



Australian Government
Department of Finance



**Submission to the
Senate Economics Legislation Committee**
**Inquiry into the Digital ID Bill 2023 and the Digital ID
(Transitional and Consequential Provisions) Bill 2023**

January 2024

Contents

Executive Summary	3
What is Digital ID?	5
Common misconceptions about Digital ID	6
Australia’s Digital ID System	7
The current accreditation scheme	8
The current Australian Government Digital ID System	8
Benefits of Digital ID	9
Overview of the legislation	11
Purpose and structure of the Digital ID Bill	11
The legislated Accreditation Scheme	11
The legislated Australian Government Digital ID System	12
Transitioning from the current system to the legislated Digital ID System	13
Role of delegated legislation	13
Key issues raised during consultation on the draft Digital ID Bill	15
Voluntariness of Digital ID	15
Privacy and security of personal information	16
Phased expansion of the Australian Government Digital ID System and private sector participation	19
Charging arrangements	20
Conclusion	21
Appendix A: Current and intended future state for Australia’s Digital ID System	23

Executive Summary

The Department of Finance (Finance) welcomes the opportunity to provide a submission to the Senate Economics Legislation Committee's inquiry into the Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023. This submission aims to assist the Committee's inquiry by providing additional detail on key aspects of the Bills and the underlying policy intent — particularly in areas where stakeholders provided feedback during public consultation.

On 30 November 2023, the Minister for Finance, Senator the Hon Katy Gallagher introduced the Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023 (the Transitional Bill) into the Senate.

These Bills have their origins in the 2014 Financial System Inquiry. The Inquiry highlighted that the fragmented approach to ID verification in Australia creates significant costs to individuals, businesses and the broader Australian economy. The Financial System Inquiry recommended developing a national strategy for a federated-style model of trusted Digital IDs in which public and private sector identity providers would supply Digital IDs, thereby enhancing consumer choice, privacy, innovation and efficiency.

This led to the development of the Trusted Digital Identity Framework ('the accreditation framework') and provided key elements of the policy intent underpinning the Bills today. Development of the accreditation framework commenced in 2016 to foster a consistent national standard for Digital ID and establish the accreditation requirements for Digital ID services currently operating in the Australian Government Digital ID System. Since that time, the framework has been through a series of iterations and it now forms the basis for the Accreditation Scheme in the Digital ID Bill.

The issues raised in the Financial System Inquiry remain relevant, as recognised in the Productivity Commission's *2023 5-year Productivity Inquiry: Australia's data and digital dividend*. The Productivity Commission advocated for expansion of access to Digital ID in Australia, warning that having multiple ID verification systems between Australia's governments and the private sector would hinder the customer experience and limit the potential efficiency gains.

The Productivity Commission also recognised Digital ID's place more broadly as a major economy-wide reform with potential significant economic, security and privacy benefits. From a security perspective, recent data breaches such as the Optus, Medibank and Latitude breaches have highlighted the risks of current ID verification and personal information collection practices in the economy. Digital ID can help address these risks by providing alternative methods to verify people's ID in a safe, secure and privacy-enhancing way.

The Digital ID Bill seeks to modernise Australia's Digital ID arrangements by legislating:

- an economy-wide Digital ID Accreditation Scheme, which sets the benchmark for Digital ID services and embeds important protections including security requirements and restrictions on data collection and profiling by providers
- additional privacy safeguards beyond those in the *Privacy Act 1988* (Privacy Act), to better protect people's personal information used to verify ID with an accredited provider

- independent regulatory oversight via an independent Digital ID Regulator (initially the Australian Competition and Consumer Commission (ACCC)) and a System Administrator, an expanded role for the Information Commissioner as privacy regulator, and a Digital ID Data Standards Chair responsible for data standards; and
- an Australian Government Digital ID System that state and territory governments and the private sector can choose to participate in, and additional requirements for participants, such as:
 - requirements to ensure a Digital ID must be voluntary for Commonwealth services in the system, where a person is acting in an individual capacity, and that Commonwealth services in the system cannot be exempted from this requirement
 - interoperability obligations, to ensure people can choose which Digital ID provider they use to verify their ID when accessing services as the system expands to include more Digital ID providers; and
 - strong security and privacy requirements for participants in the system, that are additional to the requirements of the Accreditation Scheme.

The intent of these reforms is to make using a Digital ID safer, drive consistency across the economy through the Accreditation Scheme and enable people to use a Digital ID if they choose with confidence their personal information is safe and secure when they use an accredited provider. This will mean that, over time, individuals, businesses, community organisations and governments can all benefit from safe and secure Digital IDs.

The Digital ID Bill is supported by the Transitional Bill, which aims to provide for a seamless transition from the current accreditation scheme and Australian Government Digital ID System to the new statutory framework set out in the Digital ID Bill. The other key function of the Transitional Bill is to amend relevant Commonwealth legislation to ensure that the Digital ID Bill operates as intended. Specifically, the Transitional Bill will amend the:

- *Privacy Act 1988 (Cth)*
- *Taxation Administration Act 1953*
- *Competition and Consumer Act 2010*
- *Administrative Decisions (Judicial Review) Act 1977 (Cth)*
- *Age Discrimination Act 2004*; and
- *Australian Security Intelligence Organisation Act 1979*

Finance has developed this submission with input from Commonwealth agencies including the Attorney-General's Department, the Digital Transformation Agency and the ACCC.

What is Digital ID?

Digital ID is a secure and convenient way for people to verify their ID both online and in-person when required. The Bill defines Digital ID (in the context of an individual) as ‘a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services.’ It is not a new ID card or number, and relies on a distributed, federated architecture to:

- minimise data collection during ID verification, thereby reducing the potential impact of data breaches involving people’s personal information and data; and
- leverage existing government-held ID information (e.g. driver licences, passports) to enable verification, without centralising this identity information in one place.

