



Your Guide to the Digital ID Legislation and Digital ID Rules

18 September 2023



Department of Finance



© Commonwealth of Australia (Department of Finance) 2023

With the exception of the Commonwealth Coat of Arms and where otherwise noted, this product is provided under a Creative Commons Attribution 4.0 International Licence.

(<http://creativecommons.org/licenses/by/4.0/legalcode>)

The Department of Finance has tried to make the information in this product as accurate as possible. However, it does not guarantee that the information is totally accurate or complete. Therefore, you should not solely rely on this information when making a commercial decision.

The Department of Finance is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, please contact the Communications team, Digital ID at digitalid@finance.gov.au.

Version: 1801^[08]

Contents

Minister’s foreword	4
Using this guide	5
Where to find more information	5
Having your say	6
Consultation to date.....	6
Providing feedback on the legislation.....	6
Key dates for consultation	6
The need for legislation	7
Strengthening voluntary Digital ID accreditation	7
Providing legislative authority for the Australian Government’s Digital ID System to expand	7
Strengthening privacy and consumer protections	8
Strengthening governance	8
Scope of the Bill.....	8
The legislative framework	9
Digital ID Bill	10
Structure of the Bill and the Digital ID Rules	10
Objects	11
Key definitions	12
The Accreditation Scheme	13
Accredited Services.....	13
Eligibility	14
Accreditation process	15
Accreditation conditions	15
Suspension or revocation of accreditation	16
Powers of the Regulator to ensure accredited entities comply with their accreditation obligations... 16	
Privacy safeguards	18
Interaction of the Bill with other privacy laws	18
Additional privacy safeguards	18
Consumer protections for the Accreditation Scheme	22
Trustmark	22
Children and Digital IDs.....	23
The Australian Government Digital ID System	24
Phased participation in AGDIS.....	24
Additional protections applying in the AGDIS	26
Creating and using a Digital ID is voluntary	26
Interoperability	27
Australians’ information used in the AGDIS will stay in Australia	27
Eligibility to participate in the AGDIS.....	29
Conditions of approval to participate in the AGDIS.....	29
Conditions of participation in the AGDIS.....	30
The Independent Digital ID Regulator	32
Powers of the Regulator to govern the Accreditation Scheme and the AGDIS	32
Fees and charging for provision of services	33
The Data Standards Chair	34

Minister's foreword



We're all used to providing documents to verify who we are. Showing our driver licence, passport or birth certificate multiple times to access services. This can be time consuming, especially when using online services. Australians should expect to have an efficient, reusable way to verify their ID that promotes innovation and productivity across the economy. Recent data breaches involving the ID documents of millions of people shows that there is more work to be done when it comes to protecting Australians and their identities.

The Australian Government's vision for Digital ID will help address these challenges. Digital ID gives you a voluntary, secure, convenient and inclusive way to verify who you are when interacting with government and businesses online.

Digital IDs are created by verifying who you are based on ID documents that you already have, not by giving you a new number or card. By setting up a strong and secure Digital ID, people can benefit from re-using it when they are asked to verify who they are. This avoids the need for you to repeatedly share your ID documents (and worry about where that information is stored).

As a part of the 2023-24 Budget the Australian Government committed to delivering policy and legislative foundations for a whole-of-economy Digital ID system with an independent regulator.

The Digital ID Bill (the Bill) will help us achieve this vision by strengthening a voluntary accreditation scheme for Digital ID providers in the public and private sectors. The Digital ID Bill makes it clear that Digital IDs are voluntary. Choice and consent lay at the heart of the Australian Government's approach to Digital ID. The legislation contains a range of privacy and other safeguards that embed these key principles. Australians who choose to create, use or reuse a Digital ID issued by an accredited service provider can have greater confidence their personal information is being protected.

Building on the foundation provided by the existing Trusted Digital Identity Framework, a legislated accreditation scheme will enable more Digital ID providers to demonstrate they meet strong privacy protections, security safeguards, and accessibility requirements. More people and more businesses will be able to use Digital IDs, spreading the benefits of the digital economy across the community.

The Digital ID Bill will also provide a legislative basis for expanding the existing Australian Government Digital ID System (AGDIS). The AGDIS is already well established within government. Millions of Australians use a Digital ID provided by the Australian Government (myGovID) to access over 130 services provided by federal, state and territory agencies participating in the AGDIS. The Digital ID Bill will enable the AGDIS to include Digital IDs provided by states and territories and, over time, private sector providers that choose and are approved to participate in the system.

By promoting the use of Digital IDs, this legislation will make it easier for Australians to more securely verify who they are to safely and easily interact with government and businesses online. Having a secure Digital ID means there are fewer copies of our most sensitive documents out in the world, such as our passports, birth certificates and driver licences.

The release of this exposure draft of the Digital ID Bill is an important part of the process to ensure the legislation is robust, fit-for-purpose, and meets public expectations. I encourage you all to review the materials and provide your feedback to help us ensure this important work is done right.

Senator The Hon Katy Gallagher
Minister for Finance, Minister for Women and Minister for the Australian Public Service

Using this guide

This guide provides an overview of the exposure draft Digital ID Bill (**the Bill**) and the Digital ID Rules (**the Digital ID Rules**), including high-level information about the voluntary Accreditation Scheme and how it will work with the Australian Government Digital ID System (**AGDIS**).

This guide lists the key dates for consultation so that you can have your say. See the following page for more information on consultation.

This guide is not intended to be an exhaustive description of the content of the exposure draft of the Bill and the Rules, as details have been necessarily simplified or omitted. We recommend you read it alongside the source documents themselves, which remain the authoritative description on the proposed laws.

Where to find more information

To help you understand more about the AGDIS we recommend reading the resources that can be found on the [Digital ID website](#): Australian Government Digital ID System

Having your say

Consultation to date

This Bill incorporates previous work and consultation to ensure that Digital IDs will be a voluntary, secure, convenient, and inclusive way for Australians to prove who they are, meeting the expectations of Australians and businesses.

This includes extensive consultation with the community and industry on the precursor to the proposed legislative Accreditation Scheme, the Trusted Digital Identity Framework (**TDIF**) accreditation scheme, consultation on a previous Bill in 2021, and ongoing engagement with various industry sectors and the state and territory governments in lead up to the release of this exposure draft of the Bill.

Providing feedback on the legislation

Your views on the Bill and the Digital ID Rules are important. This guide seeks views on key questions, which will help refine any legislation introduced to Parliament. If you wish to provide a submission, please read this guide and address the questions in each section.

The consultation period will close 5:00 pm AEST Tuesday 10 October 2023.

Details on how to provide your feedback are available below and on the [Digital ID website](#).

Key dates for consultation

Our consultation phases for all key documents relating to the Digital ID Bill are as follows:

Document	Dates for consultation
Digital ID Bill (or Bill) and Digital ID (Digital ID) rules	19 September – 10 October
Accreditation Rules (please see separate Guide)	19 September – 31 October

The need for legislation

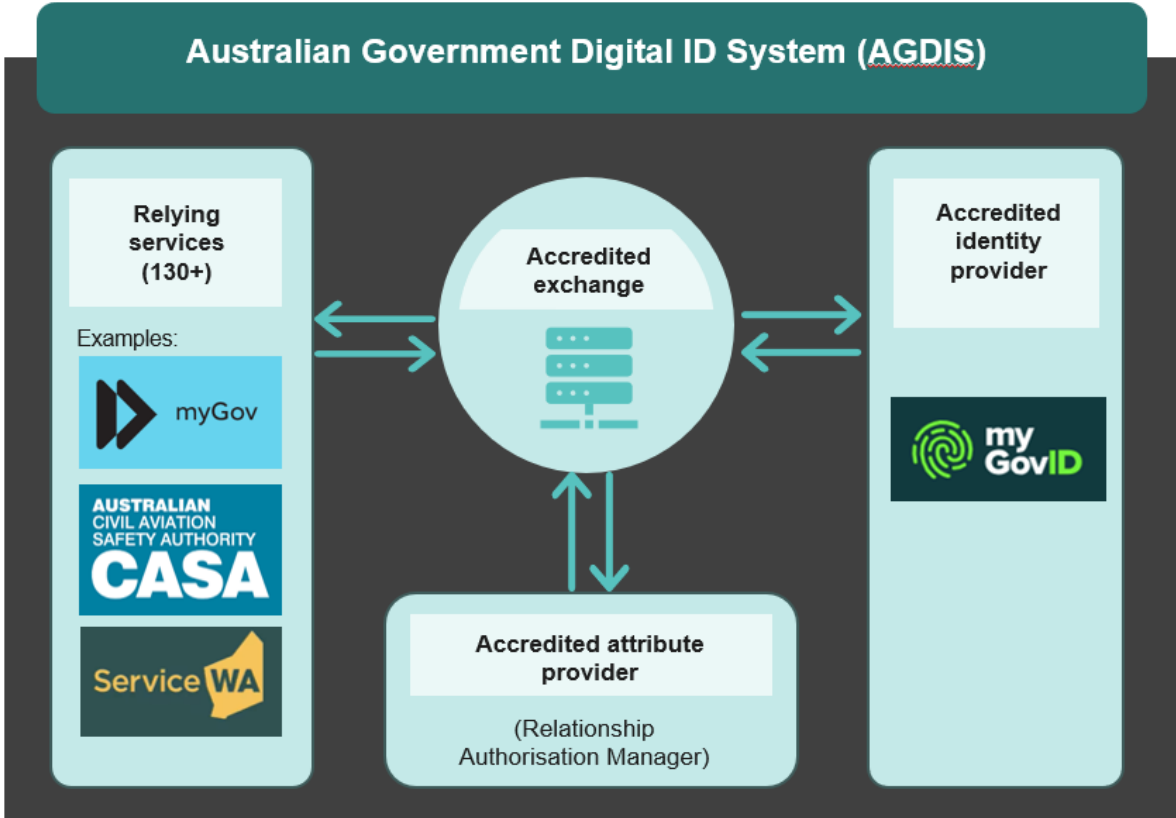
Strengthening voluntary Digital ID accreditation

