Australia's Digital ID System

Australian Government

Your guide to the Digital ID Rules, Digital ID (Accreditation) Rules and Digital ID (Accreditation) Data Standards

May 2024 public consultation

www.digitalidentity.gov.au

Department of Finance

Contents

Introduction

Digital ID Bill 2024

The Digital ID Bill 2024 and the Digital ID (Transitional and Consequential Provisions) Bill 2024 were passed on 16 May 2024. The Bills are expected to receive Royal Assent in the coming weeks with the Acts expected to commence by November 2024.

This legislation authorises a package of multiple legislative instruments which govern the Accreditation Scheme and the Australian Government Digital ID System. The Digital ID Act 2024 will be the primary legislation for the Accreditation Scheme and the Australian Government Digital ID System. The Act will allow for legislative rules and data standards to be made. This public consultation focuses on three of these rules and standards:

- the draft Digital ID Rules 2024 (Digital ID Rules),
- the draft Digital ID (Accreditation) Rules 2024 (Accreditation Rules), and
- the draft Digital ID (Accreditation) Data Standards 2024 (Accreditation Data Standards).

Using this Guide

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

Where to find more information

To help you understand more about the legislation and Australia's Digital ID System we recommend reading the source documents and resources that can be found on the Digital ID website.

Having your say

Consultation to date

The process of developing the Digital ID Rules, Accreditation Rules and Accreditation Data Standards to date has included extensive consultation with the community and industry over the past 6 years on the Trusted Digital Identity Framework (TDIF), the precursor to the voluntary legislated Accreditation Scheme. The unlegislated accreditation scheme and the Australian Government Digital ID System have been in operation since 2019. The previous public consultation on the draft Accreditation Rules and Digital ID Rules ran from September to October 2023 (previous public consultation), and development of the rules and standards has been ongoing through engagement with government stakeholders in the lead up to release of the new exposure drafts of the rules and standards.

Providing feedback

Your views on the Accreditation Rules, Accreditation Data Standards and Digital ID Rules are important. This round of consultation seeks your views on the key changes to these rules and standards since the previous public consultation. Your views will help refine the legislative instruments to be made under the Digital ID Act. If you wish to provide a submission, please read this guide.

An optional feedback template is available for your use and can be downloaded from the Digital ID website via Have your say | Digital Identity. It contains consultation questions that you may wish to use to direct your feedback. These questions are also in the tables in the Attachments in this Guide.

The consultation period will close 5:00 pm 25 June 2024 AEST. Details on how to provide your feedback are available below and on the Digital ID website.

Consultation purpose

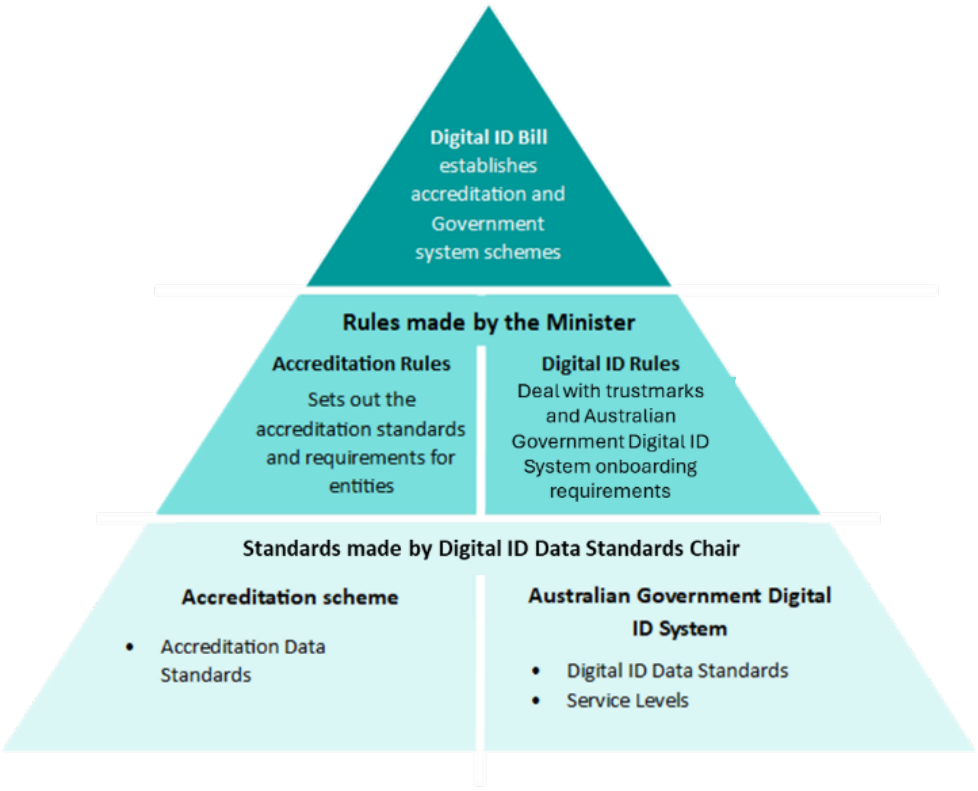
The consultation is directed towards the changes made to the Digital ID Rules, Accreditation Rules and Accreditation Data Standards since the previous public consultation for matters regarding Digital ID that are critical for your organisation.

- The key changes from the September 2023 draft Digital ID Rules are in tables A1 and A2 in from page 21.
- The key changes from the September 2023 draft Accreditation Rules are in tables B1, B2 and B3 from page 25.

Consultation timeline

Step	Estimated Timeframe
This public consultation closes	**5:00pm 25 June 2024 AEST**
Engagement on transitional arrangements engagement with accredited entities and stakeholders	**Ongoing**
Digital ID Act 2024, rules and data standards commence	**Expected November 2024**

The Digital ID legislative framework



The Digital ID legislative framework is a package of multiple legislative instruments which govern the Accreditation Scheme and the Australian Government Digital ID System.

The Digital ID Act

The Digital ID Act aims to provide individuals with secure, convenient, voluntary, and inclusive ways to verify their identity for use in online transactions with government and businesses. Promoting trust in digital ID services (including by ensuring less data is shared and stored, and in a more secure way), will facilitate economic benefits for, and reduce burdens on, the Australian economy.

The Digital ID Act:

- legislate and strengthen a voluntary Accreditation Scheme for digital ID service providers that wish to demonstrate compliance with best practice privacy, security, identity proofing, and authentication standards.
- legislate and enable expansion of the Australian Government Digital ID System for use by the Commonwealth, State and Territory governments and eventually private sector organisations.
- embed strong privacy and consumer safeguards, in addition to the *Privacy Act 1988* (Cth) (Privacy Act).
- establish independent Digital ID Regulators:

- The Australian Competition and Consumer Commission (ACCC) will be the initial independent regulator to oversee the Digital ID Accreditation Scheme and governance of the Australian Government Digital ID System.
- Services Australia will be the System Administrator, which will oversee the day-to-day operation of the Australian Government Digital ID System.
- The Information Commissioner will be the privacy regulator for accredited Digital ID services.
- A Digital ID Data Standards Chair will make technical and data standards.

The Digital ID Act enables, and in some cases requires, the Minister for Finance to make rules to set out details of how the Accreditation Scheme and the Australian Government Digital ID System will operate.

Digital ID Rules

The Digital ID Rules are to be made by the Minister for Finance to set out the requirements for entities participating in the Australian Government Digital ID System. The rules also provide for any other general requirements, such as trustmark requirements, reporting to the Digital ID Regulator and the System Administrator, and record keeping. As the Australian Government Digital ID System expands enabling state and territory governments and private sector participation, additional rules will be added supporting this phased expansion.

The Digital ID Rules will be progressed in two tranches, with tranche 1 commencing with the Act in late 2024 and tranche 2 up to 12 months later.