Different types of Digital ID services have progressively become available in Australia and internationally. For example, Australia Post launched its Digital iD service in 2017, and the Australian Government’s Digital ID provider myGovID launched in 2019. Internationally, governments and private sector organisations have introduced a variety of Digital ID services over the past two decades to make it easier and safer for people to verify their ID when interacting with different services.

People can create a Digital ID by sharing a set of attributes (information that is associated with the individual) with a Digital ID provider. This can include basic information that can help verify an individual’s ID, such as their:

- current or former name
- date of birth
- current or former address; or
- their mobile phone number or email address.

The Digital ID provider then confirms the person’s attributes through various processes. This can include comparing the attributes to existing government-issued ID documents, such as passports, driver licences and birth certificates. This checking typically occurs through use of the Identity Verification Services, administered by the Attorney-General’s Department, which enables once-off electronic verification of the person’s details against the document issuer’s official record; or through non-digital processes such as having people present in-person with their ID documents or provide certified copies.

The strength of the Digital ID a person wants to create will determine the type and number of attributes they need to provide to a Digital ID provider. For example:

- A **basic** Digital ID (Identity Proofing Level 1) requires one email address or mobile phone number. Someone might use this type of Digital ID to book accommodation for a holiday or access a video streaming service – where verifying ID to a high level is unnecessary.
- A **standard** Digital ID (Identity Proofing Level 2) requires two acceptable ID documents such as an Australian driver licence, Medicare card, or Australian birth certificate. This level of proofing might occur where someone is setting up a new utility account or for certain financial transactions.
- A **strong** Digital ID (Identity Proofing Level 3) requires at least two ID documents, one of which must include a facial photograph of the person (e.g. an Australian passport).

A person also needs to prove they are the same person as shown on the ID documents, by scanning their face with their smart device, and where available consenting to the use of Face Verification Services to biometrically verify the face presented to the source document held by the issuer. This level also requires one 'commencement of identity' document such as a visa or birth certificate. This level of proofing is common when accessing income support and related government services online, noting the Digital ID Bill includes requirements to maintain alternative (e.g. non-digital) access channels.

Once a Digital ID provider has received the appropriate attributes and verified them, it can issue a person with a Digital ID. In most instances a Digital ID is issued via a mobile application. A Digital ID only needs to be created once and can then be reused across different services whenever the person is asked to verify their ID or other attributes about themselves (e.g. that they are over 18 or hold a licence).

Common misconceptions about Digital ID

To assist the Committee's consideration, the following section aims to clarify common misconceptions about what a Digital ID is and how it can be created and used under the Digital ID Bill:

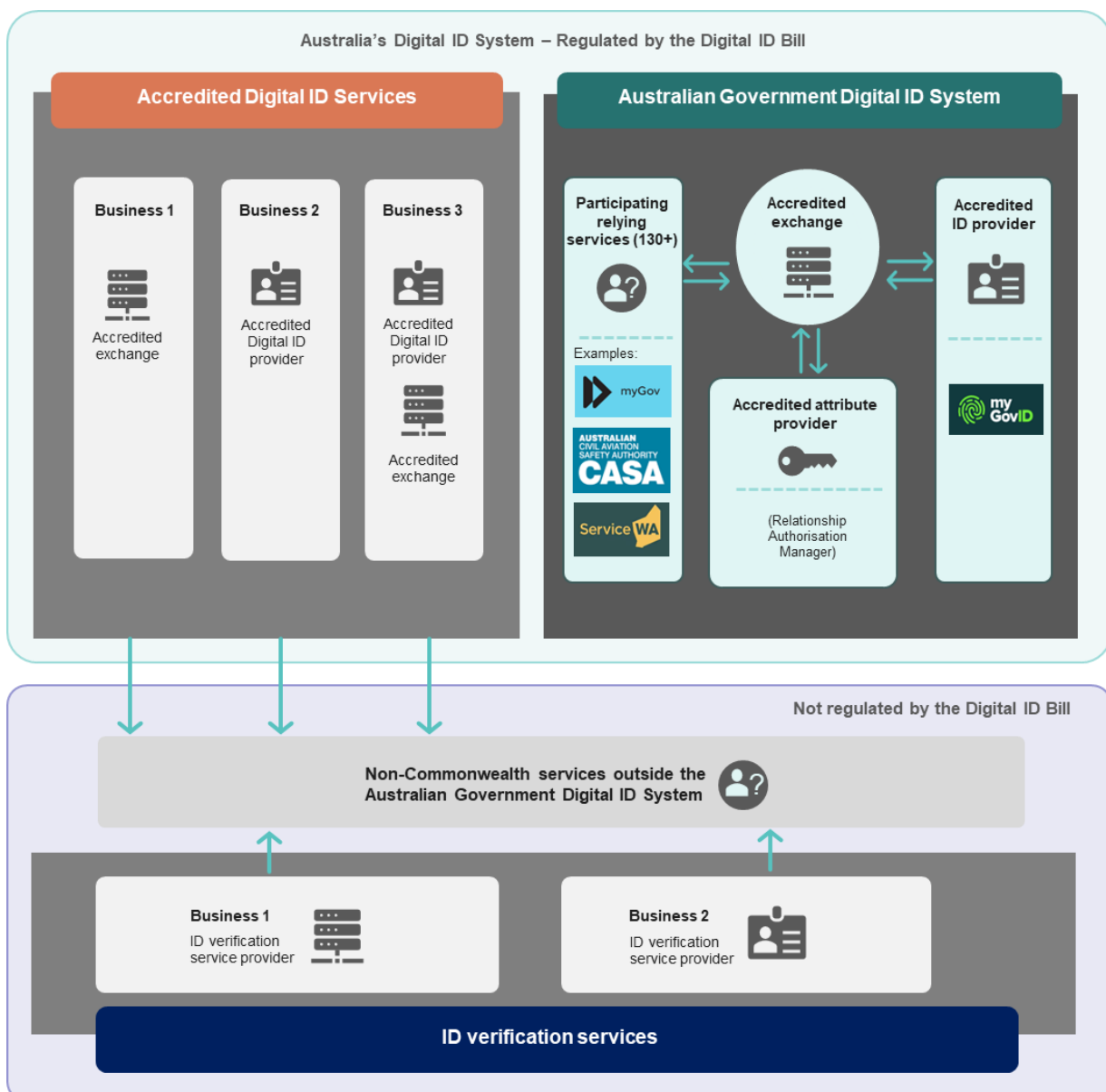
1. A Digital ID is not a new ID card or unique number or identifier for individuals. A Digital ID is created by verifying information against existing government-issued ID documents, which then allows a person to be distinguished from other people when interacting with a service online.
2. A Digital ID cannot be used to track individuals or their activities across different services or for general surveillance of people via their Digital ID. The Digital ID Bill contains protections to ensure surveillance cannot occur, as discussed on Page 18.
3. Creating a Digital ID does not lead to centralisation of ID data and information in one place, such as a single database or system. Australia's Digital ID arrangements rely on a federated architecture which avoids centralisation of ID data. In particular, an individual's different identity documents are kept by the issuer. Pages 16-19 provide further detail on protections to minimise data collection and sharing.
4. The Digital ID Bill does not make a Digital ID compulsory for individuals and includes specific requirements in the Australian Government Digital ID System to ensure a Digital ID remains voluntary for individuals accessing Commonwealth services unless they are representing a business.