The Bill and the Accreditation Rules (discussed in a separate Guide) legislate a voluntary Accreditation Scheme for providers of Digital ID services operating across the digital economy. The Accreditation Scheme is an evolution of the existing Trusted Digital Identity Framework (TDIF). Legislation is required to ensure the strength of the Accreditation Scheme meets the Australian community's expectations that Digital IDs will be private, safe and secure. For example, legislation allows civil penalties to be imposed, which was not possible in the TDIF. For Australians with accessibility requirements, the Accreditation Scheme requires providers of Digital ID services to meet standard accessibility and usability requirements.

Under the Accreditation Scheme, Digital ID service providers must comply with privacy, security and user experience obligations and safeguards. The Accreditation Scheme will ensure Australians who use accredited service providers to create and reuse a Digital ID can have confidence to transact using their Digital ID. The Accreditation Scheme offers an opportunity for Australian businesses and organisations to show they can meet high standards of privacy and protective security.

Providing legislative authority for the Australian Government's Digital ID System to expand

Right now, the Australian Government Digital ID System (AGDIS) already provides Australians with access to over 130 government services (See the diagram below). However, legislative authority is required for the Australian Government to expand and regulate the AGDIS.



The states and territories and the Commonwealth will work together so that Australians can access services in any jurisdiction, regardless of the Digital ID they use. More state and territory relying party services will be available through AGDIS as states and territories agree to participate. Private sector relying party services will also be able to participate in AGDIS if they choose to.

The Bill can facilitate accredited state and territory Digital IDs being used to access Commonwealth services.

Finally, the Bill provides the capacity in the future for Australians using their accredited private sector Digital IDs to access government services participating in AGDIS. This expansion will mean that more Australian businesses, community organisations, state and territory governments and individuals can benefit from safe and secure identity services.

Strengthening privacy and consumer protections

To trust their Digital ID and reuse it to access services, Australians need to know their personal information is securely protected by law.

The Bill enshrines new privacy and consumer safeguards, in addition to the protections which already exist under Australian privacy law. The Bill will require any accredited entity providing identity services to meet these protections. The Bill will also require participants in the AGDIS to meet specific protections that are relevant to the AGDIS, for example the requirement for information not to be held outside Australia. These AGDIS-specific protections are discussed further in Chapter 'The Australian Government Digital ID System', below.

The Bill harnesses Australia's existing privacy regulator, the Information Commissioner, to enforce the privacy aspects of the Accreditation Scheme and the AGDIS. This means Australians with Digital IDs will benefit from the experience, staff and expertise of the Office of the Australian Information Commissioner.

Strengthening governance

Good governance of the Accreditation Scheme and participation in the AGDIS is essential to maintain public trust and confidence. Currently, oversight of the accreditation scheme sits with the Commonwealth Department of Finance, and oversight of the AGDIS is shared between Services Australia and the Commonwealth Department of Finance. The Bill will establish an independent, Digital ID Regulator (**Regulator**) to perform this governance function.

Scope of the Bill

The Bill will not regulate Digital ID services or systems generally: entities will choose whether to seek accreditation. When accredited, an entity can operate in any Digital ID system as an accredited provider. Accredited entities and relying parties can then decide whether to participate in the government system (AGDIS), as each expansion phase is rolled out (see [Phased participation in AGDIS](#)). However, only accredited service providers can be approved to participate in the AGDIS. Relying parties are not subject to accreditation and can participate in the AGDIS if they apply to do so.

The legislative framework

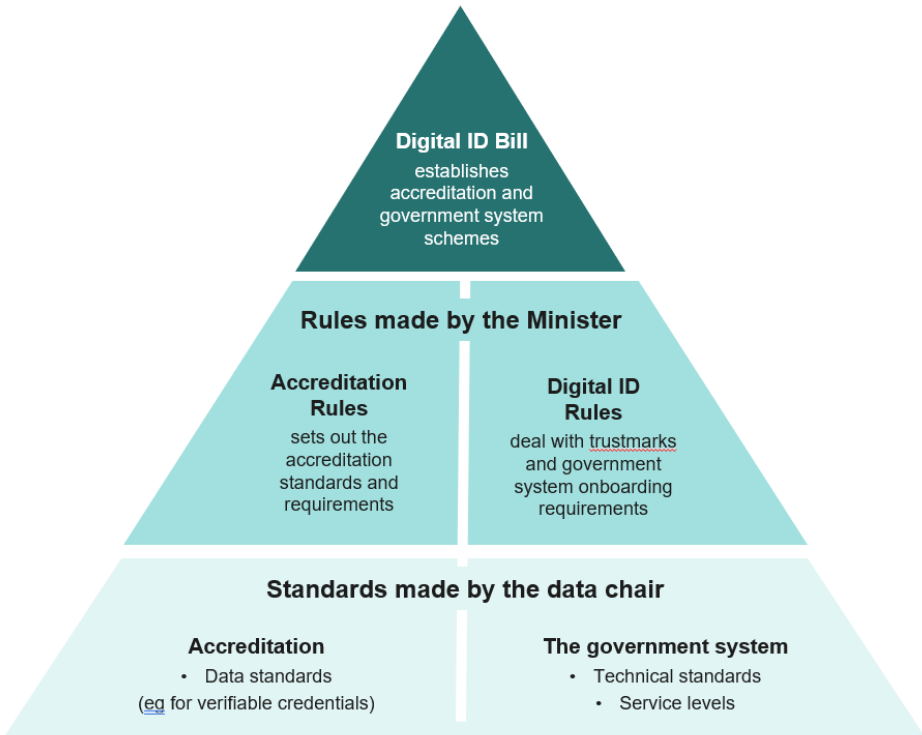
The Digital ID legislation is a package of multiple legislative instruments which govern the Accreditation Scheme and the Australian Government Digital ID System. The different components of the legislation are:

Digital ID Bill (the subject of this guide) – the primary legislation for the Accreditation Scheme, providing high-level rules for accredited Digital ID services or relying parties to participate in the Australian Government Digital ID System.

Accreditation Rules – made by the Minister, these Rules provide the requirements for entities obtaining and maintaining accreditation in the Accreditation Scheme. These rules are a legally binding instrument which must be tabled in, and can be ‘disallowed’ by, Parliament. A separate guide to the Accreditation Rules is available from the [Digital ID website](#).

Digital ID Rules (the subject of this guide) – made by the Minister, these Rules provide the requirements for entities participating in the Australian Government Digital ID System. The Rules also provide for any other general requirements, for example, Trustmark requirements and reporting. These rules are a legally binding, ‘disallowable’ instrument, which must be tabled in, and can be ‘disallowed’ by, Parliament.

Standards made by the Data Chair (to be developed in future) – relate to technical integration requirements or technical features for entities in relation to accreditation, or to onboard to the AGDIS. These are legally enforceable standards published by the Data Standards Chair.



A Digital ID (Transitional and Consequential Amendments) Bill will be developed to ensure entities who wish to transition their TDIF accreditation or participation in the Australian Government services can do so efficiently from the date of commencement of the Digital ID Bill. The Digital ID (Transitional and Consequential Amendments) Bill will also make any changes to other Commonwealth legislation necessary to enable Digital IDs.