- Tranche 1 of the Rules will cover things required on commencement like the trustmark, reportable incidents and requirements and conditions to participate in the Australian Government Digital ID System.
- Tranche 2 will make updates to rules and cover additional areas not covered by tranche 1 including dispute resolution, interoperability and charging that require further policy development and consultation or are not required until the Australian Government Digital ID System opens up for non-Commonwealth organisations to participate.

Accreditation Rules

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

There will be three types of service an entity can be accredited to provide when the Digital ID Act commences. This table offers a simplified description of each kind of accreditation (more formal definitions will be set out in section 9 of the Digital ID Act):

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

Entities accredited under the TDIF pilot program for these roles are listed on the Digital ID website.

Accreditation Data Standards

The Accreditation Data Standards are a non-disallowable legislative instrument that support the Accreditation Rules by setting out various technical requirements associated with the accreditation scheme. These include:

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

Digital ID Data Standards

The Digital ID Data Standards are also a non-disallowable legislative instrument that support the Digital ID Rules by setting out various technical requirements relating to entities participating in the Australian Government Digital ID System.

The Digital ID Data Standards are not included in this consultation process but will be released for public consultation shortly.

Making of standards

As a transitional measure, the initial versions of the data standards may be made by the Minister so that they can take effect upon commencement of the Act and rules. After that time, it is expected that the Minister will appoint an independent Data Standards Chair.

Public consultation response to the Digital ID Rules

The Digital ID Bill and Digital ID Rules received a strong response to the request for feedback from stakeholders across the government, private sector, industry bodies and other relevant groups. Key consultation themes and our response are summarised in Table 1, with more detailed information provided in the pages following.

Table 1: September and October 2023 Digital ID Rules consultation key themes

Description	Consultation feedback	Comments
Interoperability obligation	Some stakeholders considered that limiting some Commonwealth services to myGovID (and not commercial digital ID identity service providers) would limit consumer choice of accredited digital ID providers. Stakeholders sought clarity regarding the criteria for exemptions to the interoperability obligation. This included clarity as to how a consumer could minimise the need to hold multiple digital IDs. Stakeholders supported the development of publicly available data standards to help inform interoperability requirements to support the digital ID whole of economy ecosystem.	The interoperability obligation appeared in rule 11 in the previous draft of the Digital ID Rules. This has been removed and will be dealt with in future consultations before phased expansion of the Australian Government Digital ID System to the private sector. The interoperability arrangements are not essential to the effective operation of the system while it remains 'government only' but will be required in future phases of the Australian Government Digital ID System rollout when non-government organisations may join.
Data localisation	A range of stakeholders raised concerns that requirements to store or process data in Australia for those participating in the Australian Government Digital ID System would diminish security, add to costs, and limit new participants. Additionally, stakeholders sought clarity about the data localisation rules to be made under s 77 of the Digital ID Act (a civil penalty provision).	Data localisation rules may be made under s 77 of the Digital ID Act (a civil penalty provision) to require accredited entities to keep Australian Government Digital ID System data in Australia. These would apply in addition to existing legislative obligations to store data onshore. It is not proposed that these would be dealt with on commencement of the Act as further consultation with industry is needed to ensure that these requirements do not preclude users of Digital ID systems from benefiting from best-in-class security solutions that may rely on internationally hosted cloud services.
Liability	Some stakeholders called for stronger indemnity rules for non-compliance with legislated requirements such as a guaranteed protection from liability for claims and caps on liability.	The Digital ID Rules, for commencement, are proposed to contain interim liability arrangements in respect of participants in the Australian Government Digital ID System, in line with current arrangements for the non-legislated system. The interim liability arrangements provide that accredited entities participating in the Australian Government Digital ID System will not be liable to each other or to any participating relying party for breaching the statutory contract taken to be in force under s 85 of the Digital ID Act. The interim liability arrangements will be reviewed before the phasing in private sector participants into the Australian Government Digital ID System.
Cyber security incidents	It was suggested by some stakeholders that the Digital ID Bill's definition of cyber security	The cyber security notification requirements have been simplified, better aligning the

Description	Consultation feedback	Comments
	incident should better align with other Commonwealth legislation. Notwithstanding, there was widespread support for the adoption of best-practice cyber security principles in the rules.	proposed Digital ID Rules with the Digital ID Act, incorporating the System Administrator's role into the reporting requirements (reflecting arrangements in the current unlegislated accreditation scheme (the Trusted Digital Identity Framework)). The draft Digital ID Rules specify that any notification be made as soon as practicable after, and in any event no later than, 1 business day (in place of 24 hours) after the entity becomes aware of the incident or a suspected incident
Reporting and Redress - Response to data breaches and support for those affected - Other reporting matters	Many stakeholders commented on the reporting rules – requesting additional clarity and consultation concerning the data breach reporting process, and support mechanisms for people impacted by any data breach and liability for data breaches.	Under the draft Digital ID Rules, there are specific obligations (and associated penalties for non-compliance) for the reporting and management of cyber security and digital ID fraud incidents (including suspected incidents). This includes undertaking risk assessments to identify, evaluate and manage the risks of a cyber security incident and digital ID fraud incident. These have been developed to supplement other initiatives and mechanisms for the reporting and management of data breaches such as the Notifiable Data Breach scheme. The Digital ID Act will require that rules on redress be made within 12 months of commencement of the Act. Consultation on redress will continue to inform policy development of these rules and ensure that any rules proposed are work alongside other government identity resilience and anti-scams initiatives such as the Credential Protection Register managed by the Attorney-General's Department.
Trustmarks	A range of stakeholders sought additional information and clarity about the design and use of the Digital ID trustmarks. This included how best to ensure any trustmarks are used appropriately and not fraudulently.	Section 83 of the Digital ID Act will provide that an entity must not hold out that it has approval to participate in the Australian Government Digital ID System if that is not the case. There is a civil penalty associated with this section of the Digital ID Act. Sections 117 to 119 of the Digital ID Act provide for a Digital ID Trustmark. The draft Digital ID Rules contain rules for the Australia's Digital ID System Accreditation Mark and how it can be used by accredited entities.
Onboarding - Supporting Relying Party participation - Small business - Other matters	Some stakeholders sought clearer processes to support the onboarding of relying parties to the Australian Government Digital ID System e.g. seeking consistent technical, security and operational requirements that can be easily accessible to interested entities wanting to build solutions or participate in the future in the Australian Government Digital ID System.	The Digital ID Data Standards and associated guidance material will assist with this and will be published closer to the commencement of future phases of the Australian Government Digital ID System expansion prior to private sector being eligible to apply to join.

Description	Consultation feedback	Comments
	There were also calls for a clear roll-out plan from the government for the Australian Government Digital ID System to best prepare private entities participate as phased expansion commences.	
Record keeping requirements	There were some concerns about the appropriate length of time to retain records, supporting Australian Government Digital ID System compliance processes.	The draft Digital ID Rules (and the draft Accreditation Rules) propose a six-year period for record keeping after the date the record was created or last used by the accredited entity.

Changes to the Digital ID Rules

This section details the main changes to the Digital ID Rules since the September 2023 draft went out for consultation. Attachment A from page 22 sets out the changes in more detail.

Consultation feedback

Stakeholders identified several areas for improvement or refinement in the previous draft of the Digital ID Rules. This feedback was predominantly centred around the rules being too complex or too broad, and some rules requiring clarification.

Changes since consultation

The draft Digital ID Rules have been updated to reduce complexity and improve readability for interested stakeholders seeking to apply for approval to participate in the Australian Government Digital ID System. The draft Digital ID Rules are structured as follows:

- Chapter 1 - Preliminary
- Chapter 2 – Fit and proper person considerations
- Chapter 3 – Participation in the Australian Government Digital ID System
- Chapter 4 – Reportable incidents
- Chapter 5 – Trustmarks
- Chapter 6 – Record-keeping
- Chapter 7 – Interim liability arrangements

While the overall structure is similar to the previous draft, the current draft has been amended to reflect stakeholder views. This includes new application provisions within each Chapter and changes to some processes to clarify to whom and how the rules in each Chapter apply. Three rules were removed from the current draft, which are identified in Table A1 of Attachment A (page 22). The next section highlights some of the key changes in the current draft of the Digital ID Rules.

