiple identity service providers and attribute service providers who are connected via a Digital ID exchange to relying parties like your business or organisation.

Does my business need to be accredited to use Digital ID?

Relying party services are not required to be accredited or comply with the Digital ID Act. However, you may be subject to the privacy obligations under the Privacy Act 1988 if you collect personal information as part of providing your services to a customer.

Identity strength levels

Identity strength indicates the confidence you can have that the person is who they say they are. The strength is determined by the "identity proofing level" or IP level. The higher the IP level, the stronger their Digital ID is. Each strength builds on the last by verifying more ID and, at higher levels, ensuring a person's face matches the photo on their photo ID.

It's important to choose an identity strength requirement that is appropriate for the goods and services your business is providing. As a relying party, you should consider the:

- **Risk and impact** of incorrectly identifying a customer before providing your service to them.
- **Accessibility** of certain documents or information for customers who want to access your service.
- **Suitability** of Digital ID for your customers. It is important to remember that not all customers will be able to or want to obtain and use a digital ID.
- **Kinds of attributes you need** a customer to verify for them to access your service(s). For example, the customer's name and date of birth.

Attributes

Attributes are something about a person that is associated with them. For example, a person's:

- name
- address
- date of birth.

Some attributes are restricted from being disclosed to relying parties, except in certain circumstances.

Restricted attributes are attributes protected by additional privacy protections in the Digital ID Act 2024.

Getting attributes

Identity service providers can provide you with an individual's attributes that have been verified as part of the identity proofing process for generating a Digital ID. Common attributes that may be disclosed along with the strength level of a Digital ID are an individual's name and contact details, such as an email address or mobile number.

Attribute service providers can provide other verified attributes to you, such as business authorisations. There may be other kinds of accredited attribute service providers in the future to provide other verified attributes about an individual such as the kinds of licences (e.g. electrician, medical etc.) or qualifications (e.g. master's degree) they hold.

Connecting to an accredited Digital ID provider

There are different ways for your business to connect to accredited Digital ID providers and the best option will depend on what kind of Digital ID service your business or organisation needs. You should consider:

- the needs of your customers to access your service
- regulatory requirements you may need to comply with in your industry
- the kind of verified information you need from a customer to provide them with your service.

Connecting through an Digital ID exchange allows a wide variety of customers who may already have a Digital ID with various providers to use their existing Digital ID to access your services.

Directly connecting allows you to use a single provider for your identity needs. There are several Digital ID providers that have been accredited right now.

Authentication for reusable Digital ID

A reusable Digital ID is suitable for an organisation or business that requires or allows a customer to return to access a service.

This is referred to as authentication, where a customer uses their Digital ID to 'log in' or authenticate to your service. A successful authentication provides reasonable risk-based assurance that the customer accessing your service today is the same person as the customer who accessed your service previously. The robustness of this assurance is described via an **authentication level (AL).**

How will using Digital ID service cost?

Charging for accredited services operating outside of the Australian Government Digital ID System is not regulated by the government, meaning that each accredited Digital ID provider may set different prices for their services.

More information and support

Please see using a Digital ID for your business for more detailed information. This page also covers **data minimisation**, **fraud control** and **redress and user support**.

For more information on:

- Digital ID in Australia, visit: digitalidsystem.gov.au.
- Scams and identity crime, including how to report an incident, visit: https://www.digitalidsystem.gov.au/id-support