Australia’s Digital ID System

Australia’s Digital ID System provides a secure, convenient, voluntary and inclusive way for people to verify their ID when interacting with government and businesses. It consists of:

- the current accreditation scheme for Digital ID services, and the Accreditation Scheme created by the Digital ID Bill; and
- the Australian Government Digital ID System, which will be legislated via the Digital ID Bill and currently enables people to use a Digital ID across a range of government services.

Figure 1: Australia’s Digital ID System and regulatory scope



The Digital ID Bill aims to establish governing regulation across the Australian Government Digital ID System and the Accreditation Scheme. The Bill does not regulate ID verification services more broadly, or non-Commonwealth services outside the Australian Government Digital ID System (e.g. businesses) that choose to use ID verification services.

Additional context on the current and intended future state for Australia's Digital ID System and the Accreditation Scheme established by the Digital ID Bill, including the continuum of existing ID verification methods available in the economy today, is at **Appendix A**.

A key policy intent of the Digital ID Bill is to, over time, enable more ID verification to occur using accredited Digital ID providers, thereby enhancing security and protections for people when they verify their identity. This also includes incentivising providers to seek accreditation (e.g. via a trustmark they can use to show they are accredited) and encouraging services to use accredited providers to meet their ID verification needs (where applicable).

The current accreditation scheme

The accreditation framework specifies standards for Digital ID service providers currently accredited under the scheme, including providers operating in the Australian Government Digital ID System. Development of the accreditation framework commenced in 2016 in consultation with industry, government agencies, international standards organisations and foreign governments.

The current accreditation scheme sets a range of requirements for Digital ID services. This includes requirements to ensure their services are secure and easy to use, and includes requirements for:

- accessibility and usability
- privacy protection
- security and fraud control
- risk management; and
- technical integration and interoperability.

Since 2016, the accreditation framework has been through six iterations, guided by continued stakeholder consultation, to ensure it remains fit for purpose and continues to enhance privacy and security as technology and user needs develop. This iterative improvement has cemented the accreditation framework as the key standard for Digital ID in Australia and supported its evolution to form the basis of the Accreditation Scheme.

The current Australian Government Digital ID System

Currently, more than 10.5 million Digital IDs have been created using the Government's Digital ID provider, myGovID, which can be used to access over 130 Commonwealth and state and territory government services.

As illustrated at **Figure 1**, the Australian Government Digital ID System includes:

- myGovID, which is the Australian Government's Digital ID provider and has been operating since 2019 (Accredited)
- the Services Australia identity exchange (Accredited)
- the Australian Taxation Office's (ATO) Relationship Authorisation Manager (RAM), which provides access to business authorisations as attributes in the Government System (Accredited); and

- a range of Commonwealth and state and territory government relying services that consume services provided by the above accredited Digital ID services.

The Australian Government Digital ID System initially focused on Commonwealth services, however, over time, some state and territory government services have joined to test its expansion outside Commonwealth services. Existing participating services will have the option to transition under the new legislative framework created by the Digital ID Bill via the Transitional Bill and associated legislative rules.

Benefits of Digital ID

Enabling wider use of Digital ID via the Accreditation Scheme and the Australian Government Digital ID System will deliver a range of benefits to individuals and the community, businesses and government.

From a **broader economy perspective**, Digital ID can help improve productivity by reducing time spent verifying people's ID and can also reduce losses associated with data breaches involving people's ID data and information.

For **individuals and the community**, Digital ID can:

- Provide a safe, secure, convenient and reusable way to verify their ID online if they choose, without repeatedly sharing copies of their ID documents with different services.
- Make it easier to access government and business services at home, or without having to travel to a shopfront or make a phone call to verify their ID – particularly benefiting groups such as regional and remote communities and people with a disability.
- Enhance privacy and reduce collection of personal information by government and private services, thereby reducing the impacts of any data breaches that may occur.
- Reduce the need to remember many different usernames and passwords for different services by providing a reusable Digital ID that can be used instead.

