Australian Government

Australia's Digital ID System

Your Guide to the Digital ID (AGDIS) Data Standards

July 2024 Public Consultation

Department of Finance

Contents

Introduction

Digital ID Act 2024

The Digital ID Act 2024 (**the Act**) and the *Digital ID (Transitional and Consequential Provisions) Act 2024* (**Transitional Act**) were passed on 16 May 2024 and received Royal Assent on 30 May 2024. The Acts are expected to commence on 1 December 2024.

This legislation authorises a package of multiple legislative instruments which set out additional details of the Accreditation Scheme and the Australian Government Digital ID System (AGDIS), the two main components of Australia's Digital ID System. As the primary legislation for the Accreditation Scheme and the Australian Government Digital ID System, the Act allows for legislative rules and data standards to be made.

Following earlier consultation on some of these rules and data standards, this public consultation focuses on:

- The draft Digital ID (AGDIS) Data Standards 2024 (**AGDIS Data Standards**).

Using this Guide

This guide is not intended to be an exhaustive description of the content of the proposed draft AGDIS Data 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 legislative instrument.

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

Consultations to date

The AGDIS Data Standards were developed through extensive consultation with the community and industry over several years on the Trusted Digital Identity Framework (TDIF), which was the basis for the unlegislated AGDIS that has been in operation since 2019. The AGDIS Data Standards draw heavily upon international standards, and build off the following Chapters of the TDIF:

- 06 (Federation Onboarding Requirements),
- 6A (Federation Onboarding guidance),
- 6B (OpenID Connect 1.0 Profile) and
- 6D (Attribute Profile)

Consultation purpose

The Government is seeking your feedback on the AGDIS Data Standards. The AGDIS Data Standards set out the technical requirements entities need to comply with to be approved to participate in the Australian Government Digital ID System (AGDIS).

The AGDIS Data Standards are intended to maintain the technical arrangements for entities onboarded to the unlegislated AGDIS in the legislated AGDIS. The AGDIS Data Standards are drafted on the premise that the Transitional Act or its Rules will facilitate the entities currently accredited and/or onboarded to the unlegislated AGDIS to participate in the legislated AGDIS.

Schedules in the Data Standards define requirements for accredited Attribute Service Providers, Identity Service Providers and Identity Exchange Providers seeking to participate in the AGDIS and guidance for Relying Parties seeking to participate in the AGDIS.

The AGDIS Data Standards have changed from the TDIF in three main ways, namely:

- including legal information to meet requirements of the *Legislation Act 2003*,
- introducing identity proofing level data minimisation for attribute requests, and
- a change to the technical approach to prevent user profiling (known as 'blinding')

We would value your feedback on these changes.

Providing feedback

Your views will help refine the legislative instrument. If you wish to provide a submission, please read through this guide and the information included in the feedback form to support your feedback.