Digital ID Bill

Structure of the Bill and the Digital ID Rules

The Bill consists of 9 chapters:

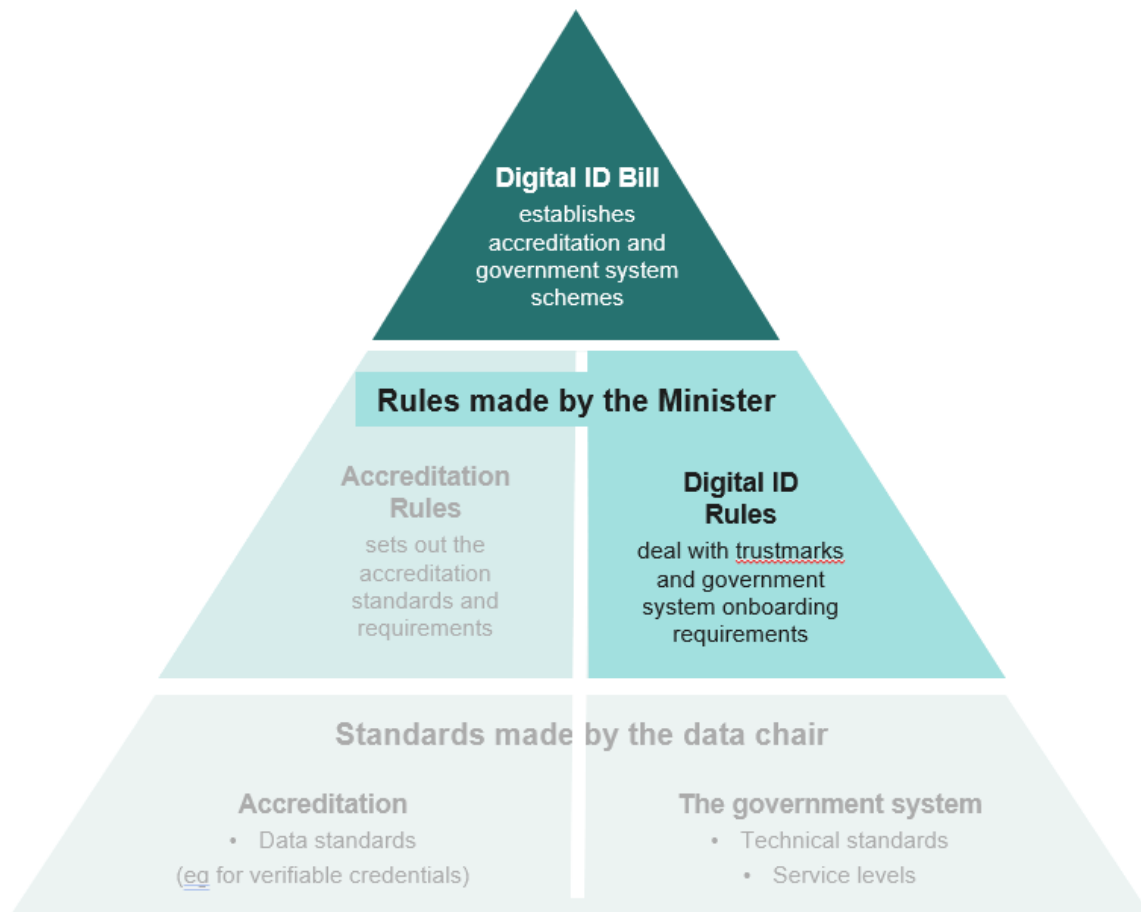
- **Chapter 1:** Introduction
- **Chapter 2:** Accreditation
- **Chapter 3:** Privacy
- **Chapter 4:** The Australian Government Digital ID System
- **Chapter 5:** Digital ID Regulator
- **Chapter 6:** Digital ID Data Standards
- **Chapter 7:** Trustmarks and registers
- **Chapter 8:** Administration
- **Chapter 9:** Other matters

The Digital ID Rules will be made by the Minister, after consultation (unless there is an imminent threat or hazard requiring rules to be made urgently).

The Digital ID Rules consist of 6 parts:

- **Part 1:** Preliminary
- **Part 2:** Fit and proper person
- **Part 3:** Participation in the Australian Government ID System
- **Part 4:** Reportable Incidents
- **Part 5:** Trustmarks
- **Part 6:** Record-keeping

In this summary, we do not explain concepts in the order they appear in the Bill or Rules. Instead, we have bundled concepts thematically to assist your understanding. This guide only covers the Digital ID Bill and the Digital ID Rules.



For a guide to the Accreditation Rules, please see [2023 Digital ID Accreditation Rules](#) webpage.

Objects

The objects of the Bill are to:

- provide a simple and convenient way for people to verify their identity in transactions with government and business
- protect privacy and the security of personal information
- promote economic activity by fostering innovation, productivity and reducing regulatory burdens

These objects will be achieved by

- establishing in legislation a voluntary accreditation scheme to promote trust in Digital ID services across the economy
- establishing in legislation an Australian Government Digital ID System (a network of organisations that provide and/or use Digital ID services in delivering participating government and commercial services)
- facilitating choice for individuals amongst providers of services within the Australian Government ID system

Key definitions

The Bill gives a particular meaning to certain words, which may not be the way that you interpret that word. You should note that words defined to have a particular meaning in the Bill will have the same meaning in the Accreditation Rules and the Digital ID Rules.

From this point in the guide, language used with a specific definition in the Bill is identified in *italic text*. However, it is important to note that we have only extracted a small number of the most important definitions. To properly understand the meaning of any italicised word not defined in this section, you will need to consult the Bill (specifically, Chapter 1, Part 2).

Below we have extracted and simplified some of the key definitions which are fundamental to the Bill or to helping you understand this guide. In addition, these are simplified descriptions that are designed only to aid understanding. They do not match the exact definitions in the Bill.

Attribute: an *attribute* of an individual is information that is associated with the individual and includes information that is derived from another *attribute*. The legislation provides a non-exhaustive list of *attributes* including first name, last name, date of birth, email address and mobile phone number. The list of attributes explicitly includes sensitive information about an individual as defined in the *Privacy Act 1988 (Cth)*, so the *Regulator* has powers to restrict and prohibit the collection of certain attributes and enforce that prohibition. For example:

Restricted attributes: information which is subject to additional protections in the Bill, including sensitive information as defined in the *Privacy Act 1988 (Cth)*. The legislation defines *restricted attributes* to include information such as tax file numbers (TFNs), Medicare numbers, health information, and membership of a professional or trade association. Additional *restricted attributes* may be prescribed in the Digital ID rules after consultation.

Prohibited attributes: information that accredited entities are not permitted to intentionally collect. This is sensitive information about a person, such as a person's racial or ethnic origins, or religious beliefs. Accredited entities may unintentionally collect that information – for example if a person's photo could disclose their religious belief because of their clothing.

Biometric information: a kind of information subject to significant additional protections in the Bill. *Biometric information* is information about any measurable biological characteristic of an individual that could be used to identify the individual or verify the individual's identity (for example, a photo).

Digital ID: a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online.

Participating: describes an entity which is connected to the *Australian Government Digital ID System*. The definition of *participating* prescribes specific circumstances when an entity will be considered connected to the *Australian Government Digital ID System*.

Verifiable credential: a digital form of traditional credentials like a driver licence or university qualification.



See further: [Bill Chapter 1, Part 2](#)

The Accreditation Scheme

The Accreditation Scheme is an evolution of the Trusted Digital Identity Framework (TDIF) policy document. The TDIF is an accreditation standard recognised as the Australian benchmark for Digital ID services. Digital ID services that currently can be accredited are identity provider, identity exchange and attribute provider.