The Office of the Australian Commissioner's (OAIC) 2023 Australian Community Attitudes Towards Privacy Survey indicated that three-quarters of Australians' surveyed feel data breaches are one of the biggest privacy risks they face today, according to. By using Digital ID to reduce the potential impact of future data breaches, people can be better protected from scams and identity crime, which are estimated to have an annual economic impact of more than \$3.1 billion each year (Australian Institute of Criminology estimates).

The legislation will also help ensure that accredited Digital ID providers are governed by enforceable requirements, so people can trust their information is safe and secure.




For **business and government**, Digital ID can:

- Provide a simpler way to verify the ID of customers (subject to specific legislative obligations and Digital ID's suitability to meet these obligations).
- Reduce business risk, such as risks of identity fraud and data breaches, by reducing the need to collect and store people's ID documents and/or personal information.

- Enhance efficiency and productivity, by making it quicker and easier to verify a person's ID or attributes (e.g. that they are over 18, are authorised to work with vulnerable people including children, or have a certain business authorisation).
- Provide assurance that a person's ID has been verified to a high standard during an online transaction, particularly where they use an accredited provider.
- Enable faster delivery of assistance for people or businesses in need, such as:
 - people affected by scams or fraud
 - during and following natural disasters where people's ID documents are lost or destroyed; and
 - where people have left their homes due to the impacts of family or domestic violence and can use a Digital ID to maintain access to support.

For businesses offering Digital ID services (or considering doing so), a legislated scheme and associated rules will provide a nationally consistent set of standards they can seek accreditation against. This can help drive consistency in the market and allow providers to demonstrate they have meet stringent privacy and security requirements set by government.

Practical examples of where Digital ID can provide benefits for individuals and businesses currently and in future are provided below:

	Without a Digital ID	With a Digital ID
 <p>Accessing government services Raya recently had a child and will need to apply for a Centrelink Customer Reference Number (CRN) for her child, so she can claim child-care benefits.</p>	Raya will need to travel to a shopfront to show her ID.	Raya can log on to her computer, verify her ID online with a Digital ID, and apply for a CRN online at home.
 <p>Natural disaster support Amir and his family lost their house during a recent flood, and he needs to prove who he is to access government support.</p>	Amir will find it more difficult to prove his identity, given his ID documents were lost in the recent flood.	Amir had already set up a Digital ID before the flood. With his mobile, he can log on online and quickly verify his ID to access support.
 <p>Future use case – Applying for a rental property Nina is looking for a rental property and has connected with real estate agent Quian to apply for a property.</p>	Nina has to send her ID documents to Quian, who has to store copies. Every time Nina applies for a rental property, she is sending copies of her ID documents, putting them at risk of theft.	Nina can verify her ID with a Digital ID provider instead, avoiding the sharing of copies of her ID documents with Quian and other real estate agents. Quian and other real estate agents also avoid having to store copies of all their rental clients' ID documents.

Overview of the legislation

Purpose and structure of the Digital ID Bill

The objects of the Digital ID Bill are to provide individuals with secure, convenient, voluntary and inclusive ways to verify their ID in online transactions with government and businesses. The Digital ID Bill will promote trust in Digital ID services, including by ensuring less ID data is shared and stored, and where it is stored, it is stored more securely. It will also facilitate wider economic benefits.

The Digital ID Bill establishes:

- an economy-wide Digital ID Accreditation Scheme for Digital ID services
- additional privacy safeguards beyond those in the Privacy Act, to better protect people's personal information used to verify their ID with an accredited provider
- independent regulatory oversight via an independent Digital ID Regulator (initially the ACCC) and a System Administrator for the Australian Government Digital ID System, as well as an expanded role for the Information Commissioner as privacy regulator and a Digital ID Data Standards Chair responsible for data standards; and
- a legislative basis for the Australia Government Digital ID System that Australia's governments and the private sector can choose to participate in over time, and additional requirements for participants in this system.

The legislated Accreditation Scheme

The Accreditation Scheme will promote greater adoption of, and trust in, Digital ID services across the economy by providing strong, consistent standards and enforcement mechanisms such as civil penalties.

People who use an accredited service to create and re-use a Digital ID can have greater confidence that their personal information is private, safe and secure. The Accreditation Scheme is voluntary, except where Digital ID service providers want to participate in the Australian Government Digital ID System. The Accreditation Scheme enables Digital ID services to seek accreditation, to demonstrate compliance with the nationally consistent and best practice standards and safeguards in the Digital ID legislation.

On commencement of the Act, accreditation will be available for three types of Digital ID services:

- attribute service providers
- identity exchange providers; and
- identity service providers.

These services are typically found in a federated Digital ID System, which involves an identity exchange that facilitates connections between Digital ID service providers and the organisations that use their services (known as relying parties).

The federated system also involves attribute providers that can provide additional attributes to verify certain claims – such as whether a particular person can operate on behalf of a particular business.

The legislated Australian Government Digital ID System

Through the Digital ID Bill, governments and businesses in Australia will be able to provide and make use of accredited Digital ID services in the Australian Government Digital ID System. The Digital ID Bill allows services to apply to participate, either as:

1. a participating accredited Digital ID service provider – a provider offering services in the Australian Government Digital ID System, such as a Digital ID provider or identity exchange, and
2. a participating relying party – an entity that provides people with the option to use a Digital ID to access their services. This mechanism also presents the opportunity for government and business services to use accredited Digital ID services that are available in the system, such as myGovID as a Digital ID provider.