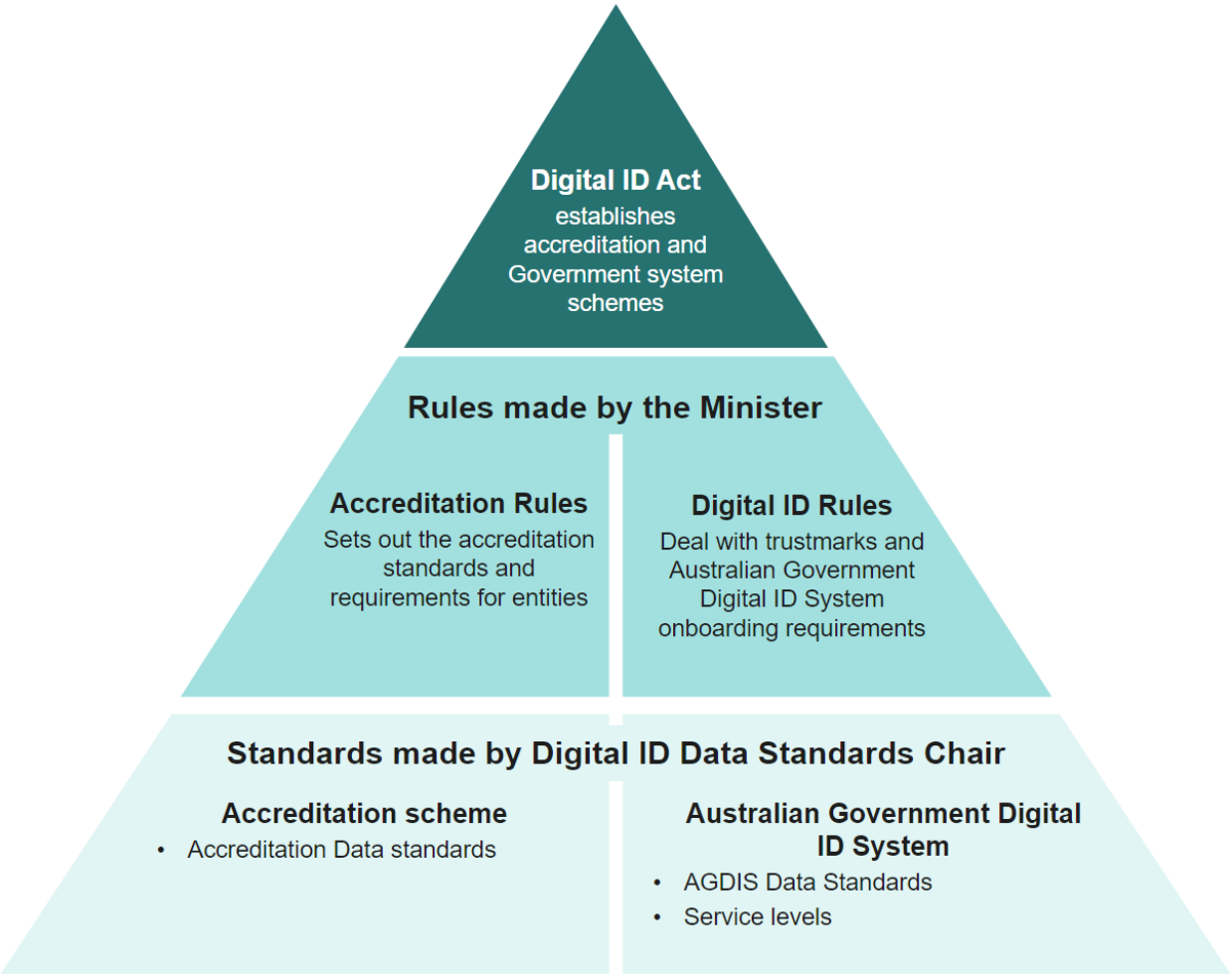
An optional feedback template is available for your use and can be downloaded from the Digital ID website.

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

Consultation timeline

Step	Estimated Timeframe
This public consultation closes	5:00pm 5 August 2024 AEST
Engagement on transitional arrangements with Accredited Entities, Relying Parties involved in the unlegislated AGDIS	Ongoing
Digital ID Act 2024, all rules and data standards commence	Expected 1 December 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 Act

The Act establishes the accreditation scheme, AGDIS, additional privacy and other safeguards, and governance arrangements including a Digital ID Regulator, expanded role for Information Commissioner, AGDIS System Administrator and Data Standards Chair who will have responsibility for maintaining these standards.

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 AGDIS. 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 AGDIS expands enabling state and territory governments and private sector participation, additional rules will be added supporting this phased expansion.