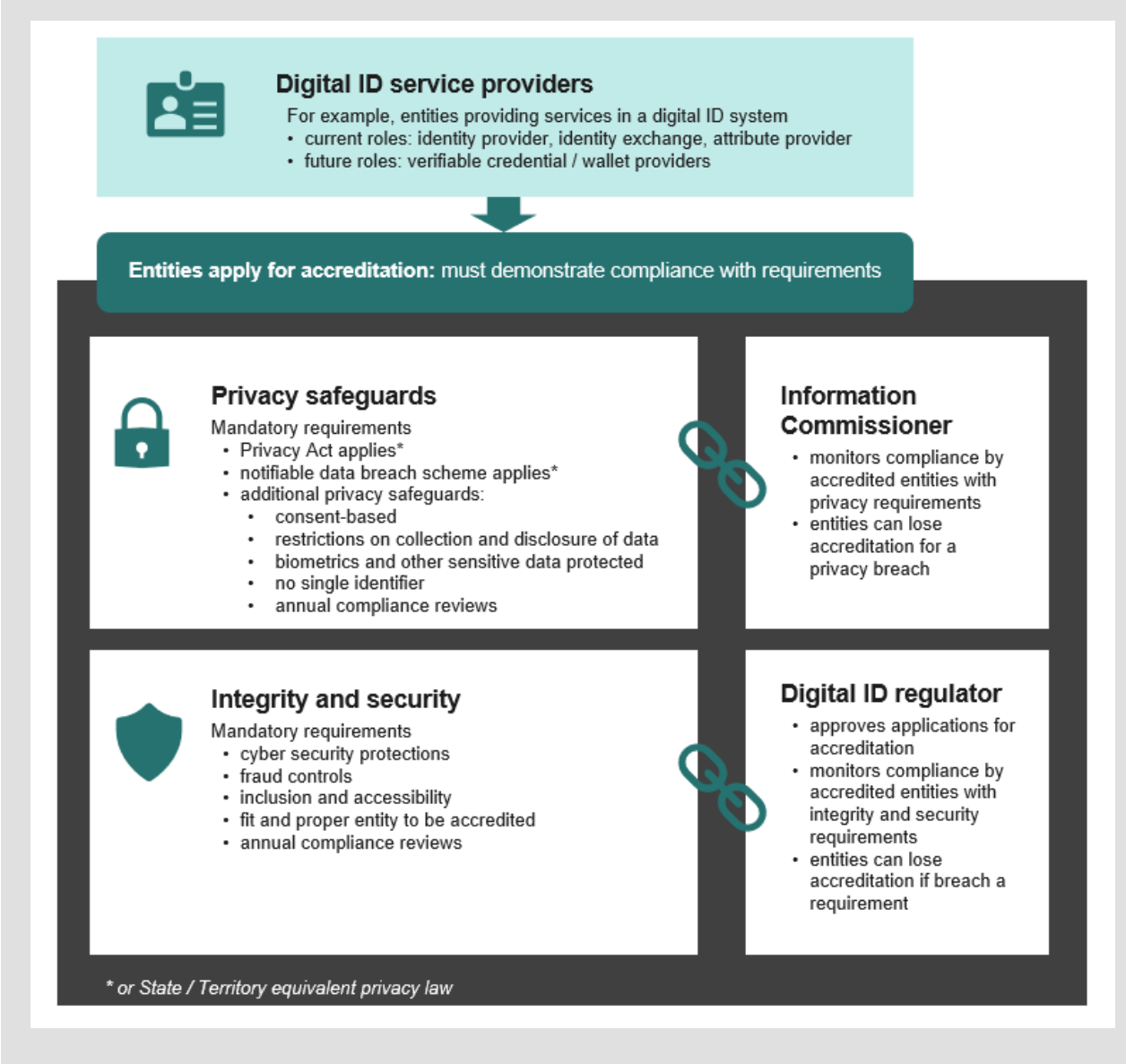


Figure 2. Accreditation Scheme under the Bill

Figure 2 provides a summary of the requirements for entities seeking accreditation and the roles of the Regulator and the Information Commissioner. Accreditation will be mandatory for entities providing Digital ID services (e.g., identity provider, exchange or attribute provider) in the AGDIS.

Accredited Services

There will be three types of service an entity can be accredited to provide when the Bill takes effect. This table offers a simplified description of each kind of accreditation (more formal definitions can be found in section 9 of the Bill):

Service	What they do
identity service provider	helps a user set up or manage a digital ID. For example, the myGovID is an identity service provider operated by the Australian Taxation Office (ATO). There are currently three other private sector TDIF-accredited identity service providers.
attribute service provider	verifies and manages <i>attributes</i> which are additional pieces of information that can be associated with a person's Digital ID. For example, the Relationship Authorisation Manager operated by the ATO provides business attributes, to enable people to access services on behalf of businesses.
identity exchange	facilitates interactions and information-flow between identity service providers, attribute service providers and relying parties in a <i>digital ID system</i> (like a switchboard). For example, Service Australia operates an identity exchange facilitating transactions between people using their myGovID to access government services. There are currently three other TDIF-accredited private sector identity exchanges.

Accreditation obligations will apply equally to entities approved to participate in the AGDIS or which participate in another Digital ID system (e.g. a Digital ID system operating within the private sector).

Accredited entities participating in the AGDIS will have some additional obligations relevant to the operation of the AGDIS.

The Accreditation Scheme is designed to be as technology neutral as possible with the Accreditation Rules able to be amended to respond to the evolving Digital ID and verifiable credential environment, including innovative service delivery models as they emerge. For example, state and territory bodies that issue digital driver licences may not fit the definition of an 'identity provider.'

The Minister will be empowered to create additional types of services to be added in the future to accommodate the evolving Digital ID landscape. Future services provided may deal, for example, with verifiable credentials such as digital driver licences and digital wallets.



Question: What other types of Digital ID service should be included in the legislation, either now or in future?



Question: Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?

Eligibility

Under the Bill, Australian Government, state and territory governments, Australian companies and foreign companies registered with the Australian Securities and Investments Commission (ASIC) can apply for accreditation. An entity that wants to be accredited and also approved to participate in the AGDIS can apply in one application, streamlining the assessment processes.

The Bill gives the Minister authority to make legislative rules setting out fees the *Regulator* may charge entities for accreditation applications.

An entity that is currently TDIF-accredited and compliant can choose to transition to the Accreditation Scheme. This can be done when legislation is in force by re-applying to be accredited, or be actioned through a Transitional and Consequential Bill.

Accreditation process

Applications for accreditation are assessed by the *Regulator*.

The Bill outlines matters the *Regulator* must consider in deciding to accredit or refuse to accredit an entity, including that the entity can comply with obligations set out in the Act and the Accreditation Rules. Additional privacy safeguards specific to management of Digital IDs by accredited entities are included in the Bill (see 'Privacy Safeguards' below for further information).

The *Regulator* may consider whether the entity is a fit and proper person, or other relevant matters. The *Regulator* may require the entity to undergo a compliance assessment to demonstrate it is capable of complying with the obligations in the Bill and Rules relevant to the role (or service) for which it is seeking accreditation.

The Minister may direct the *Regulator* not to accredit or to suspend accreditation of an entity on national security grounds and the *Regulator* will rely on national security assessments made by national security agencies. For example, on the basis of an adverse or qualified security assessment provided in accordance with the *Australian Security Intelligence Organisation Act 1979*.

An entity may apply to be accredited for one service, or for any number or combinations of services.

Accreditation conditions

Accredited entities must comply with accreditation conditions specified in the Act, the Accreditation Rules and in any special conditions imposed by the *Regulator*.

The *Regulator* may place special conditions on an entity's accreditation. It may be necessary for the *Regulator* to impose special conditions due to the different circumstances and services provided by different kinds of accredited entities and their different service delivery models. Special conditions may deal with the particular services the entity is accredited to provide (see the types of services in the definition for each accredited role).

For example, an identity provider may wish to offer its customers the choice of two strength levels of Digital ID ('strong' and 'very strong'). The identity provider wants to use biometric verification for its 'very strong' Digital ID. For its 'very strong' Digital ID service, the *Regulator* may impose a special condition about the types of biometrics the identity provider is accredited to use (e.g. face images only, or fingerprints only, or both). That special condition would not apply to the identity provider's 'strong' service.

For identity providers, special conditions may authorise them to collect biometric information and 'restricted attributes' (i.e. particularly sensitive information such as passport numbers and health information). Without that authorisation, collection of those attributes is prohibited.

Before imposing an accreditation condition authorising collection or disclosure of a restricted attribute, the *Regulator* must consider certain criteria, including a risk assessment and privacy impact assessment, and, for transparency, must publish its reasons for the approval on its website.

Such conditions can be imposed on the entity's accreditation at the accreditation stage or afterwards and modified at any time, including when requested by the accredited entity. The *Regulator* will give notice before varying a condition on accreditation.



Question: Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?



Question: Is the application for accreditation process appropriate, or should other matters be included or some excluded?



See further: Bill Chapter 2, Part 2, Division 2

Suspension or revocation of accreditation

An entity's accreditation for a service may be suspended or revoked by the *Regulator* in certain circumstances, including:

- if the entity has breached its obligations under the Bill or Accreditation rules
- if the entity has been (or will be) involved in a *cyber security incident*
- for insolvency reasons.



See further: Bill Chapter 2, Part 2, Division 3

Powers of the Regulator to ensure accredited entities comply with their accreditation obligations

Once they achieve accreditation, an *accredited entity* must fulfil a range of obligations in the Bill and Accreditation Rules, including:


- the additional privacy safeguards in the Bill (see [Additional Safeguards](#))
- consumer safeguards relating to the deactivation of Digital IDs and accessibility of services (see [Additional Safeguards](#))
- requirements relating to coverage by the Privacy Act (see [Privacy Act requirement](#))
- requirements relating to data breach reporting (see [Data Breach](#))
- Accreditation rules (see [Accreditation](#))
- requirements relating to the use of trustmarks (see [Trustmarks](#))

The Digital ID *Regulator* will have power to issue an accredited entity with directions to do, or refrain from doing, something. For example, a direction may:

- require an entity whose accreditation is to be suspended or revoked to notify other participants in the AGDIS of this so they can take appropriate action
- direct a suspended entity to take specified remedial action before the suspension will be lifted.

The *Regulator* will also have the power to compel an accredited entity to produce documents or information to enable the *Regulator* to assess whether an accredited entity is complying, or has complied, with its obligations under the Act.


Accredited entities, suspended and former accredited entities must also comply with obligations involving record-keeping, destruction of records containing personal information and trustmark requirements.



See further: Bill Chapter 8, Part 2, Division 2

Failure to comply with one of these obligations can lead to compliance action or civil penalties as set out in the following table.