The Digital ID Bill also enables the gradual expansion of the system to enable more people to create and use Digital IDs to verify who they are and to provide access to additional state and territory and private sector services that choose to participate. Over time, the Digital ID Bill will provide people with greater choice in which accredited public and private sector Digital ID providers they use to access Commonwealth services, and vice versa.

The phased approach to expanding the Australian Government Digital ID System aims to ensure expansion only occurs once the system has achieved sufficient maturity, such as appropriate readiness of different relying party services to support users of Digital IDs. It will also allow time for the market of accredited Digital ID providers to evolve and demonstrate implementation of the Accreditation Scheme's stringent requirements, before taking the next step to enable use of these providers in the Australian Government Digital ID System.

Under the Digital ID Bill, the Accreditation Scheme and the capacity to participate in the Australian Government Digital ID System carry different benefits and levels of regulation. This will affect an entity's choice to either: participate in the system; be accredited and operate within or outside the system; or not participate.

Overall, the Australian Government Digital ID System will have the following key features as provided for in the Digital ID Bill:

- a Digital ID service provider must be accredited to participate
- the Digital ID Regulator must:
 - maintain public registers of both accredited service providers and of entities participating in the system; and
 - approve which services can participate in the system.
- a System Administrator (Chief Executive Centrelink) will be responsible for certain functions related to providing assistance to participating entities, and managing fraud and cyber incident reporting, and the availability and performance of the system; and

- participating relying parties (which provide access to government websites and apps) are not required to be accredited, however once they are participating in the system they will be required to:
 - make sure that Digital ID is voluntary for individuals acting in a personal capacity (discussed further on Page 15); and
 - provide a choice of identity provider once multiple identity providers have joined (for example, a government website will be required to allow a user to choose between a state/territory identity provider and myGovID once a state/territory identity provider has been accredited and approved to participate).

Transitioning from the current system to the legislated Digital ID System

The Transitional Bill provides for transitional arrangements, with the intent of ensuring entities participating in the current Australian Government Digital ID System prior to the commencement of the Bills will be taken to be approved by the Digital ID Regulator to participate in the legislated system. The aim is to ensure that current arrangements continue without disruption.

Entities participating in the Australian Government Digital ID System may also participate in other Digital ID systems. For example, a future accredited private sector provider could participate in the Government System (subject to phasing) and also (or alternatively) participate in a separate Digital ID system operating solely in the private sector.

Role of delegated legislation

The legislative framework for Digital ID will comprise the Digital ID Bill and a range of disallowable and non-disallowable legislative instruments. To provide certainty and accountability, all the key features of the Accreditation Scheme and Australian Government Digital ID System are in the primary legislation. This includes strong privacy and consumer safeguards (in addition to the Privacy Act).

Matters such as security requirements and data standards will be in rules, as these will require regular and time critical updates to respond to emerging fraud and cyber security risks and threats, or changes to international technical standards. The suite of technologies that underpin Digital ID are also constantly evolving. As new technologies mature and adoption grows, these technologies have the potential to disrupt existing patterns for establishing and using a Digital ID. For example, emerging verifiable credentials technologies have the potential to provide similar functionality to Digital ID in certain contexts where people need to provide details about themselves (e.g. worker screening, proving you hold a certain licence or qualification).

The Digital ID Bill includes two key mechanisms that provide the legislative framework with the appropriate level of flexibility and responsiveness to adapt as new technologies and solutions emerge. These allow the responsible Minister (the Minister) and the independent Digital ID Data Standards Chair to set new rules and standards (respectively) that would,

amongst other things, accommodate new technologies and support the implementation and ongoing administration of the legislation.

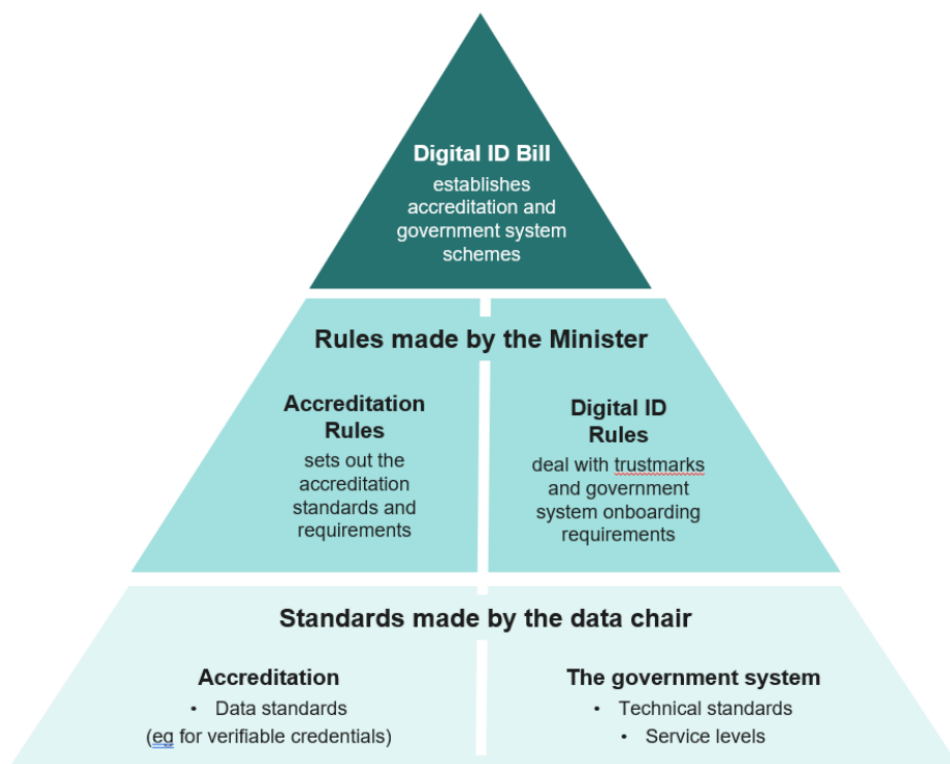
Figure 2: Structure of the legislative framework

Digital ID Bill – the primary legislation for the Accreditation Scheme, providing for all the main features of the Accreditation Scheme, Australian Government Digital ID System, regulatory powers and privacy and consumer protections.