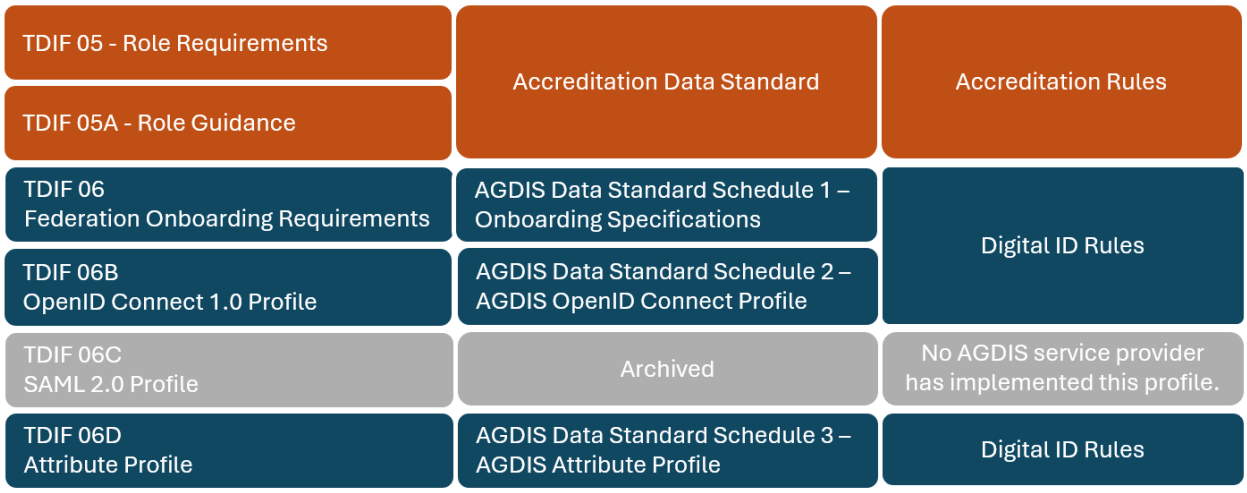
Digital ID (Accreditation) Rules

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.

Digital ID (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.

The diagram below shows how the TDIF documents have informed the Accreditation Data Standards and Accreditation Rules



Digital ID (AGDIS) Data Standards (this is the instrument this consultation process seeks feedback on)

The AGDIS Data Standards work with the Digital ID Rules to govern the AGDIS. The AGDIS Data Standards set out various technical requirements and processes, to ensure for example there are appropriate levels of security protecting the AGDIS. The AGDIS Data Standards are a non-disallowable legislative instrument.

The Digital ID Data Standards draw heavily upon international standards, and build off the Trusted Digital Identity Framework (TDIF) – specifically:

- 06 – Federation Onboarding Requirements
- 06A – Federation Onboarding Guidance
- 06B – OpenID Connect 1.0 Profile
- 06D – Attribute Profile.

As a legislative instrument, the AGDIS Data Standards include standard provisions necessary for legal interpretation, such as cross references to definitions used in the Digital ID Act, the Rules, and the Accreditation Data Standards. The AGDIS Data Standards set out the meaning and effect of technical terms used in documents published by the Internet Engineering Taskforce RFC 2119 (for example MAY, MUST, RECOMMENDED, OPTIONAL, REQUIRED). The AGDIS Data Standards refer to information in other international standards as in force as at the date the Data Standards are made.

The Data Standards then sets out technical requirements in 3 Schedules:

- Schedule 1 – AGDIS Onboarding Specifications.
- Schedule 2 – AGDIS Open ID Connect Profile.
- Schedule 3 – AGDIS Attribute Profile.

Further detail about these schedules, and specific questions we seek your views on, are outlined below.

Making of standards

Until a Data Standards Chair is appointed, the Minister for Finance is the Data Standards Chair (see section 9 of the Digital ID Act). Before commencement of the Digital ID Act, the Minister may make Data Standards. If made, the AGDIS Data Standards are expected to commence at the same time as the Digital ID Act and its Rules.

Schedule 1 – AGDIS Onboarding Specifications

- Introduction to the Specifications.
- Mapping of definitions
- Reading guide/applicability

Introduction

The AGDIS Onboarding Specification outlines the requirements and obligations that Accredited Participants must meet to be approved to participate in the AGDIS. Relying parties seeking to participate in the AGDIS should use this specification as guidance when preparing their services to join the AGDIS.

Drafting of the AGDIS Data Standards has been informed by the Act, the retired TDIF 06 Federation Onboarding Requirements (release 4.8), and feedback gathered from AGDIS participants.

