What is the Digital ID Act?

The *Digital ID Act 2024* (the Digital ID Act) is Commonwealth legislation that aims to provide individuals with secure, convenient, voluntary and inclusive ways to verify their identity for use in online transactions with government and businesses. The Digital ID Act sets out the principles, governance, and oversight mechanisms for the regulation of entities providing or relying on Digital ID services.

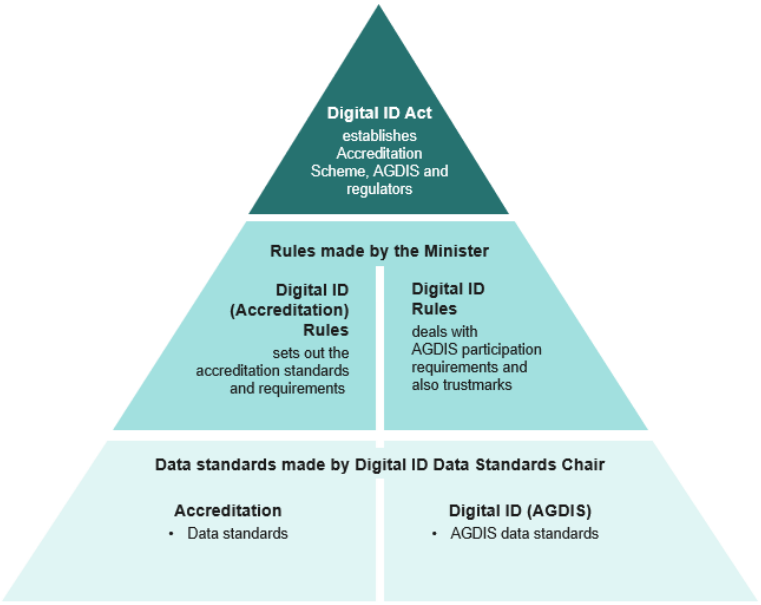
The commencement date of the Digital ID Act is 1 December 2024.

The Digital ID Act is supported by legislative instruments, which also commence on 1 December 2024 (collectively, the 'legislation'). The legislation:

- strengthens a pre-existing voluntary Digital ID Accreditation Scheme
- provides legislative authority for the Australian Government Digital ID System (AGDIS) to expand
- enshrines privacy and consumer protections in law; and
- strengthens governance for Digital ID.

What does the Digital ID legislation include?

The figure below depicts the various parts of the Digital ID legislation. The **Accreditation Rules, Accreditation Data Standards, Digital ID Rules and AGDIS Data Standards** (the rules and standards) are legislative instruments that support the operation of the Digital ID Act.



Strengthening a voluntary accreditation scheme

The Accreditation Scheme operates economy-wide and builds on the learnings from the Trusted Digital Identity Framework (TDIF) pilot accreditation program.

Accreditation requirements are set out in the Act – **Accreditation Rules** and **Accreditation Data Standards**. The **Accreditation Rules** prescribe requirements about identity verification levels, privacy, security, accessibility and useability. The **Accreditation Data Standards** set out the technical detail which an accredited entity must meet when implementing these requirements.

The Accreditation Rules

The **Accreditation Rules** apply to entities that choose to obtain accreditation.

The **Accreditation Rules** set out the accreditation application process, controls required for an accredited entity's effective management of fraud, protective security, privacy, and accessibility and usability, and annual review processes to assess compliance for these controls. The **Accreditation Rules** also set out requirements for the operation of digital ID services an entity may be accredited for.

There are 3 types of service an entity can be accredited to provide under the Digital ID Act. This table offers a simplified description of each kind of accredited service (more formal definitions are set out in section 9 of the Digital ID Act).

Service	What they do
Identity service provider (ISP)	Generates, manages, maintains or verifies information about the identity of an individual to create or manage a digital ID.
Attribute service provider (ASP)	Verifies and manages attributes, which are additional pieces of information that can be associated with a person's Digital ID.
Identity exchange provider (IXP)	Facilitates interactions and information flow between identity service providers, attribute service providers and *relying parties in a digital ID system (like a switchboard).

*A relying party means an entity that relies, or seeks to rely, on an attribute of an individual that is provided by an accredited entity to provide services or enable individuals to access services.

Privacy and consumer safeguards

While the scheme is voluntary, if an entity becomes accredited, they must adhere to additional privacy safeguards that go beyond those in the Privacy Act. Key safeguards include prohibitions on the use of single identifiers, a prohibition on disclosing information for marketing, and restrictions on the collection, use and disclosure of biometrics and other personal information. The Act provides the Information Commissioner with powers to make sure those safeguards are provided, and any breaches are penalised.

There are obligations and conditions on accredited entities regarding the use of Australia's Digital ID Accreditation Trustmark (the digital ID trustmark), which helps users see that the service they are using meets the strict rules and standards under the scheme.