Conduct	Penalty units	Maximum penalty (as at September 2023)	Regulated by
Failure to comply with a direction without reasonable excuse	200 units	For individuals: \$62,600 For corporate or government entities: \$313,000	Digital ID <i>Regulator</i>
Failure to provide documents/ Information without reasonable excuse	200 units	For corporate or government entities: \$313,000	Digital ID <i>Regulator</i>
Non-compliance with trustmark requirements	200 units	For corporate or government entities: \$313,000	Digital ID <i>Regulator</i>



Question: Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?

Privacy safeguards

The Bill will establish Digital ID-specific privacy obligations for accredited entities and clarify how the Bill's protections will interact with privacy laws. The Bill includes privacy safeguards that are in addition to the protections already provided by Commonwealth and state and territory privacy laws.

Interaction of the Bill with other privacy laws

Australians' privacy is already protected by Commonwealth and state and territory laws. The Bill provides specific protections tailored to the Digital ID context. These protections build on, but do not duplicate, existing regulatory frameworks.

To provide accredited services, entities must be subject to the Commonwealth Privacy Act. For state or territory entities, providers of accredited services must be subject to an equivalent state or territory privacy law.

Accredited entities will also be subject to the notifiable data breach scheme in the Privacy Act or an equivalent state/territory data breach scheme. The *Regulator* will receive the data breach notification at the same time, so the *Regulator* can mitigate or remediate the breach.

To the extent an entity is not covered by a notifiable data breach scheme, the Bill's provisions extend the Privacy Act's scheme to that entity.

The Bill extends the definition of 'personal information' from the term used in the Privacy Act to ensure the definition in the Bill includes any attributes used by an accredited provider that are not covered by the Privacy Act definition.



See further: Bill Chapter 3, Part 1 and Part 2, Division 1

Additional privacy safeguards

The Bill introduces ten new privacy-related protections (additional to those already provided by the Commonwealth Privacy Act) to be regulated by the Information Commissioner. These protections apply to all *accredited entities*, regardless of whether they participate in the AGDIS.

The table below sets out these protections, and groups some of these together. It contains a simplified explanation of the requirements in the Bill. For further detail on the precise scope and operation of the protections, see Chapter 4, Part 2, Division 2.

Protection	What the Bill requires
It is prohibited to collect certain attributes	<p>Accredited entities are prohibited from intentionally collecting some attributes entirely. For example, a person's racial or ethnic origin, political opinions, religious beliefs or sexual orientation (amongst others).</p> <p>It is possible that an accredited entity may unintentionally collect this information – for example a person's facial image collected by an accredited entity to verify against a document may show religious clothing indicating a religious belief. That unintentional collection is not prohibited.</p>

Protection	What the Bill requires
Requirement for express consent	When verifying or authenticating an individual's identity, an accredited entity must not send the user's attributes to a relying party without the user's express consent (e.g. the user may be required to check a tick box).
Disclosure of restricted attributes	<p>When verifying or authenticating an individual's identity, an accredited entity must not send a restricted attribute (e.g. passport or licence number) of an individual to a relying party unless:</p> <ul style="list-style-type: none"> • authorised to do so by an accreditation condition; and • only with the individual's express consent. <p>For example, this means that an accredited identity provider cannot disclose a passport or driver licence number to any relying party unless it is a condition of their accreditation, and the individual has consented to the disclosure.</p>
Restricting the disclosure of unique identifiers	<p>An accredited entity may assign a unique identifier to an individual within a digital ID system for technical reasons to provide their customers with a service or feature. For example, the unique identifier could be used to bind attributes (or in the future, credentials) to a Digital ID.</p> <p>To ensure this unique number can't be used to track a person's online behaviour or the services they access, restrictions apply to the disclosure of a person's unique identifier. Exceptions apply to the restriction on disclosing the unique identifier if the disclosure is necessary to detect fraud, or where the disclosure facilitates the person to access a service using their Digital ID.</p>
Prohibition on one-to-many matching using biometric information	The Bill will prohibit a person's biometric information from being used by an accredited entity to compare against biometric information to identify the individual.
Restrictions on biometric information	<p>The Bill places a range of safeguards on the use of biometric information by accredited entities, including:</p> <ul style="list-style-type: none"> • Biometrics can be collected and used for verification or authentication purposes, can only be retained for those purposes and must be deleted after that use ceases. • In relation to authentication, biometrics can be retained where the individual has consented to this so the biometric can be used to authenticate the individual in the future: e.g. to log back into a Digital ID account using a face biometric match with the individual's consent. The rules may require that biometrics are stored in an encrypted manner or on the individual's local device to prevent access to the original image while maintaining the authentication functionality. • Only limited secondary uses of biometrics are permitted including: <ul style="list-style-type: none"> • for fraud investigation and testing. However, a biometric retained for fraud and testing activities must be deleted within 14 days (subject to the authentication purposes mentioned above)

Protection	What the Bill requires
	<ul style="list-style-type: none"> • disclosure to the individual involved • disclosure to law enforcement with a warrant issued by a magistrate, judge or tribunal • disclosure to law enforcement with consent for an investigation/prosecution or identity verification. <p>Biometrics collected by identity providers may be disclosed to a government body that wishes to use it to create an identity document/credential when an individual consents to that use (e.g. a licence or passport). This is to enable a seamless service to individuals (noting these document-issuer agencies, whether accredited or not, already hold the biometrics in their systems).</p>
<p>Rules to govern emerging issues involving biometric information</p>	<p>The restrictions on the disclosure of biometric information (which prevents disclosure to a relying party) may affect individuals being able to use verifiable credentials if they become a part of the Accreditation Scheme in the future.</p> <p>A credential is a document, record, electronic representation or object which asserts a claim about an entity, individual, object or thing. Verifiable credential provides a trustworthy way of digitally proving something about an individual that can be presented to a third party for validation through the use of robust cryptographic methods. A verifiable credential needs to be linked to the particular person it represents. For example, if a plumber is holding a copy of their driver licence in a digital wallet, it needs to be verified that the licence is linked to the correct person. This can be done by the app retaining and disclosing a facial image of the person.</p> <p>The Bill will allow for the Minister to make rules, disallowable by Parliament, to allow disclosure of biometric information where the disclosure is to allow an individual in control of their own verifiable credential to expressly consent to share that credential. The Minister must consult with the Information Commissioner before making any rules about biometrics.</p> <p>The technology around verifiable credentials is new, rapidly advancing and requires the ability to make prompt changes to ensure the legislation keeps up with future advancements. An important safeguard for any future rule is that it cannot undermine the protection in the Bill that requires the individual to give their consent to use or disclose the biometric or verifiable credential.</p>
<p>Prohibition on data profiling</p>	<p>Accredited entities must not use or disclose information about an individual's online activities (i.e. the individual's access and use of the Digital ID services provided by the entity) except in permitted circumstances. Those circumstances would include using the information to provide services, or for the entity to demonstrate its compliance with obligations in the Act (when the Bill is enacted) or the Rules.</p>
<p>Restrictions on disclosure of information for law enforcement purposes</p>	<p>The Privacy Act generally permits disclosure of personal information to an enforcement body if is necessary for an 'enforcement related activity'.</p> <p>The Bill narrows the scope of such use or disclosure by not allowing personal information held by an accredited entity to be disclosed to law-enforcement agencies unless they are otherwise authorised to collect that information and:</p>

Protection	What the Bill requires
	<ul style="list-style-type: none"> • there is a warrant; or • the enforcement body reasonably believes that a person has committed an offence or has breached a law; or • the enforcement body has started proceedings against a person for such an offence or breach.
Prohibition on certain marketing purposes	Accredited entities must not use or disclose an individual's personal information for marketing purposes that are unrelated to the Digital ID services the entity provides to the individual. Consent from the individual will not override this prohibition.
Identity exchanges must not retain attributes	An accredited identity exchange must not retain an individual's name, address, date of birth, phone number, email or restricted attributes after the end of an authenticated session. This ensures an exchange cannot become a repository of information about an individual.



Question: Are the additional privacy safeguards sufficiently robust, clear and practical?



Question: Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?



See further: Bill Chapter 3, Part 2, Division 2

The additional privacy safeguards will be regulated and enforced by the Information Commissioner. The following table details the civil penalties proposed in the Bill in relation to the additional privacy safeguards.

Conduct	Penalty units	Maximum penalty (as at September 2023)	Regulated by
Breach of an additional privacy safeguard	300 units	Maximum of \$469,500 for corporate or government entities	Information Commissioner



Question: Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?

Consumer protections for the Accreditation Scheme

The legislation creates two additional safeguards to be regulated by the *Regulator* which apply to all *accredited entities*. The table below sets out these protections; however, please note that these are heavily simplified explanations of the requirements in the Bill. For further detail on the precise scope and operation of the protections, see Chapter 4, Part 2, Division 2.