Aligning with Anti-Money Laundering and Counter-Terrorism Financing requirements

A new draft condition on participation in the Australian Government Digital ID System is included in the Digital ID Rules to complement a condition in the Accreditation Rules and to better align the Australian Government Digital ID System with under the *Anti-Money Laundering and Counter - Terrorism Financing Act 2006 (Cth)* (AML/CTF) obligations.).

Under this draft condition, participating relying parties may collect a limited set of restricted attributes of an individual in order to comply with AML/CTF reporting requirements: namely the passport number, driver licence number, visa number, Medicare card number, or proof of age card number of an individual. This draft condition will remain subject to privacy safeguards in the Digital ID Act. For example, the customer must provide express consent for the accredited identity service provider and the participating relying party to collect and disclose the customer's restricted attributes for the purpose of the participating relying party complying with its AML/CTF obligations.

Under s 121 of the Digital ID Act, the Digital ID Regulator will be able to publish which participating relying parties are authorised to collect restricted attributes (and the restricted attributes they can collect) for AML/CTF purposes. The Regulator's compliance and enforcement powers in Chapter 9 of the Digital ID Act would enable the Regulator to monitor which entities within the Australian Government Digital ID System are collecting restricted attributes for AML/CTF purposes and ensure only entities which have AML/CTF reporting requirements have access to the restricted attributes.

Further changes to the draft condition may be required pending the outcomes of the second stage of consultation by the Attorney-General's Department on reforming Australia's AML/CTF regime to extend the existing AML/CTF legislation to certain high-risk services. High risk services include those provided by lawyers, accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones.

Reportable incidents (Chapter 4)

Consultation feedback

Some stakeholders identified a need for the reportable incident requirements in the rules to better align with pre-existing requirements that entities may be required to meet through other government regulatory schemes. Overall, stakeholders supported a strong stance in the rules to ensure strong legislative obligations for cyber security record-keeping and reporting.

Changes since previous consultation

Questions were raised during consultations on the Digital ID Bill about the scope of powers for the Digital ID Regulator across the wider digital ID system. The Digital ID Act will provide for a second regulatory body (the System Administrator). The functions of the System Administrator include to identify and manage operational risks relating to the performance and integrity of the Australian Government Digital ID System. The draft Digital ID Rules reflect this change, with some reportable incidents now required to be reported to the System Administrator.

New requirements have been added for entities to report proposed changes to their information technology systems to the System Administrator prior to the change taking place, with associated notification timeframes attached to incidents or change reports to mitigate system impacts where appropriate.

Trustmarks (Chapter 5)

Consultation feedback

A range of stakeholders sought clarity regarding the design and operation of the trustmark including ensuring non-fraudulent use of the trustmark.

Changes since previous consultation

The trustmark rules have been redrafted to clarify the conditions for the use or display of a digital ID trustmark by accredited entities. Trustmark designs are being developed in consultation with stakeholders including accredited entities, regulators and end users.

The draft Digital ID Rules contain rules for the Australia's Digital ID System Accreditation Mark and how it can be used by accredited entities.

Liability (Chapter 7)

Section 84 of the Digital ID Act will provide an indemnity to an accredited entity participating in the Australian Government Digital ID System from claims that might be made by other accredited entities or relying parties participating in the system where the accredited entity provides or does not provide its accredited services in good faith and in compliance with Digital ID Act, other than the service levels.

Section 85 of the Digital ID Act will provide that a separate statutory contract is taken to be in force between an accredited entity participating in the Australian Government Digital ID System and each other accredited entity or relying party participating in the system under which the accredited entity agrees to: provide certain accredited services in compliance with the Digital ID Act (other than the service levels); and comply with requirements in relation to intellectual property rights that are prescribed by the Digital ID Rules.

Consultation feedback

Some stakeholders sought specific indemnity provisions in the draft Digital ID Rules such as for unintentional non-compliance with legislative requirements, and caps on liability.

Changes since previous consultation

The draft Digital ID Rules, for commencement, will contain interim liability arrangements, in line with current arrangements in the unlegislated (TDIF) accreditation scheme. Under the interim arrangements, it will not be possible for a party to the statutory contract to be compensated for any purported breach of the contract. This arrangement does not apply to any other person (i.e., a person who is not a party to the statutory contract). These interim liability arrangements will be reviewed before the phased expansion of the Australian Government Digital ID System to allow for private sector participation.

Public consultation response to the Accreditation Rules

The Accreditation Rules received strong feedback from stakeholders across the government, private sector and industry bodies and groups. 30 submissions amounted to over 800 comments on the Accreditation Rules or wider Digital ID program. Key consultation themes and our summary response are set out in Table 2, with more detailed information provided in the pages following.

Table 2: September and October 2023 Accreditation Rules consultation key themes

Description	Consultation feedback	Comments
Digital ID minimum age	Stakeholders pointed to various views about an appropriate minimum age for getting a Digital ID across Commonwealth and state and territory services, legislation, and guidance. Some stakeholders supported a reduction in the minimum age for an identity service provider to create and manage a Digital ID, from 15 to either 13 or 14 years of age.	The Accreditation Rules keep the minimum age for an identity service provider to create and manage a Digital ID as 15 years of age. This is consistent with Office of the Australian Information Commissioner Australian Privacy Principles guidelines on the age an organisation or agency may assume an individual has capacity to consent to a decision about their personal information.
Regulation and barriers to entry	Some stakeholders pointed to the cost, effort and potential regulatory burden imposed by the draft Accreditation Rules as a barrier to entry of the Accreditation Scheme.	The Accreditation Rules seek to balance reducing the complexity of the regulation with delivering strong, effective privacy and security-enhancing requirements for operation of digital ID services to keep individuals' identity information safe and secure. The Accreditation Rules are primarily based on requirements published in the TDIF. Public consultation feedback and the TDIF pilot accreditation program has been used to continually assess and improve the draft Accreditation Rules.
Evidencing compliance	Some stakeholders asked for further guidance on how to show compliance with some Accreditation Rules, including what kind of evidence the Regulator would require as part of compliance reporting.	The Accreditation Rules and Accreditation Data Standards will be accompanied by explanatory statements which will provide additional rationale, impact explanation and context for the Rules. Additionally, the ACCC has established a Digital ID regulatory guidance function and will be responsible for publishing appropriate guidance information to assist entities with accreditation.
Data minimisation	Stakeholders supported the core policy for data minimisation and recommended improvements to the draft Accreditation Rules. Some entities expressed concern that compliance responsibility rested with the accredited entity rather than the relying party in deciding how a relying party enables an individual to access the service.	The data minimisation rule relating to disclosure of information has been redrafted to ensure that accredited entities who disclose personal information must provide a way for relying parties to request only the data they require an individual to provide in order to access its relying party service. This means that if a relying party only needs to confirm an individual's age to access the relying party's service (or just that they are over 18 years old), an accredited entity must have the technical capacity to be able to only disclose that information—and not, for example, any