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, disallowable instrument.

Digital ID Rules – 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.

Standards made by the Data Chair – relate to technical integration requirements or technical features for entities in relation to accreditation, or to participate in the Australian Government Digital ID System. These are legally enforceable standards published by the Digital ID Data Standards Chair.



Data standards will need to be updated as Digital ID solutions continue to evolve worldwide. The Digital ID Bill (clause 99) allows for the Digital ID Data Standards Chair to make nationally consistent standards to support the operation of the Accreditation Scheme and the Australian Government Digital ID System. Data standards made under the Digital ID Bill would be legislative instruments covering matters such as data standards, design standards, and service level determinations.

The mechanisms that allow the Minister and the Digital ID Data Standards Chair to set new rules and standards are accompanied by consultation requirements to ensure that the relevant decision-makers seek the views of a broad range of stakeholders. This is critical to ensure any rules and standards leverage the expertise of the wider market and industries where new technologies are emerging, ensuring the standards are fit for purpose.

Draft accreditation rules and Digital ID rules were publicly released with the exposure draft of the Digital ID Bill and stakeholder feedback is currently being considered. Further consultation will be undertaken on these rules and any rules required under the Transitional Bill, to allow stakeholders to provide additional feedback to inform the final rules that will accompany the commencement of the Digital ID Bill and Transitional Bill.

Key issues raised during consultation on the draft Digital ID Bill

During consultation on the exposure draft of the Digital ID Bill, stakeholders provided feedback across a broad range of topics. Finance received 113 submissions on the Digital ID Bill, providing feedback on topics such as the voluntariness of Digital ID, privacy and security, interoperability and future expansion of the Australian Government Digital ID System to include the private sector, and future charging arrangements.

To aid the Committee's consideration, the following sections provide additional information on the policy rationale for key topics raised during public consultation.

Voluntariness of Digital ID

The overall policy intent in the Digital ID Bill is that creating and using a Digital ID must be voluntary for individuals when accessing government services in their personal capacity. This aims to ensure nobody is excluded from these services if they either choose not to create a Digital ID or are unable to do so.

Clause 74 of the Digital ID Bill deals with the voluntariness of Digital ID in the Australian Government Digital ID System. This requires that creating and using a Digital ID must be voluntary for individuals acting in a personal capacity, and that Commonwealth services cannot be exempted from this voluntariness requirement by the Digital ID Regulator.

This approach also aims to accommodate circumstances where a person may not have the necessary ID documents to undertake identity proofing to the level required to access a particular service via Digital ID (e.g. Identity Proofing Level 3, which currently requires an Australian passport for face verification). In these instances, those services must maintain alternative access channels, such as paper-based, by phone, at a shopfront or other means.

Recognising the increased risk of fraud associated with some government services involving business entities, clause 74(3) of the Digital ID Bill includes a limited exception to the voluntariness requirements where a service is being provided to an individual who is acting on behalf of another entity in a professional or business capacity. Examples of these business circumstances include the creation or management of business entities and the claiming of substantial taxation or other financial benefits in a business context.

Exemption from the voluntariness requirements for non-Commonwealth services in limited circumstances

Reflecting the policy intent that creating and using a Digital ID must be voluntary for individuals acting in a personal capacity, the Digital ID Bill includes limited scope for the Digital ID Regulator to grant exemptions from the voluntariness requirements for non-Commonwealth services.

Clause 74(4) of the Digital ID Bill enables the Digital ID Regulator to consider requests for exemptions from the voluntariness requirements requested by non-Commonwealth relying parties. Commonwealth relying parties cannot seek exemptions from the voluntariness requirements.

The Digital ID Bill also recognises some specific instances where it may be appropriate for the Digital ID Regulator to grant an exemption from the voluntariness requirements for a non-Commonwealth relying party (subclause 74 (5)), such as where a relying party:

- is a small business (within the meaning of the Privacy Act)
- operates solely online, or
- is providing a service in exceptional circumstances where requiring a Digital ID may be appropriate – such as a temporary emergency situation like a flood or fire where people's ID documents have been destroyed and digital-only service still requires a high confidence in someone's identity (e.g. to access financial support).

This policy position was strengthened in response to feedback received during consultation on the exposure draft of the Digital ID Bill. In the exposure draft, a relying party service could require use of Digital ID if required by another law. This provision was removed to ensure other laws could not mandate use of a Digital ID by an individual seeking a service from the relying party, which would be inconsistent with the Digital ID Bill's intent.

Privacy and security of personal information

The Digital ID Bill aims to ensure that personal information used by accredited providers should be protected by strong privacy and security safeguards to provide the community with trust and confidence in Digital ID services.

The Digital ID Bill leverages existing privacy laws and then provides a set of additional privacy safeguards. These aim to ensure information collected when verifying or authenticating an individual cannot be used for other purposes such as marketing and behavioural tracking, in line with the community expectations that this information is handled with a heightened level of protection.

The Digital ID Bill will require accredited entities to continue to comply with existing privacy protections in the Privacy Act or an equivalent state/territory privacy law when providing their accredited services, because individuals and relying parties need to trust that these accredited entities are complying with a core set of privacy obligations.