Protection	What the Bill requires
Digital ID de-activation	An accredited entity must, if requested by an individual, deactivate the individual's Digital ID as soon as practicable after receiving the request. The information may be retained for a period for fraud investigation.
Accessible and inclusive services	The Accreditation Rules must specify standards that accredited entities must meet about: <ul style="list-style-type: none">• compliance with accessibility standards• useability testing• device or browser access.
Measures against fraud and identity theft	An accredited entity must comply with the Accreditation Rules. The Accreditation Rules impose requirements on accredited entities to block compromised Digital IDs from being transacted with.



See further: **Bill Chapter 2, Part 2, Division 5**

Trustmark

The Digital ID Rules establish a trustmark, which are symbols showing the service provider you're choosing to use for your Digital ID meets the Accreditation Scheme's standards. The accredited entity can use the trustmark to distinguish itself as a provider of safe and secure Digital ID service. The Rules require accredited Digital ID providers to display the trustmark on each of its website pages that a person accesses to create or use their Digital ID.

The Regulator will oversee the use of the trustmarks. For example, the Regulator can impose a civil penalty if an entity uses a trustmark in a way that would be likely to lead a reasonable person to believe they are accredited for a service, or participating in the AGDIS when they are not. In this way, the Bill envisages that Australians will become familiar with trustmarks of accredited providers and the services that rely on a person's Digital ID to allow them access to a service.



See further: **Bill Chapter 7, Part 2 and Digital ID Rules Part 5**

Children and Digital IDs

Increasingly, children are ‘digital natives,’ able to use technology effectively to empower engagement in the Australian community. The Bill aims to strike a balance between protecting children who may be unable to provide informed consent when creating and using a Digital ID and empowering them to access the services they need independently from an adult.

The Bill will give the Minister flexibility to make rules specifying an age for children to create a Digital ID. The rule making power will allow for flexibility to respond to changes across other schemes and systems dealing with age. Currently the Accreditation Rules will prohibit an identity service provider from creating a Digital ID for a child under 15. However, subject to compliance with the *Age Discrimination Act 2004 (Cth)* it is proposed to change the age to 14 in the Accreditation Rules.

Guidance on the Privacy Act is that at 15 years old a child can generally be expected to provide informed consent. However, an age of 14 is proposed based on feedback that children aged between 14 and 15 will be disadvantaged if they cannot access online services related to employment and training, such as applying for a Tax File Number or universal student identifier to access training opportunities. Restricting the age at 14 would be consistent with other age limits, such as when a young person can independently apply for a Tax File Number between the ages of 13 and 15. The age limit will consider any changes made as part of the review of the *Privacy Act 1988 (Cth)* to strengthen privacy protections for children.



Question: What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?



See further: Bill Chapter 2, Part 2, Division 4

The Australian Government Digital ID System

The AGDIS consists of a network of Commonwealth entities that together provide individuals with a simple, secure and convenient way to verify their identity in online transactions with government while protecting their privacy. The Bill will establish the foundations for broader use of Digital IDs, by expanding the AGDIS to include state, territory and private sector entities who choose to participate. This expansion will occur in phases, as discussed below.

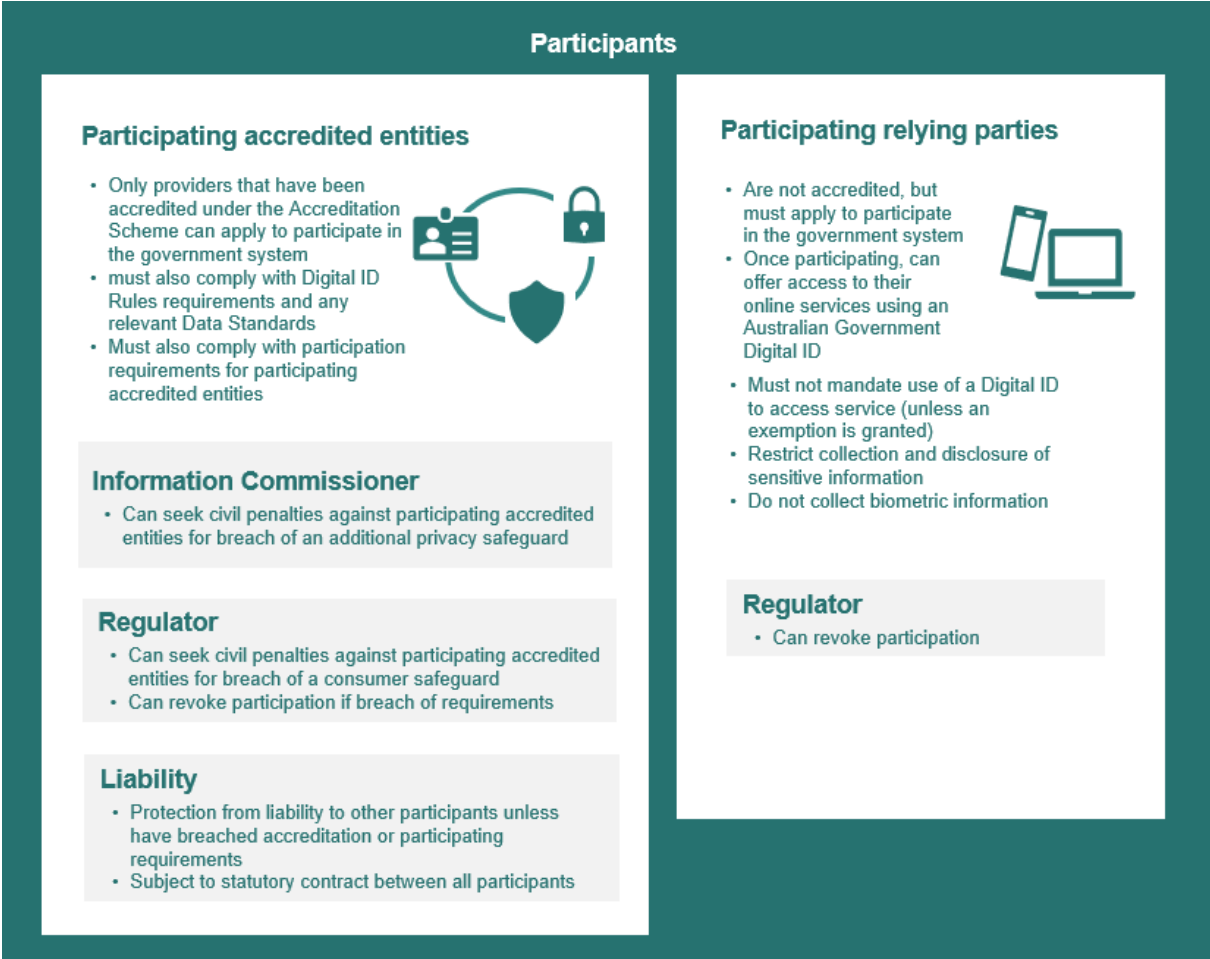


Figure 3. Overview of the government system participants

Phased participation in AGDIS

Expansion of the AGDIS is planned to occur in four phases. The Bill will enable this phasing by authorising the Minister to determine who can apply to the *Regulator* to participate in the AGDIS. Once the Minister has made a determination that an entity or class of entities can apply to participate in the AGDIS, that determination cannot be revoked. This is necessary to give certainty to entities expending resources in preparing to apply to participate in AGDIS.

The approach of expanding in phases will allow for the AGDIS to be matured within government, develop the Digital ID market, and increase community awareness of Digital ID before opening AGDIS participation economy-wide.