Description	Consultation feedback	Comments
		other additional information such as the individual's name or contact details.
Independent assessor requirements for assurance assessments and systems testing	Some stakeholders asked for further guidance materials on the external, independent assessor requirements (i.e., in addition to the need for an assessor to have the skills, knowledge, and training necessary to complete the kind of assessment or system testing). Some entities were concerned the assessor requirements may not be prescriptive enough, and this may impose unnecessary costs if their assurance assessment or systems testing did not meet the regulator's requirements.	The Accreditation Rules and Accreditation Data Standards will be accompanied by explanatory statements which will provide additional information, rationale, impact explanation and context for the Rules. Additionally, the ACCC has established a Digital ID regulatory guidance function and will be responsible for publishing appropriate guidance information to assist entities with accreditation.
Data standards	Stakeholders said some parts of the draft Accreditation Rules relating to technical rules and configurations of a type of service were too prescriptive and may not support quick system responses in a rapidly changing risk and technology landscape.	The rules relating to authentication management and the testing of biometric technology have been removed and proposed to be made as Accreditation Data Standards. This will provide greater flexibility for technical data requirements to remain contemporary.
Inclusion and nominees	Stakeholders expressed support for the Accreditation Rules to focus on inclusion, usability and accessibility rules, as well as identity proofing processes and nominee arrangements.	The Accreditation Rules have been further updated to incorporate and support feedback that accredited services must be accessible and inclusive, including a new requirement for accredited entities to report on inclusion for their accredited services. This and additional updates to the rules align with provisions of the Digital ID Act that prescribe that certain inclusion-related rules must be made. The Accreditation Rules may be updated in the future to facilitate nominee arrangements. Progress on this issue is currently underway, though this is a complex area requiring much policy development and consultation.

Changes to the Accreditation Rules

This section details the main changes to the Accreditation Rules since the September 2023 draft Accreditation Rules. Attachment B from page 26 sets out the changes in more detail.

Improved structure of the rules

Consultation feedback

Consultation feedback indicated the September 2023 draft Accreditation Rules were difficult to navigate at times; requiring users to move back and forth through different chapters to understand the requirements applicable to them.

Changes since previous consultation

The draft Accreditation Rules have been restructured to improve accessibility and usability for accreditation applicants, accredited entities, and other users of the Accreditation Rules. The draft Accreditation Rules are now structured as follows:

- Chapter 1 - Preliminary
- Chapter 2 - Applying for accreditation
- Chapter 3 - Assurance assessments and systems testing
- Chapter 4 - Requirements for maintaining accreditation
- Chapter 5 - Requirements when providing accredited services
- Chapter 6 - Annual reviews
- Chapter 7 - Other matters relating to accreditation.

Accredited services must be accessible and inclusive (Part 4.4)

Consultation feedback

Feedback from the previous public consultation indicated wide support for the accessibility and usability rules but recommended that the Accreditation Rules could expand further on rules around future planning and goals for inclusion for accredited services.

Changes since previous consultation

The accreditation rules were amended to address consultation feedback and other provisions in the Digital ID Act to further support accessibility and inclusion. This includes annual inclusion reporting for entities and compliance with WCAG Version 2.1 to level A conformance for their websites and digital ID related information (such as privacy policies). Additionally, accredited entities with public-facing accredited services must take reasonable steps to comply with WCAG version 2.1 to level AA conformance for their applications or web services.

Enduring consent (rule 4.41)

An accredited entity may want to allow an individual's consent (to use or disclose personal information in the provision of accredited services) to endure for a certain period. This allows the individual to experience a more seamless user-experience with their digital ID. Advice from the OAIC is that consent should not be indefinite.

Consultation feedback

Consultation feedback indicated that there was a gap in the draft Accreditation Rules regarding the duration of consent and other related rules that were present in the TDIF. Comparable legislative frameworks such as the Consumer Data Right (CDR) ensures that the duration of consent of individuals must only be for a maximum of 12 months.

Changes since previous consultation

Accreditation Rule 4.38 (new) ensures that the duration of consent given by an individual for any future collection, use or disclosure of the individual's personal information must only be for a maximum of 12 months. Additionally, entities with public-facing services must provide individuals with a clear and simple process to withdraw or vary that consent.

Data minimisation principle (rule 4.42)

The data minimisation principle intends to minimise the collection and disclosure of personal information. The rules are designed to reduce the risk of proliferation of personal information across the digital economy.

Consultation feedback

The previous rule as written in the September 2023 draft Accreditation Rules required that an accredited entity must be satisfied that disclosure of personal information to a relying party is reasonably necessary. This meant that an accredited entity must decide what personal information a relying party requires based on an assessment of the relying party's service, and any justification provided to support the relying party's request for attributes. Most of the feedback received on this issue highlighted the difficulties that would be faced by accredited entities if they were responsible for assessing these risks. The data minimisation principle has been redrafted to incorporate and address this feedback.

Changes since previous consultation

The amended rule 4.42 ensures that accredited entities that disclose personal information can provide a way for relying parties to minimise the data they require to provide their services or enable an individual to access their services.

Accredited entities will be required to support a technical capability for relying parties and other entities in a digital ID system to choose to only request some attributes and not others. This means that if a relying party only needs an individual's age to allow that individual to access the relying party's service (or just to confirm that the individual is over 18 years old to purchase alcohol online), an accredited entity must have the technical capability to be able to only disclose that information if it is available—and not, for example, any other additional information such as the individual's name or contact details. This does not mean that a digital ID provider cannot offer a bundled attribute option which contains all of those attributes if a relying party requires them, just that they must also enable relying parties to select and receive a single attribute.

Aligning with Anti-Money Laundering and Counter-Terrorism Financing requirements (rule 7.3 (item 8))

A new draft condition on Accreditation is included in the Accreditation Rules that would authorise Accredited Identity Service Providers to disclose a limited set of restricted attributes to relying parties with obligations to collect this information under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)*. The restricted attributes specified in the condition on Accreditation are: the passport number, visa number, driver licence number, Medicare card number, or proof of age card number of an individual.

This draft condition would work in tandem with the Digital ID Act requirement for that an individual to provide express for the Accredited Identity Service Provider to disclose their restricted attributes to the relying party which has AML/CTF reporting requirements.

This draft condition is part of initial work considering how the Digital ID could be leveraged by AML/CTF reporting entities. Further changes may be required to the draft condition pending the outcomes of the Attorney-General's Department's second stage of consultation on reforming Australia's AML/CTF regime to extend the existing AML/CTF legislation to certain high-risk services. High risk services include those provided by lawyers, accountants, trust and company service providers, real estate agents, and dealers in precious metals and stones.

Other matters relating to accreditation (chapter 7)

A new Chapter 7 of the Accreditation Rules has been created to capture new rules required to be made under the Digital ID Act as well as to capture sections of requirements that fall outside of the standard rules and requirements structure in chapters 2-6 (protective security, fraud, accredited service requirements etc.). Chapter 7 is set out into 4 parts, including:

- Part 7.1—Matters relating to attributes (new)
- Part 7.2—Accreditation conditions (new)
- Part 7.3—Reportable incidents (moved from chapter 4)
- Part 7.7—Data standards relating to accreditation (new)

Digital ID (Accreditation) Data Standards

Consultation feedback

The September 2023 draft Accreditation Rules identified that requirements that were of a technical nature, including standards for how a type of technology is issued, configured or tested may be removed from the rules and instead made as data standards.

Stakeholder feedback supported such transition into data standards for certain rules that were prescriptive and may need to be updated more frequently than the Accreditation Rules (e.g. to quickly address the rapidly changing risk and technology landscape) to data standards.

Changes since previous consultation – new provisions

Rules relating to authentication management and the testing of biometric technology used in biometric binding solutions, including the testing of a biometric matching algorithm, presentation attack detection technology and eIDVT solutions have been removed from the Accreditation Rules.

These are now proposed to be included in the Digital ID (Accreditation) Data Standards. The Accreditation Data Standards will offer greater flexibility for these requirements to be updated when needed and in response to changes in testing standards or development of new technology.

There have been some minor adjustments to the authentication requirements because of consultation feedback and expert advice to align with the most recent published update of the National Institute of Standards and Technology (NIST) 800-63b Authentication and Lifecycle Management standard, which is the standard on which the requirements for authentication in the Accreditation Rules are based.