Where a state or territory entity is not subject to a local privacy law, and seeks to become an accredited provider, the Digital ID Bill provides for the entity to enter into a binding agreement under which it undertakes to comply with the Australian Privacy Principles in the Privacy Act and for its accredited services to be subject to regulation by the Information Commissioner. Similarly, small businesses not subject to the Privacy Act will need to bring themselves under the Privacy Act to be accredited.

The Digital ID Bill also extends the definition of 'personal information' (defined in clause 9) from the current term used in the Privacy Act, to include any attributes that are otherwise not covered by the Privacy Act definition. This will put beyond doubt that any attributes held by accredited entities (particularly identity exchanges) would be regulated and protected even if otherwise not considered 'personal information'. The definition will be reviewed against any future amendments made to the Privacy Act.

Other additional privacy safeguards in the Digital ID Bill that enhance how information must be protected and used by accredited entities, to enhance community trust in Digital ID, include:

- requirements for express consent of a person to create a Digital ID and before information about them can be collected, used or disclosed to a service they wish to access
- requirements to deactivate a person's Digital ID if they withdraw their consent at any time
- prohibitions on collecting particularly sensitive types of personal information, such as a person's political opinions or sexual orientation
- restrictions on the use and retention of biometric information, including a prohibition on one-to-many biometric matching
- restrictions on the use of certain single identifiers between entities
- restrictions on data profiling; and
- restrictions on the use of personal information for direct marketing purposes.

The Digital ID Bill includes measures which mean the Digital ID Regulator must be notified of any data breaches of accredited entities under the notifiable data breach scheme in the Privacy Act; or an equivalent state or territory data breach scheme. This intends to facilitate the quick mitigation of the risk, or remediation of the breach. Where an entity is not covered by a notifiable data breach scheme, the Digital ID Bill's provisions extend the Privacy Act's existing scheme to that entity.

To allow these protections to be meaningfully regulated and enforced, the Digital ID Bill provides the Information Commissioner with a full suite of investigative and compliance powers. The Digital ID Bill provides for accredited entities to be subject to financial penalties imposed by a court, enforceable undertakings, injunctions and infringement notices for a breach of an additional privacy safeguard.

During consultation, some stakeholders raised concerns that community trust in Digital ID services would be at risk without strong restrictions on law enforcement access to Digital ID information held by accredited entities.

Based on this feedback, the Digital ID Bill now has revised restrictions on accredited entities disclosing both biometric and non-biometric information to law enforcement bodies. Non-biometric information may only be disclosed to law enforcement bodies in certain circumstances, including if an enforcement body has commenced proceedings against a person for an offence or breach of law imposing a penalty; if the disclosure is required under warrant; or if the individual gives express consent and the disclosure is for the purpose of verifying the individual's ID or investigating or prosecuting an offence. The ability to disclose to law enforcement is narrower for biometric information, which may only be disclosed if authorised under warrant or if the individual gives express consent and the disclosure is for the purpose of verifying the individual's ID or investigating or prosecuting an offence.

Protections against surveillance

Consultation feedback and initial privacy impact assessments on the accreditation framework recognised the need for protections to ensure accredited providers and the Australian Government Digital ID System could not be used for unwarranted tracking or general surveillance of people across services via their Digital ID.

The Digital ID Bill includes provisions which prohibit accredited Digital ID service providers from tracking customers. It also prevents the creation of identifiers by service providers to match or profile more broadly. These protections in the Digital ID Bill include:

- 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 exchanges cannot become a repository of information about an individual.
- restrictions on the disclosure of unique identifiers, to ensure a unique number created by a service to allow it to function cannot be used to track a person's online behaviour or the services they access. This reflects that a service may, in some instances, need to assign a unique identifier to an individual within a Digital ID system for technical reasons to provide their customers with a service or feature.
- Digital ID service providers 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 are limited and would include using the information to provide services, or for the entity to demonstrate its compliance with obligations in the Act.
- restrictions on the purpose a biometric can be collected and disclosed, which are primarily for verification or authentication purposes. One to many matching, which can be associated with surveillance, is completely prohibited by the Digital ID Bill.

Protections to minimise data breach risks

During consultation, some stakeholders raised concerns that enabling wider use of Digital IDs could increase the risk of data breaches involving people's personal information.

One of the key benefits of Digital IDs is the ability to reduce the sharing of people's ID documents and information with different services, and the associated storage of this information by different services. This reduction in sharing and collection can reduce the impacts of a data breach if one of these services is compromised, and reduce the number of potential avenues for such a data breach to occur (by limiting the collection of ID information by services).

With respect to accredited Digital ID service providers that need to collect some personal information to provide Digital ID services, the Digital ID Bill provides protections by:

- leveraging the existing federated architecture in Australia for ID verification, which relies on existing government-held ID information (e.g. driver licences, passports) to enable verification, without centralising this identity information in one place
- minimising the collection of biometric information held by Digital ID service providers; and
- requiring accredited Digital ID service providers to meet minimum security requirements, including appropriately minimising data holdings and threats.

Phased expansion of the Australian Government Digital ID System and private sector participation

The original Financial System Inquiry vision for Digital ID in Australia recommended a federated-style model of trusted Digital IDs, in which a user could choose to create a Digital ID from public and private sector identity providers. To address risks of fragmentation, the Financial System Inquiry recommended developing a common national strategy to set the framework and standards. This aimed to foster efficient development of a market of Digital ID providers to enhance choice, privacy and security.

Consistent with this policy intent, the Digital ID Bill enables gradual expansion of the Australian Government Digital ID System to include states and territories and, in time, the private sector. As it occurs, this expansion will enable people to choose which Digital ID provider they use to access services in the system. As more identity providers are accredited and join the system, users will have more choice. The intent is this will ultimately foster specialisation among Digital ID services to meet different user requirements, while maintaining the highest levels of security and privacy.