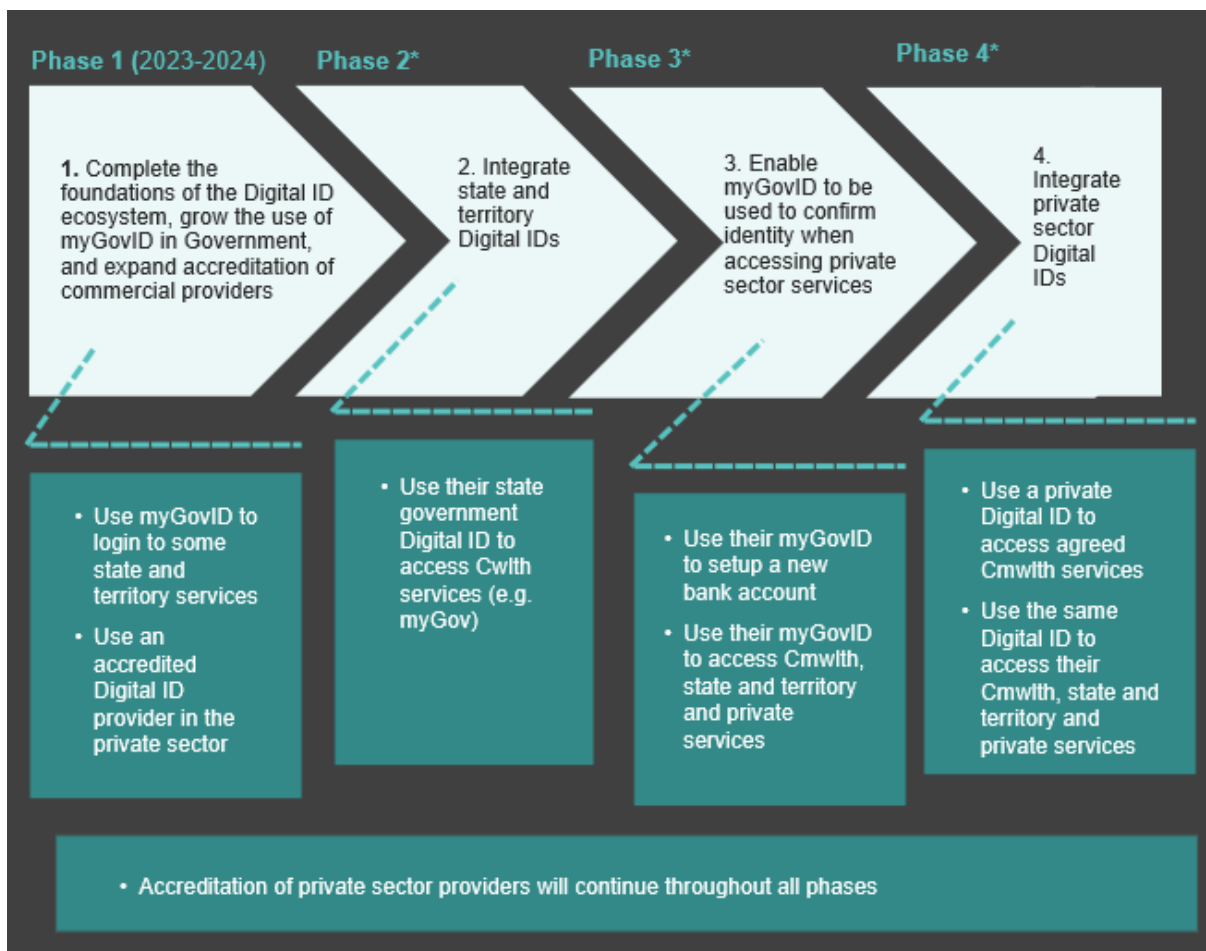


Figure: Expansion of AGDIS phases illustrates the phased approach. A phased approach allows the Australian Government to consider a range of factors before committing to further expansion. Considerations may include Digital ID market maturity, penetration of the Accreditation Scheme, and the capacity of the relevant agencies (e.g. Services Australia as the accredited identity exchange). The phased approach will also provide the Government with time to consider when to enable further expansion of Digital ID to accommodate emerging technologies like verifiable credentials and digital wallets.



Question: What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?



Question: What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?

Phase 1 will focus on the Commonwealth adding more services to the AGDIS, including state and territory services. Phase 2 will allow access to Commonwealth services using a Digital ID issued by jurisdictions' accredited identity providers. Phase 3 will enable customers to use their Digital ID issued either by Commonwealth or state and territory identity providers to access private sector services. Phase 4 will allow customers access to some government services using Digital IDs issued by accredited private sector Digital ID providers.

Accreditation of commercial providers for Accredited Services in the Accreditation Scheme will continue throughout each phase, so that they may continue to provide strong and secure Digital IDs for Australians to use within the private sector, and eventually for some government services.



Question: How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?

Additional protections applying in the AGDIS

The AGDIS is currently the primary system providing the Australian community with online access to Commonwealth services. Accordingly, the AGDIS establishes additional protections to meet the expectations of the Australian community about their taxpayer-funded services.

Creating and using a Digital ID is voluntary

Unlike a typical market for services, Australians do not have a choice to go to another provider if they want to obtain government assistance. For example, if an Australian wants to access a benefit or subsidy under government legislation for childcare, Centrelink is the only Commonwealth provider of that service. For Australians who are unwilling or unable to access taxpayer funded services online, the Bill will ensure that using a Digital ID to access government services through the AGDIS is voluntary.

This requirement for voluntary use of Digital ID is achieved by the Bill preventing a relying party participating in the AGDIS from requiring an individual, acting in a personal capacity, to use a Digital ID to verify their ID to accessing their service. The relying party must provide an alternative way for the person to verify their ID and obtain the service i.e. paper-based, by phone, at a shopfront or online.

In limited, specific circumstances, it may be appropriate to require a person to use a Digital ID to access a government service participating in the AGDIS. The Bill sets provides for exceptions to the voluntary requirement, when:

- the relying party is acting as an intermediary, and the service a person ultimately accesses is available without using a Digital ID through the AGDIS
- another law requires the individual to use of a Digital ID to verify their ID to access the relying party service; or
- a person is using the participating relying party service to act on behalf of a business (for example, as a tax agent or accountant).
- the *Regulator* provides an exemption to the requirement for access to be voluntary. Only non-Commonwealth entities can apply to the Regulator for an exemption.

A relying party must apply for an exemption and the *Regulator* must be satisfied that it is appropriate for a service to be non-voluntary. For example, if the service is a small business, or only provides its services online, or is providing services in exceptional circumstances (a natural disaster, for example). The exemption from the requirement for access to be voluntary is appropriate in those contexts as the services are either not taxpayer funded, or the cost of providing alternative ways to access the service would hinder economic participation, or the benefit of providing the services in a time of crisis is appropriate.



Question: Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?

Interoperability

The Australian community expects access to government services to be convenient. This means that the services available through the AGDIS should work efficiently together. The Bill and Rules require participating accredited entities and participating relying parties not to refuse to provide services to other participating accredited entities or participating relying parties. This ensures Australians can choose any participating accredited Digital ID provider and their Digital ID from that provider to access services. It also prevents a relying party controlling which Digital ID a person can use to access its service.

In limited circumstances, an entity can apply to the Minister for an exemption to the interoperability obligation. The Minister can grant an exemptions, including;

- if it was necessary to limit access to some government services to a government-issued Digital ID, rather than a Digital ID issued by a participating (and accredited) private sector Digital ID provider
- if the exemption was only needed short term to overcome technical barriers before implementation
- if the relying party service would promote the use of Digital IDs in the AGDIS
- if the entity will assist people who would otherwise be disadvantaged when accessing the AGDIS
- if other legislation requires an exemption to be made
- If the governance arrangements of an accredited entity prohibit or restrict the entity from interacting with another service.

The Minister cannot grant an interoperability exemption for the identity exchange providing exchange services to the AGDIS.



See further: Bill Chapter 4, Part 2, Division 4 and Digital Identity Rules Part 3



Question: Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?

Australians' information used in the AGDIS will stay in Australia

The Australian community expects their Digital ID information used to access government services, will be stored, handled and transferred securely. The Bill provides for the Digital ID Rules to restrict or prohibit participating accredited entities from holding, storing, handling or transferring information from the AGDIS outside Australia. These data localisation requirements in the Rules will be updated in line with change of government policy on data sovereignty, and to respond promptly to any risk situations that may arise.

The Digital ID Rules will be enforced by the Digital ID *Regulator*. Breach of this requirement will attract a pecuniary penalty of 300 penalty units, which is \$469,500 for corporate or government entities.

The Rules allow accredited entities to transfer information used in AGDIS overseas when an Australian wants to use their Digital ID from outside Australia to access services, to facilitate that transaction occurring.

The data localisation rules do not apply to accredited-only entities who are not participating in AGDIS or to relying parties providing services in the AGDIS, as they may choose not to implement it due to cost constraints.



See further: Bill Chapter 4, Part 2, Division 4 and Digital Identity Rules Part 3

Protections for participants in AGDIS

<p>Statutory contract</p>	<p>The Bill leverages the statutory contract model to provide certainty to its participants, used in the Consumer Data Right (CDR) legislation. Under this model, each accredited entity within the AGDIS is taken to have a separate contract with:</p> <ul style="list-style-type: none"> • every other accredited entity; and • each participating relying party. <p>The term of the contract is that each accredited entity agrees to comply with the obligations under the Act, the rules, technical standards and service levels.</p> <p>A party to the contract alleging a breach by another party may apply to the Federal Court for remedies, including:</p> <ul style="list-style-type: none"> • compensation; • an order to comply with the contract; and • any other order the court considers appropriate.
<p>Liability</p>	<p>The Bill provides that accredited entities within the AGDIS will have no civil liability to other onboarded entities or criminal liability in relation to the services they provide in the government system provided they have:</p> <ul style="list-style-type: none"> • complied with their obligations under the Act; and • acted in good faith. <p>The Bill allows the Minister to make rules further limiting liability, for example, to exclude types of losses or to cap losses (such as for minor breaches).</p>
<p>Redress</p>	<p>The Bill will not initially provide specific financial or non-financial redress obligations on accredited entities participating in the AGDIS, or on the <i>Regulator</i>. The Bill will allow the Minister to provide a redress framework in the Digital ID rules.</p>



Question: Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?