Attachment A: Digital ID Rules – changes since first consultation

Table A1: Digital ID Rules - removed or reordered since September 2023 consultation

Rule (September 2023)	Changed since September 2023 draft Digital ID Rules?
10 Holding etc. information outside Australia	Removed – Data localisation rules made under s 77 of the Digital ID Act (a civil penalty provision) are not proposed for the commencement phase of the legislated Australian Government Digital ID System.
11 Interoperability obligation	Removed – Interoperability obligation rules made under s 79(3) of the Digital ID Act are not proposed for the commencement phase of the legislated Australian Government Digital ID System.
18 Capacity of the Australian Government Digital ID System	Removed – Reportable incident rules made under s 78 of the Digital ID Act (a civil penalty provision) regarding capacity of the Australian Government Digital ID System are not proposed for the commencement phase of the legislated system.
21 This Part not to affect other rights	Transferred – Contents of rule now in rule 5.1.

Table A2: Digital ID Rules - changes from September 2023 consultation

Rule	Amended since Sept 2023	Explanation
Chapter 1—Preliminary		
1.1 Name	No	
1.2 Commencement	Yes	Drafting simplified.
1.3 Authority	Yes	Drafting clarified.
1.4 Definitions	Yes	Updated to reflect other amendments; drafting simplified and clarified; new definitions (e.g., 'material change', 'material effect', 'pairwise identifier').
Chapter 2—Fit and proper person considerations		
2.1 Application of this Chapter	N/a	New application provision.
2.2 Mandatory relevant matters	Yes	Formerly rule 5; paragraph (c) amended to add new s 52(1A)(ba) of the Privacy Act; paragraph (f) amended to clarify references to external dispute resolution schemes; new paragraphs (1)(g) (whether prior application for accreditation was refused) and (j) (whether approval to participate is or has been suspended or revoked).
Chapter 3—Participation in the Australian Government Digital ID System		
Part 1—Applications for approval to participate		
3.1 Application of this Part	N/a	New application provision.
3.2 Applications for approval to participate—all entities	Yes	Formerly rule 6; process and drafting clarified.
Consultation question for Rule 3.3 – The requirements included in this rule 3.3 are based on existing requirements applicable to Government entities seeking to onboard to the Australian Government Digital ID System. They are designed to ensure that the System Administrator and the government relying parties reach an agreement prior to onboarding on how different types of incidents relating to the AGDIS are managed, so that if an incident occurs these can be resolved effectively. We are seeking feedback on how to achieve this coordinated response in future phases of the AGDIS rollout, where non-Government organisations who may not have large fraud and security teams may find these requirements difficult to meet. • How would you consider clarifying these rules for non-government organisations while still maintaining strong minimum security and fraud protections for individuals who may use their digital ID to access that relying party service?		
3.3 Applications for approval to participate—relying parties	Yes	Formerly rule 7; process and drafting clarified; requirement for continuity procedures for critical functions of its information technology system omitted
Part 2—Approval to participate		
3.4 Conditions on approval to participate	Yes	Formerly rule 8; item 1 (notification of change of contact details timeframe reduced from 28 to 7 days). New conditions: item 2 (participating relying parties to report proposed changes to IT systems and outages to the System Administrator); item 3 (participating relying parties to collect and store the pairwise identifier); item 4 (participating relying parties to notify the digital ID Regulator regarding 'reporting entity' status under AML/CTF laws); item 5 (participating relying parties may collect/disclose certain restricted attributes for the purpose of complying with AML/CTF obligations); item 6 (accredited identity service providers may

Rule	Amended since Sept 2023	Explanation
		collect/disclose certain restricted attributes for the purpose of participating relying parties to comply with their AML/CTF obligations); item 7 (IP rights warranty condition for accredited entities to complement rule 3.5).
Part 3—Statutory contract		
3.5 Intellectual property rights	Yes	Formerly rule 9; redrafted.
Chapter 4—Reportable incidents		
4.1 Application of this Chapter	N/a	New application provision.
Consultation question for rule 4.2 – This rule is based on reporting requirements that are currently used in the Australian Government Digital ID System. Do you have any suggested changes to this rule supporting the relevant regulator in accessing the necessary information to undertake investigations into cyber security or fraud incidents that could occur within the Australian Government Digital ID System?		
4.2 Cyber security incidents and digital ID fraud incidents	Yes	Formerly rules 12 and 13; incident reportable to System Administrator; former paragraph (4)(f) omitted; drafting clarified (including to refer to law enforcement agency and pairwise identifier).
4.3 Changes in control of corporations	Yes	Drafting clarified, including to replace 'proposed change' with 'future change' in control and permit Commonwealth, State and Territory governments to change control of their corporations within their government structures without notifying the Digital ID Regulator.
4.4 Change in contractor	Yes	Drafting clarified; new exception to reporting a change in contractor within 28 days before an engagement is proposed to start where it is necessary to manage a material change in circumstances (so long as the engagement and material change in circumstances are reported under rule 4.5).
4.5 Other incidents	Yes	Drafting clarified; new requirement for accredited entities to report proposed changes to IT systems and outages to the System Administrator.
4.6 Other digital ID systems	Yes	Drafting clarified; paragraph 3(g) amended to require information held by the entity for the purposes of the Australian Government Digital ID System to be located and distinguished from other digital ID system information.
4.7 System Administrator may disclose information	Yes	Formerly rule 19; redrafted consistent with other amendments including change from Digital ID Regulator to System Administrator; notes inserted to clarify Digital ID Regulator and System Administrator functions are not limited.
Chapter 5—Trustmarks		
5.1 Application of this Chapter	N/a	New application provision.
5.2 Digital ID trustmark	Yes	Drafting simplified and clarified.
5.3 Conditions in relation to use or display of digital ID trustmark	N/a	New rule prescribing conditions in relation to use or display of digital ID trustmark.

Rule	Amended since Sept 2023	Explanation
Chapter 6—Record-keeping		
Consultation question for rule 6.2 – The record keeping provisions required for the logging of information in relation to Australian Government Digital ID System transactions and other system information required by rule 6.2 in the proposed Digital ID Rules has been amended to 6 years. This is different from the proposed Accreditation Rules requirement for logging the same information under rule 4.20. Rule 4.20 in the proposed Accreditation Rules maintains that logs required that rule are required to be kept for 3 years. • Is 6 years an appropriate timeframe to retain the logging and transaction information required by rule 6.2 in the proposed Digital ID Rules in relation to transactions and personal information on the Australian Government Digital ID System? • What do you consider an appropriate minimum timeframe for the retention of this type of information? **Note:** other kinds of personal information such as an individual's name or restricted attributes collected for the purpose of a Digital ID are not required to be kept under the logging requirements in rule 4.20 of the proposed Accreditation Rules.		
6.1 Application of this Chapter	N/a	New application provision.
6.2 Record keeping requirements for accredited entities	Yes	Formerly rule 22; drafting simplified; record-keeping requirement standardised from 7/3 years to 6 years; additional requirement to not destroy/de-identify personal information in specified circumstances.
Chapter 7—Interim liability arrangements		
Consultation question for Chapter 7 – The interim liability arrangements in Chapter 7 are prescribed for the initial phases of the Australian Government Digital ID System, where participants are Australian or state and territory government entities. The liability arrangements in the proposed Digital ID Rules will be reviewed prior to the expansion of the Australian Government Digital ID System to the private sector. • What kinds of liability arrangements would your organisation expect to see operational on Australian Government Digital ID System? • Are there any existing liability frameworks that the Digital ID Rules could draw from?		
7.1 Simplified outline of this Chapter	N/a	New outline provision confirming interim liability arrangements for commencement phase of the legislated Australian Government Digital ID System.
7.2 Breaches of the statutory contract	N/a	New interim rule prescribing conduct that does not, and circumstances that do not, constitute a breach of the statutory contract.
7.3 Limits on the kinds of losses or damages and amount of compensation	N/a	New interim rule limiting kinds of losses or damages, and limiting amount of compensation, in relation to non-compliance with the statutory contract.