Accredited entities must comply with accessibility and useability requirements which facilitate the equal opportunity and inclusion of individuals in digital society. Importantly, the creation and use of a digital ID by an individual is voluntary, and an entity cannot require an individual to create a digital ID in order to receive or access a service.

A key change from TDIF is the strengthening of enforcement mechanisms – civil penalties will apply to accredited service providers in some circumstances.

Digital ID Accreditation Data Standards

The **Accreditation Data Standards** support the **Accreditation Rules** by setting out various technical requirements associated with the legislated Accreditation Scheme. These include:

- Testing requirements for presentation attack detection technology, biometric matching algorithms, and electronic Identity Document Verification Technology (eIDVT).
- Authentication requirements, including the kinds of authenticators, authentication levels bound to a digital ID, and requirements for authenticating an individual to their digital ID using their biometric information.

The Data Standards Chair makes the **Accreditation Data Standards** as provided for under the Digital ID Act.

Australian Government Digital ID System

The Act enables the phased expansion of the Australian Government Digital ID System (AGDIS) beyond the Commonwealth. This will facilitate the use of Digital IDs between public and private sector organisations.

- The AGDIS is currently based around the Australian Government's Digital ID provider (myID), attribute provider (Relationship Authorisation Manager, or RAM) and identity exchange (operated by Services Australia). Some Commonwealth and state and territory agencies also participate in the AGDIS to verify their users.
- The phased expansion of the AGDIS will enable the reciprocal use of Digital ID and attribute providers in Commonwealth and state and territory services with private entities by December 2026. At this time, only public sector entities are eligible to participate in the AGDIS.
- Providers of Digital ID services operating within the AGDIS must be accredited and will be subject to additional regulatory requirements, some of which will also apply to participating relying parties.

Digital ID Rules

The **Digital ID Rules** set out requirements relating to entities seeking approval, or who have been approved, to participate in AGDIS. This includes:

- accredited digital ID service providers (as listed in the table above); and
- other entities (known as relying parties) who participate in AGDIS to use Digital IDs as a way for their clients or customers to verify their ID.

The **Digital ID Rules** operate alongside the **Accreditation Rules** and provide for additional privacy and security protections to individuals who use AGDIS.

The **Digital ID Rules** include specific details on:

- fit and proper person considerations relevant to AGDIS participation
- requirements for participating in the AGDIS
- record keeping obligations for certain entities
- arrangements relating to the notification and management of cyber security and digital ID fraud incidents in relation to AGDIS (including information sharing powers for the System Administrator)

AGDIS Data Standards

The **AGDIS Data Standards** sets out the technical integration and design requirements for entities to participate in the AGDIS.

Entities subject to these standards must treat the **AGDIS Data Standards** as requirements, in addition to their obligations outlined in the **Digital ID Act**, **Digital ID Rules** and the **Accreditation Rules** and **Accreditation Data Standards**.

Phasing-in of participation in the AGDIS

From 1 December 2024, Commonwealth, state and territory government entities can apply to the Digital ID Regulator to participate in the AGDIS. The AGDIS will be expanded to private sector entrants by no later than 2 years after commencement of the Digital ID Act. This will provide even more choice for individuals considering who

to use to create a Digital ID to access some government services.

A phased expansion of AGDIS allows Government to ensure the AGDIS continues to operate safely and securely as new categories of entities commence participation.

Establishing a robust regulatory scheme

The legislation establishes an independent regulator who will regulate entities who wish to:

- be accredited for the digital ID services they provide, or
- relying parties within the AGDIS who wish to rely on a digital ID to verify the ID of their customers.

The Australian Competition and Consumer Commission (ACCC) is the initial Digital ID regulator.

The ACCC is responsible for:

- accrediting digital ID services
- approving which entity can participate in the AGDIS
- using its investigative and compliance powers in the legislation to ensure digital ID providers and services comply with the legislation to keep people's information safe.

Separate to the independent Digital ID Regulator, the Office of the System Administrator oversees the day-to-day technical operation of the AGDIS.

The Information Commissioner has an expanded role as the regulator for privacy obligations under both the Privacy Act and the Digital ID Act.

A Digital ID Data Standards Chair is responsible for developing data standards.

Civil penalties and certain enforcement powers

The Digital ID Act provides for civil penalties and certain enforcement powers for the Regulator to help promote compliance of accredited providers. The Digital ID Act gives the Digital ID Regulator a calibrated set of powers ranging from the power to request information, giving remedial directions, issuing enforceable undertakings, before suspending or revoking an entity's accreditation or participation in the AGDIS.

The Digital ID Act clarifies that breaches of the Digital ID Act's privacy safeguards may be treated as an interference with privacy under the Privacy Act. This means the Information Commissioner can apply the powers and penalty provisions available to them under the Privacy Act to Digital IDs.

Want more information?

The legislation and accompanying explanatory statements can be downloaded from the Federal Register of Legislation.

You can access previous consultation papers on the legislation here.

Figure 1: Phased expansion of the AGDIS