Question: Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?

Eligibility to participate in the AGDIS

Accredited entities (currently identity providers, attribute providers and exchanges) will be able to participate in AGDIS to provide the service they are accredited for, subject to the phasing of the expansion of AGDIS (see **Phased participation in AGDIS**). Accredited entities must continue to be accredited for the service they provide while participating in the government system.

The *Regulator's* decision on whether an accredited entity should participate in the AGDIS is separate to the accreditation decision. In making its decision the *Regulator* will consider whether the accredited entity can meet the obligations that are specific to participating in the AGDIS.

Relying parties may rely on a Digital ID to verify a customer's identity when providing them with a service or access to a service. Centrelink is an example of a relying party that relies on a Digital ID to verify the identity of a person before providing a service to that person.

If a service wishes to rely on the Digital ID issued by the Commonwealth's Digital ID provider, myGovID, to verify their customer, an entity can apply to the *Regulator* to participate, subject to the phasing of the expansion of AGDIS (see **Phased participation in AGDIS**). Relying parties are not subject to the Accreditation Scheme as they receive, and do not provide a Digital ID service – they rely on the services of accredited Digital ID service providers.

Eligible relying parties may be government entities, registered foreign companies and Australian private sector entities. Eligible private sector entities include companies, trusts, partnerships and associations can apply to the *Regulator* to participate in the AGDIS.

Foreign companies not registered in Australia are ineligible to participate in the AGDIS.

The AGDIS is an important national asset and will be protected accordingly. If an entity is eligible to participate in the AGDIS, the Minister may direct the *Regulator* not to approve participation in the AGDIS on national security grounds. The Minister may make this direction based on an adverse or qualified security assessment provided in accordance with the *Australian Security Intelligence Organisation Act 1979 (Cth)*.



See further: Bill Chapter 4, Part 2, Division 2

Conditions of approval to participate in the AGDIS

The Australian community expects that only trusted and reliable entities will be able to offer them Digital ID services.

To meet that expectation, the Bill will give the *Regulator* the power to ensure entities looking to participate in the AGDIS meet those expectations. Before the *Regulator* approves an accredited entity to participate in the AGDIS, entities must satisfy the *Regulator* that they will be able to comply with:

- Digital ID data standards
- The relevant service levels

- Any conditions imposed on them by the *Regulator*, such as those relating to the collection or disclosure of a restricted attribute.
- The Interoperability principle (see [Interoperability](#))
- Any other conditions set out in the Digital ID Rules.

The Rules will include conditions that prohibit participants from holding information involved in the AGDIS overseas, and requiring entities to have procedures in place to notify the *Regulator* of any significant changes to its IT system that would affect the proper functioning of the AGDIS.

To ensure the relying party services available through the AGDIS meet Australians' expectations, the *Regulator* must be satisfied that a relying party is appropriate to participate in the AGDIS. To make that decision, the *Regulator* may assess whether the relying party is a fit and proper person before approving them to participate in the AGDIS. The fit and proper person test will be detailed in the Digital ID Rules. Note, accredited entities will already have satisfied this requirement as part of their accreditation.

In addition to these general requirements, the Bill will enable the *Regulator* to make discretionary, administrative decisions about who can and cannot participate in the AGDIS. The *Regulator* may also consider the risk to the security, reliability and stability of the operation of the AGDIS when making its decision. The Bill will provide for decisions of the *Regulator* to be subject to review, including by the Administrative Appeals Tribunal (AAT).



See further: Bill Chapter 4, Part 2, Division 2 and 4 & Digital ID Rules, Part 3

The Bill requires the *Regulator* to maintain a register of all entities participating in the AGDIS. The Bill outlines the information the register must contain, such as:

- services the entity is allowed to perform in the AGDIS
- any conditions imposed on the entity, including the identity proofing and types of credentials that the entity is authorised to provide
- whether the entity's accreditation or approval to participate has been suspended or revoked at any time.



See further: Bill Chapter 7, Part 3

Conditions of participation in the AGDIS

The Australian community expects that entities participating in AGDIS are trusted and reliable whenever they offer Australians Digital ID services through the AGDIS.

To meet those expectations, the Bill will include a default condition requiring the participant to comply with the Act (see above at 'Conditions of approval to participate in the AGDIS') after they are approved to participate. If the entity does not comply, their participation could be suspended or terminated.

Entities participating in the AGDIS must also comply with conditions in the Digital ID Rules, such as the requirement to report matters to the *Regulator*. The matter to be reported will include fraud or cyber security incidents, change in control of companies, insolvency events and changes in key contractors providing Digital ID services for the entity.

Any special conditions imposed by the *Regulator*. Special conditions may deal, for example, with:

- the kinds of attributes or restricted attributes of individuals the entity is authorised to collect or disclose if not already imposed as an accreditation condition; and
- for relying parties, details of its services which can be accessed using an AGDIS Digital ID.

This is to ensure the *Regulator* has transparency over the kinds and numbers of services using Digital IDs within the AGDIS.

Special conditions will be necessary due to the different circumstances and services provided by participating entities.

If the entity does not comply with their conditions of participation, the Regulator will be able to suspend or terminate their participation (See **Powers of the Regulator govern the Accreditation Scheme and the AGDIS**)



See further Bill Chapter 4, Division 2 and Division 4

The Independent Digital ID Regulator

The Australian Competition and Consumer Commission (**ACCC**) will be the initial independent *Regulator* with responsibility for governing the Accreditation Scheme and approving entities to participate in the AGDIS. For other, more operational matters about the AGDIS only, Services Australia may have a governance role to ensure the integrity and performance of the AGDIS.

The *Regulator* will be required to give an annual report to the Minister, for presentation to the Parliament about its regulatory functions for Digital IDs. The report will include details on the number of applications and approvals for accreditation or participation in AGDIS, and the number of digital identity fraud or cyber security incidents and the responses to any such incidents reported to the *Regulator*.

Powers of the Regulator to govern the Accreditation Scheme and the AGDIS

The Bill grants the *Regulator* a range of specific powers to monitor and enforce compliance with the obligations in the legislation and rules. The Bill grants the *Regulator* powers to:

- give directions to entities
- require an entity to produce information or documents
- issue a notice requiring the entity to remedy the breach or to undertake a compliance assessment
- suspend or revoke an entity's accreditation or approval to onboard to the AGDIS
- place conditions on an entity's approval to participate
- anything else necessary to fulfill its functions.
- For matters other than the additional privacy safeguards (where the Information Commissioner is the relevant *Regulator*) the legislation grants the *Regulator* powers to:
 - issue infringement notices
 - seek enforceable undertakings
 - seek injunctions and
 - seek civil penalties (a financial penalty or a fine) from *onboarded* entities which commit the following:

Conduct	Penalty units	Maximum penalty (as at September 2023)	Regulated by
Participating without approval	200 units	200 units For individuals: \$62,600 For corporate or government entities: \$313,000	<i>Regulator</i>
(accredited entities only) Failure to comply with redress obligations			
Misuse of trustmarks			
Failure to comply with directions		300 units For individuals: \$93,900 For corporate or government entities: \$469,500	
Failure to comply with notices to produce documents			
Failure to keep records			
Failure to destroy or de-identify information			
Holding digital identity information outside Australia	300 units		

The *Regulator* and its staff commit an offence (punishable by 2 years' imprisonment or a civil penalty of 120 penalty units) if personal information or commercially sensitive information is disclosed outside of the conduct of their duties unless a valid exemption applies (for example, they are required to disclose it under another law or the individual to whom the information relates has expressly consented).

Fees and charging for provision of services

The Bill provides for the *Regulator* to charge fees. There is no intention to introduce charging of fees for participation in AGDIS when the Bill is introduced. The intention of the provision in the Bill is to allow for charging of fees that could be introduced in subsequent phases, subject to Government decision.

The Bill also allows the *Regulator* to set fees for accreditation, and to set rules to govern how accredited entities may charge fees for their accredited services.

The Bill precludes rules being made that would charge an individual a fee to create a Digital ID to use in the AGDIS. This limitation recognises the relying party services available through the AGDIS are primarily government services, and it is not appropriate for the Commonwealth to charge individuals a fee to access taxpayer funded services.



See further: Bill Chapter 8, Part 6

The Data Standards Chair

The Bill will also ensure a body is responsible for setting and publishing nationally consistent data standards used in the Accreditation Scheme and the AGDIS. The Australian Digital ID Standards Chair (**the Chair**) will be responsible for setting these standards and making them publicly available via the Federal Register of Legislative Instruments. Data Standards can be made to cover emerging technologies such as verifiable credentials and digital wallets. The Chair will receive support and advice from committees with technical expertise any may consult with the Information Commissioner and the *Regulator*. Before making the standards, the Chair must consult the Minister.

The degree of independence of the Chair from Government, and whether an existing body or new body could perform the function of the Board, is being considered further.



Question: Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?



Question: What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?