Attachment B: Accreditation Rules changes since first consultation

Table B1: Accreditation Rules - removed since September 2023 consultation

Rule (draft September 2023 Accreditation Rules)	Reason
2.2 Information and documents to accompany an application	Removed – This will be incorporated into the Application for accreditation form which will be developed and managed by the Digital ID Regulator. (See note below.)
5.23 Source biometric matching	Removed – This is no longer required as the obligations set out by the rule were superfluous given the definitions of authoritative source, source verification and source biometric matching. The Identity Verification Services Act 2023 (IVS Act) also sets out requirements for the FVS, which may be used for source biometric matching.
5.84 Annual Transparency Report	Removed - Requirement redundant due to provisions in the Digital ID Bill 2024. See Section 155A of the Digital ID Act.
5.80 Reauthentication	Changed – This requirement has been incorporated into item 2 of **Section 2.1 Authentication levels: AL Table** of the Accreditation Data Standards. Superfluous requirements were removed to align with the NIST 800-63b framework.

Note on removed Rule 2.2 Information and documents to accompany an application

The ACCC, as the Digital ID Regulator, will set an approved application form that will be required for accreditation applications. The approved form will require information and documentation to be provided in support of an application. The information and documentation required in the approved form will likely be based off the previous version of rule 2.2, as well as the requirements set out in the Accreditation Rules and Accreditation Data Standards. Where an accredited entity or relying party joins the Australian Government Digital ID System, they will be asked to apply using an approved application form for that purpose.

The ACCC anticipates publishing the form and associated guidance prior to commencement of its role as the Digital ID Regulator. A preliminary indication of the types of documents likely to be required by the application form for accreditation is included below. However, this is subject to change, including due to any changes in the Accreditation Rules and Accreditation Data Standards. Applicants are encouraged to review the ACCC's application form and guidance prior to preparation of materials to support an accreditation application, once that material is made available.

Indicative list of documents (noting not all documents may be required depending on the scope of accreditation being sought):

- Description of DI data environment
- Statement of Scope and Applicability
- Assurance Assessments and applicant's response to each assessment
- Privacy Impact Assessment
- Penetration test report
- Usability testing report
- WCAG testing report
- Cyber Security Risk Assessment
- Fraud risk assessment
- Fraud control plan
- Data Breach Response Plan
- System Security Plan
- Privacy Management Plan
- Privacy Policy Business Continuity Plan
- Cloud Services Management Plan
- Journey Map
- Biometric information testing plan and processes
- Presentation Attack Detection Testing Report
- Alternative Proofing Proposal and processes
- System design documents for accredited services
- Authenticator use and maintenance materials

Table B2: Accreditation Rules - changes from September 2023 consultation

Rule	Amended since Sept 2023	Explanation
General questions – Accreditation Rules and data retention periods for personal information: Retention of personal information collected from an individual is managed through an accredited entity's own policies and requirements of its services as well as its tolerance for security and fraud risks associated with the retention of that information (e.g. the longer it is retained, the more at risk that information may be of being breached). • Should the Accreditation Rules set out a maximum data retention period for an individual's personal information? For example, that an accredited entity must delete personal information after a period of time if an account becomes dormant. What should that period of time be?		
General questions – Accreditation Rules and barriers to entry for the accreditation scheme: The Accreditation Rules are a set of minimum controls that are designed to address Digital ID specific risks to individuals and relying parties. Some previous feedback has indicated that because of the technical nature and complexity of the Accreditation Rules and Accreditation Data Standards, that there is a high cost of entry to the accreditation scheme due to the kinds of controls accredited entities are expected to implement. • If the Accreditation Rules were to be simplified, which rules would you suggest be removed? o If you are suggesting removal of a rule, how would you recommend mitigating the risk that rule was designed to address? • Are there any other standards that are not already incorporated into the rules that you suggest should be considered?		
Chapter 1—Preliminary		
1.1 Name	No	
1.2 Commencement	No	
1.3 Authority	No	
1.4 Definitions	Yes	Clarification of various definitions.
1.5 Incorporated instruments	Yes	Addition of (b) to ensure that legislative instruments such as the Accreditation Data Standards are not captured by this requirement.
1.6 Taking reasonable steps	No	
Chapter 2—Applying for accreditation		
2.1 DI data environment	Yes	Minor clarifications to ensure that references to contracted service providers are consistent.
2.2 Documents to accompany application	Yes	New – This requirement is to support annual review requirements for the documents mentioned in the rule. All other documentation required for accreditation will be set out in the application for accreditation form required under section 141 of the Digital ID Bill.
2.3 Criteria to be met	No	
2.4 Privacy impact assessment	Yes	Minor clarification to capture Chapter 5 rules as part of the PIA.
2.5 Technical Testing	Yes	Addition of data minimisation mechanism to be tested (see rule 4.42 (2)).
2.6 Matters to which the Digital ID Regulator must have regard	No	
2.7 Matters to which the Digital ID Regulator must be satisfied	No	

Rule	Amended since Sept 2023	Explanation
Chapter 3—Assurance assessments and systems testing		
Part 3.1—General		
3.1 Entity's obligation	No	No
3.2 Assessors	No	No
Part 3.2—Assurance assessments		
Division 1—Protective security assessment		
3.3 Requirements	Yes	Minor drafting clarifications
3.4 Essential strategies review and report	No	
3.5 Where a control is not relevant to an entity	Yes	Minor drafting clarifications
Division 2—Fraud assessment		
3.6 Requirement	No	
Division 3—Accessibility and useability assessment		
3.7 Requirements	No	
Part 3.3—Systems testing		
Division 1—Penetration testing		
Consultation Question for Rule 3.8 – The penetration testing rule has been updated to better clarify the scope and requirements of a penetration test, including what is required to be tested and what kind of testing must be included in a penetration test. Do you have any feedback regarding this requirement?		
3.8 Penetration testing requirements	Yes	Requirements have been added to better clarify what the scope of the penetration testing must include as well as what the penetration testing applies to in the accredited entity's information technology system. New requirements to clarify penetration testing requirements where an accredited entity uses a cloud service provider.
3.9 Penetration testing assessor	No	
3.10 Penetration testing report	No	
Division 2—Useability testing		
3.11 Accessible and inclusive services	Yes	Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules.
3.12 Useability testing requirements	Yes	Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules.
3.13 Useability testing report	No	
Division 3—WCAG testing		
3.14 Accessible and inclusive services	Yes	Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules.
3.15 WCAG testing requirements	Yes	Minor drafting clarification to align with section 30 of the Digital ID Bill and rules that were updated in Part 4.4 in the Accreditation Rules.
3.16 WCAG testing report	No	