Clause 60 in the Digital ID Bill enables the Minister to manage the expansion of the Australian Government Digital ID System to entities outside the Commonwealth. Under subclause 60(1), the Minister may determine the kinds of entities (other than those Commonwealth entities specified in paragraphs 61(a) and (b)), which can apply to participate at any time. This allows the Minister to ensure the system is operating appropriately once the Digital ID Bill commences and in each phase, before expansion to the next phase occurs.

It is expected that each phase will proceed sequentially as each preceding phase demonstrates sufficient maturity, for example the readiness of different relying party services to support users of Digital IDs. The Government will consult with stakeholders to inform decision-making on phasing.

Interoperability requirements and exemption from interoperability

The Digital ID Bill ensures that people can choose which Digital ID provider they use to access a service in the Australian Government Digital ID System once multiple providers are available in future phases. This is achieved via the interoperability obligation (clause 79) which prohibits participating relying parties from limiting consumer choice, and by prohibiting accredited entities from limiting their interactions with each other, unless the Minister grants an exemption.

The Second Reading Speech outlined the circumstances under which exemptions from the interoperability obligation will be considered in the system. Exemptions will only be granted in limited circumstances, such as for government services where there is potential for identity fraud to have a significant impact on the financial circumstances of individuals or businesses in Australia.

For example, services within Australia's tax and transfer system, which currently enable over \$150 billion per year in tax refunds and support around \$220 billion in payments per year, present prominent fraud targets where it is critical to carefully manage risk. It therefore may be appropriate to consider limiting the number of Digital ID providers that can be used in these service contexts, via exemptions from the Digital ID Bill's interoperability obligation.

Charging arrangements

During consultations, stakeholders sought clarity on future charging arrangements in the Australian Government Digital ID System. Some stakeholders also expressed their view that people should not be charged to create or use a Digital ID to access government services.

The policy position in the Digital ID Bill is that individuals should not be charged to create or use a Digital ID in the Australian Government Digital ID System. This aims to ensure that people are not excluded from access to a Digital ID, or government services that use it, based on their financial circumstances.

More broadly, there are three key instances where charging is relevant to Digital ID including under the Digital ID Bill:

1. Fees charged by the Digital ID Regulator (for example, fees for accreditation)
2. Fees charged by entities participating in the Australian Government Digital ID System (for example, Digital ID service providers charging services for ID verification transactions)
3. Fees charged for Digital ID services in the private sector, including by accredited Digital ID service providers that operate outside the Australian Government Digital ID System

The Digital ID Bill includes requirements relevant to the first two types of fees above but does not regulate the charging of fees for Digital ID services more broadly in the economy. This reflects that charging in the private sector is a commercial consideration for those providers, and the policy intent focuses on managing charging arrangements associated with the Australian Government Digital ID System and delivery of the Accreditation Scheme.

For the first type of charging above, clauses 144 through 147 of the Digital ID Bill govern charging of fees by the Digital ID Regulator. This includes that any fees for applications, such

as accreditation, will be prescribed in the Digital ID rules. This part specifically prohibits creating legislative rules for charging by the Digital ID Regulator that would allow the charging of a fee to an individual for the creation or use of a Digital ID of the individual. It also prohibits creating a fee via these rules that would amount to taxation.

For the second type of charging above, clause 148 of the Digital ID Bill governs fees charged by accredited entities in relation to the Australian Government Digital ID System. It requires that accredited entities charging fees for their services in the system must do so in compliance with the Digital ID Rules. Any rules made on charging will not otherwise affect the ability of an accredited entity to charge fees for their accredited services, such as in another Digital ID system. Under these arrangements, accredited entities may be able to charge fees for services such as ID verification or authentication, and other services provided to each other in the Australian Government Digital ID System.

Future charging arrangements and considerations

There are currently no charging arrangements in the Australian Government Digital ID System. In practice, this means government services currently using Digital ID (via myGovID) in the system are not charged when people choose to use a Digital ID. Similarly, there is currently no charging for accreditations under the current accreditation scheme that will be transitioned to a legislated Accreditation Scheme via the Digital ID Bill.

Any future charging arrangements remain subject to Government consideration and would be informed by stakeholder consultation. Any such arrangements would need to adhere to the requirements of the *Australian Government Charging Framework*. The Framework provides for regulatory activities (such as accreditation) to charge fees or levies to recover the costs of the regulatory effort associated with regulatory activities. This charging cannot exceed the efficient cost of delivery and can be full or partial cost recovery. Arrangements must also meet specific procedural requirements, such as having sufficient external consultation, an agreed charging model, and a Cost Recovery Implementation Statement.

Any future charging arrangements will also be subject to periodic review. As per clause 145 of the Digital ID Bill, the Minister will be required to periodically review any charging arrangements implemented via the rules under subsection 144(1), to ensure they remain fair and reflect current circumstances. The first review must occur no later than two years after rules made under subsection 144(1) commence and be completed within 12 months, with subsequent reviews being required to start within two years after the completion of the previous review.

Conclusion

The Digital ID Bill and the Transitional Bill will establish in law for the first time a national Accreditation Scheme for Digital ID services and enforceable regulation and requirements for the Australian Government Digital ID System.

The legislation will be an important foundation for wider use of Digital IDs across business and government in Australia. It will provide increased privacy and consumer protection, where people who choose to use a Digital ID provided by an accredited service provider can be confident their information is safe and secure, and that their privacy will be protected.

The legislation will also enable phased expansion of the Australian Government Digital ID System, as a key mechanism to support interoperability and user choice across government and, in time, private sector services that choose to participate. Collectively this will help enable wider use of Digital ID and realisation of its wider productivity, safety and security benefits for all Australians.

Appendix A: Current and intended future state for Australia's Digital ID System