Rule	Amended since Sept 2023	Explanation
Part 3.4—Reports		
3.17 Assessor's report	No	
3.18 Entity's response to an assessor's report	No	
Chapter 4—Requirements for maintaining accreditation		
Part 4.1—Protective security controls		
Division 1—Capability		
4.1 Protective security capability	No	
Division 2—Protective security frameworks		
4.2 Accredited entities must implement a security framework	Yes	Minor drafting clarification to address structure and clarity of interpretation
4.3 Compliance with the PSPF	Yes	Minor drafting clarification to address structure and clarity of interpretation
4.4 Compliance with ISO/IEC 27001	Yes	Minor drafting clarification to address structure and clarity of interpretation
4.5 Implementation and compliance with an alternative framework	Yes	Minor drafting clarification. Guide note: this rule is in the wrong place and will be moved to Division 2 (above) prior to public consultation.
4.6 Where a control is not relevant to an entity	Yes	Minor drafting clarification to address structure and clarity of interpretation
Division 3—Additional protective security controls		
4.7 Cyber security risk assessment	No	
4.8 Sharing information about risks	No	
4.9 Eligibility and suitability of personnel	No	
4.10 Advice to individuals	Yes	Requirement changed to implement consultation feedback. Adopted the use of "serious harm" to align with Privacy Act and OAIC advice wording and requirement now ensures that entities must "promptly" inform individuals of the risk or incident.
4.11 Support to individuals	No	
Subdivision 1—System security plan		
4.12 Requirement	Yes	Now includes security goals and strategic objectives and addition of requirements for entities to record their biometric information destruction process (TDIF requirements that were not in the September 2023 draft Accreditation Rules).
4.13 Review of the system security plan	Yes	Now includes review of security goals and strategic objectives.
Subdivision 2—Cloud service management		
4.14 Selection, use and management of cloud services	No	
Subdivision 3—Incident detection, investigation, response and reporting		
4.15 Incident monitoring and detection	No	
4.16 Incident investigation, management and response	No	

Rule	Amended since Sept 2023	Explanation
4.17 Disaster recovery and business continuity management	No	
4.18 Record keeping	Yes	Minor adjustments to improve clarity.
Subdivision 4—Information technology system controls		
4.19 Essential Eight	No	
4.20 Logging requirements	Yes	Minor adjustments to improve clarity. Requirements for logging consent explicitly included (previous TDIF requirement that was not in the September 2023 draft Accreditation Rules).
4.21 Cryptography	No	
4.22 Cryptographic standards	No	
4.23 Cryptographic key management processes and procedures	No	
Part 4.2—Fraud control requirements		
Division 1—Capability		
4.24 Fraud management capability	No	
Division 2—Fraud controls		
4.25 Fraud risk assessment	No	
4.26 Sharing information about risks	No	
4.27 Fraud controller	No	
4.28 Fraud awareness training	No	
4.29 Advice to individuals	Yes	Requirement adjusted to address consultation feedback. Adopted the use of "serious harm" to align with Privacy Act and OAIC advice wording and requirement now ensures that entities must "promptly" inform individuals of the risk or incident.
4.30 Support to individuals	No	
Division 3—Fraud control plan		
4.31 Fraud control plan	Yes	Minor adjustments to improve clarity
4.32 Review of entity's fraud control plan	No	
Division 4—Incident detection, investigation, response and reporting		
4.33 Incident monitoring and detection	No	
4.34 Incident investigation, management and response	No	
4.35 Record keeping	No	
Part 4.3—Privacy		
4.36 Privacy governance code	No	
4.37 Compliance with privacy governance code	No	
4.38 Privacy policy	No	
4.39 Review	No	
4.40 Providing information about express consent	Yes	Requirement included to address feedback about the intersection of privacy and usability. This requirement

Rule	Amended since Sept 2023	Explanation
		was previously a TDIF requirement that was not in the draft September 2023 Accreditation Rules
Consultation question for Rule 4.41 – Some feedback has indicated that the rules should not set a timeframe for enduring consent to expire and instead allow accredited entities to set their own policies for the expiry of enduring consent dependent on the service that is being provided. Do you think the rules should set a timeframe for enduring consent to expire? What should that timeframe be?		
4.41 Enduring consent	Yes	New. Added to address consultation feedback noting the gap in assurance about the timing and duration of consent. Wording and policy for the duration period aligns with similar CDR provisions. Supporting requirements for enduring consent related to usability and accessibility have been added. These requirements were previously in the TDIF but were not in the draft September 2023 Accreditation Rules
4.42 Data minimisation principle	Yes	Major change. Consultation feedback indicated the data minimisation principle was overly burdensome in regulating what kind of data relying parties required. The requirement has been amended to now ensure accredited entities can allow relying parties to select only the information they require to offer their services (e.g., a surname only instead of a bundle of first name, middle name, and surname).
4.43 Use of DVS and FVS for providing accredited services	Yes	New. Included to ensure alignment and legality of use of the DVS and FVS.
4.44 Disclosure of personal information for fraud activities	No	
4.45 Privacy awareness training	No	
4.46 Data breach response plan	No	
4.47 Record keeping	No	
Part 4.4—Accessible and inclusive accredited services		
4.48 Application	Yes	Aligned with Digital ID Act provisions.
4.49 Reporting on accessibility	Yes	New. Requirement added to ensure alignment with section 30 of the Digital ID Act and address consultation feedback encouraging the use of inclusion strategies and goals for accredited entities.
4.50 Accessibility requirements	Yes	Requirement wording has been adjusted to ensure alignment with section 30 of the Digital ID Act.
4.51 Journey map	Yes	Minor clarifications to address consultation feedback and to fold the journey map into the usability testing rules to better scope usability testing.
Part 4.5—Retention and use of biometric information for testing and fraud activities		
4.52 Requirements where biometric information is used for testing activities	Yes	Changes made to align with Section 49 (6A) and (7) of the Digital ID Act and to address consultation feedback. Additionally, changes to testing requirements include that accredited entities must only carry out testing of biometric information where the testing is unable to be conducted effectively by processing synthetic or anonymised data rather than by using biometric information of an individual. This

Rule	Amended since Sept 2023	Explanation
		aligns to international best-practice standards and requirements when using biometric information for secondary purposes.
4.53 Requirements where biometric information is used for fraud activities	No	
Part 4.6—Review of DI data environment and statement of scope and applicability		
4.54 DI data environment	Yes	New – requirement added to support the structure of the Accreditation Rules and annual review requirements for these documents in Chapter 6.
4.55 Statement of scope and applicability	Yes	New – requirement added to support the structure of the Accreditation Rules annual review requirements for these documents in Chapter 6.
Part 4.6—Review of DI data environment and statement of scope and applicability		
Chapter 5—Requirements when providing accredited services		
Part 5.1—Preliminary		
5.1 Definitions	Yes	Majority of definitions moved to Chapter 1 of the Rules or into the Accreditation Data Standards where appropriate
Part 5.2—Accredited identity service providers		
Division 1—Generating, managing, maintaining or verifying a digital ID		
5.2 General requirements	Yes	Yes. The rule has been rewritten for clarity and scope of ISP services to address consultation feedback.
5.3 Digital IDs and children	Yes	The age an individual can get a digital ID will remain at 15 years old to align with OAIC guidance regarding the age that individuals have the capacity to give express consent. Additionally, a new subrule was added to address IP1 services that cannot effectively verify an individual's age because an individual is not required to present any documents for verification at IP1.
5.4 One-off digital IDs	No	
5.5 Expiry of a reusable digital ID	Yes	Amended for clarity.
5.6 Step-up of an identity proofing level	Yes	Amended for clarity.
5.7 Updating and correcting attributes	Yes	Amended for clarity.
5.8 Suspension of a digital ID	Yes	Amended for clarity.
5.9 Digital IDs affected by a fraud or cyber security incident	Yes	Amended for clarity.
5.10 Reactivating a suspended digital ID	Yes	Amended for clarity.
Division 2—Identity proofing and verification of credentials		
Subdivision A—Identity proofing		
5.11 IP Levels Table	Yes	Amended for clarity.

Rule	Amended since Sept 2023	Explanation
5.12 Verification using an Australian passport or Australian ePassport	Yes	Amended for clarity.
5.13 Technical verification of credentials	Yes	This requirement has been amended to be scoped only to ePassport verification. This is because ePassports have a clear standard and way to be verified using Public Key Infrastructure technology and issued by the Internation Civil Aviation Organization (ICAO). As new standards and issuance processes for other kinds of credentials emerge, this rule will be updated.
5.14 Source verification using a government credential	Yes	Minor amendments and drafting clarification.
5.15 Visual verification	Yes	Minor amendments and drafting clarification to align with feedback and amendments made to Schedules 1-4.
Subdivision B—Verification using biometric information		
5.16 Application	No	
5.17 Requirements for biometric binding	No	
5.18 Requirements for online biometric binding	Yes	Minor drafting clarification.
5.19 Requirements for local biometric binding	Yes	Minor clarification to address consultation feedback.
5.20 Requirements for technical biometric matching	No	
5.21 eIDVT biometric matching	Yes	Moved some requirements from the previous eIDVT testing rules to here as they structurally belonged in this section. The eIDVT testing requirements are now located in the Accreditation Data Standards.
5.22 Requirements for manual face comparison	No	
Subdivision C—Alternative proofing processes		
5.23 Accessible and inclusive services	No	
5.24 Exceptional use case	No	
5.25 Requirements for an alternative proofing process	Yes	Minor drafting clarification.
Division 3—Generating, binding, managing or distributing authenticators		
5.26 General requirements	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.
5.27 Physical authenticators	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.
5.28 Authenticator that has been compromised	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.
5.29 Step-up of an authentication level	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.

Rule	Amended since Sept 2023	Explanation
5.30 Expired and renewed authenticators	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.
5.31 Revocation and termination of an authenticator	Yes	Amended for clarity. Note that any other requirements related to authenticators are located in the Accreditation Data Standards.
Division 4—Accessibility and useability		
5.32 Application	No	
5.33 Verification services	No	
5.34 Authentication services	No	
Part 5.4—Accredited attribute service providers		
5.35 Verifying and managing a special attribute	Yes	Amended to address consultation feedback and Digital ID policy about the scope of an ASP service.
5.36 Requirements when verifying a special attribute	Yes	Amended to address consultation feedback and Digital ID policy about the scope of an ASP service.
5.37 Special attributes that are self-asserted	Yes	Amended to address consultation feedback and Digital ID policy about the scope of an ASP service.
5.38 Special attributes affected by a fraud or cyber security incident	Yes	Amended to address consultation feedback and Digital ID policy about the scope of an ASP service.
Chapter 6—Annual reviews		
Part 6.1— Accredited entities to conduct annual reviews		
6.1 General requirements	Yes	Minor amendment to address consultation feedback by allowing entities an additional month past the anniversary of their accreditation date to submit their annual review report and supporting evidence.
6.2 Reporting periods for transitioned accredited entities	Yes	New. Required for entities transitioning their accreditation from TDIF to the legislation. This table will completed post-consultation.
6.3 Reporting periods for other accredited entities	Yes	New. Required for entities that will be accredited under the legislation.
6.4 Scope of annual review	Yes	Minor clarifications to include notes about the privacy impact assessment (PIA) and other drafting clarifications.
6.5 Assurance assessments	No	
6.6 Penetration and presentation attack detection testing	No	
Part 6.2— Accredited entities to provide annual reports		
6.7 Content of report	No	
6.8 Where previous timeframes to address risks and recommendations not met	Yes	Minor clarification to include PIA in this rule.
6.9 Information and documents	No	
6.10 Attestation statement	No	

Rule	Amended since Sept 2023	Explanation
Chapter 7—Other matters relating to accreditation		
Part 7.1—Matters related to attributes		
7.1 Individuals must expressly consent to disclosure of certain attributes of individuals to relying parties	Yes	New. Requirement included to ensure accredited entities collect express consent for attributes that are not covered in section 45 of the Digital ID Act.
7.2 Meaning of *restricted attribute* of an individual	Yes	New. Requirement included ensure that card numbers are included as a restricted attribute.
Part 7.2—Accreditation conditions		
7.3 Table of accreditation conditions	Yes	New. Included to align with Digital ID Act requirements for accreditation of entities.
Part 7.3—Reportable incidents		
7.4 General	No	
7.5 Reportable incidents	No	
7.6 Change of control for corporations	No	
7.7 Entity no longer providing accredited services	Yes	New requirement to address gap in reporting information to the Regulator.
Part 7.4—Data standards relating to accreditation		
7.8 Digital ID Data Standards Chair to make standards	Yes	New. Included to accommodate the Accreditation Data Standards (see below).
Schedules		
Schedule 1— Documents or other credentials that are a commencement of identity credential	Yes	Minor changes to support changes to verification rules and supporting requirements.
Schedule 2—Documents or other credentials that are a linking credential	Yes	Minor changes to support changes to verification rules and supporting requirements.
Schedule 3—Documents or other credentials that are a UitC credential	Yes	Minor changes to support changes to verification rules and supporting requirements.
Schedule 4—Documents or other credentials that are a photo ID	Yes	Minor changes to support changes to verification rules and supporting requirements.
Schedule 5—PSPF controls	No	This schedule will be consolidated with any updates of the PSPF published prior to commencement.

Table B3: Accreditation Data Standards - changes from September 2023 consultation

Standard	Amended since Sept 2023?	Explanation
Chapter 1 —Preliminary		
1 Name	NA	
2 Commencement	NA	
3 Authority	NA	
4 Schedules	NA	
5 Definitions	Yes	Clarification of various definitions to align with the Accreditation Rules
Schedule 1—Data standards for accredited identity service providers		
Part 1—Biometric testing		
1.1 Definitions	Yes	Minor clarifications
1.2 Biometric testing entity	Yes	Minor clarification to rule 1.2(1)(b) to ensure that the laboratory certified by ISO/IEC 17025 includes that the certification is for the assessment of biometric technology testing standards.
1.3 Testing of presentation attack detection technology	Yes	Minor clarifications to allow an accredited entity to have a minor failure in the PAD testing (as opposed to meeting a 0% failure rate) and address that failure through implementing a treatment or recommendation.
1.4 ISP's response to testing report	Yes	New. Added to support changes to section 1.3 and address feedback related to PAD testing metrics and outcomes for rule 5.28 (7) in draft September 2023 Accreditation Rules
1.5 Testing of biometric matching algorithm for technical biometric matching	No	
1.6 Testing of source biometric matching	Yes	Minor drafting clarifications
1.7 Testing of eIDVT	Yes	Some rules were moved from the testing section to the eIDVT rules in the Accreditation Rules as they related to configuration settings and requirements for eIDVT rather than testing requirements.
Part 2—Authenticating to a digital ID		
Division 1—Authentication levels		
2.1 Authentication levels: AL Table	Yes	Minor drafting clarifications for table readability. Amendments to item 2 Reauthentication requirements have been made for readability and alignment with NIST 800-63b.
Division 2—Binding authenticators to a digital ID		
2.2 Binding an authenticator when generating a digital ID	No	
Division 3—Standards for kinds of authenticators		
2.3 Memorised secrets	Yes	Minor drafting clarifications
2.4 Look-up secrets	Yes	Minor drafting clarifications
2.5 Single-factor one-time password devices	Yes	Minor drafting clarifications
2.6 Multi-factor one-time password devices	Yes	Minor drafting clarifications

Standard	Amended since Sept 2023?	Explanation
2.7 Single-factor cryptographic software	Yes	Minor drafting clarifications
2.8 Multi-factor cryptographic software	Yes	Minor drafting clarifications
2.9 Multi-factor cryptographic devices	Yes	Minor drafting clarifications
2.10 Single-factor cryptographic devices	Yes	Minor drafting clarifications
2.11 Out-of-band devices	Yes	Additional requirements added for out-of-band devices that use the PSTN to address security concerns. These requirements align to the NIST 800-63b framework.
Division 4—Standards for security requirements		
2.12 Standards for security requirements	No	
Division 5—Authentication using biometric information		
2.13 Standards for authentication using biometric information	Yes	Changes made to in-device biometric capability requirements—requirement to record in-device capability risks in the fraud control plan have been moved to the fraud control plan rules in the Accreditation Rules (see rule 4.31)