Terminology

The term 'general purpose identifiers' (section 1.2 of Schedule 1) is included to allow Accredited Identity service providers participating in the AGDIS to use additional types of unique identities in the way permitted by section 47(6) of the Act.

The unlegislated AGDIS included a 'double blind' model. A technical feature of the Identity Exchange, the double blind was implemented to limit information sharing within the Government System, in addition to the other privacy safeguards set out in the TDIF. Under the double blind model, the Identity Exchange:

- does not disclose to Identity Service Providers which relying party services its users are accessing in the AGDIS; and
- does not disclose to relying parties which Identity Service Provider a person has used to access one of their services.

The AGDIS Data Standards set out a 'single blind' approach. Continuing to meet the policy intent to protect user privacy, under this approach the Exchange would continue to conceal from Identity Services providers which relying party services users are accessing. This retains the technical barrier to the tracking and profiling of user behaviour across the System and is in addition to the now-legislated stringent privacy protections with civil penalties for non-compliance that are implemented by the Act – including a prohibition on data profiling.

By contrast, the second 'side' of the blind, where the Exchange cannot disclose a user's choice of Identity Service Provider to relying parties, has negative impacts that are outweighing the benefits, impeding a range of improvements to the AGDIS that would allow more users to realise the security and privacy benefits of Digital ID. For example, moving to a single blind approach can support improvements to user experience, such as simplifying the process for logging in to a relying party service with a Digital ID. It can also support improved fraud detection, as information about a person's choice of identity provider is information that relying parties can use to better assess the risk of fraud. Stakeholders have also told us that in a future scenario where multiple Identity Service Providers are participating in the AGDIS, access

to this would remove one of the barriers currently preventing them from using Digital IDs within the AGDIS to meet their ‘know your customer’ obligations such as those set out in the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) framework.

A set for requirements for the ’single blind’ has been provided for comment in section 2.2.1 of Schedule 1. There are different ways in a single blind could be implemented. The approach articulated in section 2.2.1.4, Table 30, section 4.4.1.4, and section 4.8.5.3 of Schedule 3 would permit the Accredited Identity Exchange to disclose an individual’s choice of IDP to any Participating Relying Party. Consistent with the intent of data minimisation, a requirement could specify that this information could only be disclosed when requested by a Participating Relying Party – so that where this information is not requested, the ‘double blind’ would remain in place for that Participating Relying Party. There may be other ways to implement a single blind approach, and feedback is sought on the best way to achieve the policy intent.

For Attribute Service Providers the Data Standards introduce a concept of a *Channel* to describe methods an Attribute Service Provider, participating in the AGDIS, may provide to make the special attributes it manages available to Participating Relying Parties. This term was not previously used in the TDIF and is not defined in the Digital ID Act. Details for the definition can be found in section 4.1.2.

Audience

Participating relying parties should use this document along with the AGDIS Open ID Connect profile, and the AGDIS Attribute Profile as guidance to determine their technical obligations when onboarding to the AGDIS. The Identity Exchange Relying Party profile also includes requirements for PRPs.

Accredited participants should treat these data standards as **requirements**, in addition to their obligations outlined in the Digital ID Act and the accreditation rules and data standards.

Schedule 2 – AGDIS OpenID Connect Profile

Introduction

The AGDIS OpenID Connect profile outlines the federation protocol specifications that must be met by AGDIS participants that use the Open ID connect protocol. The OpenID Connect profile is relevant for both accredited and non-accredited entities participating or seeking to participate in the AGDIS.

Drafting of the AGDIS Data Standards has been informed by the Digital ID Act, the retired TDIF 06B OpenID Connect Profile (release 4.8), and feedback gathered from AGDIS participants.

Terminology

The OIDC profile schedule introduces the concept of a Technical Relying Party's (TRPs) to distinguish from the definition of 'relying party' in the Digital ID Act. 'Technical Relying Party' is intended to capture the roles and responsibilities of a relying party in the context of the OIDC Protocol.

The following diagram illustrates the context in which a TRP fits withing the realm of the AGDIS and the AGDIS Data Standards, in contrast to how the term relying party is more common used in federated identity systems.

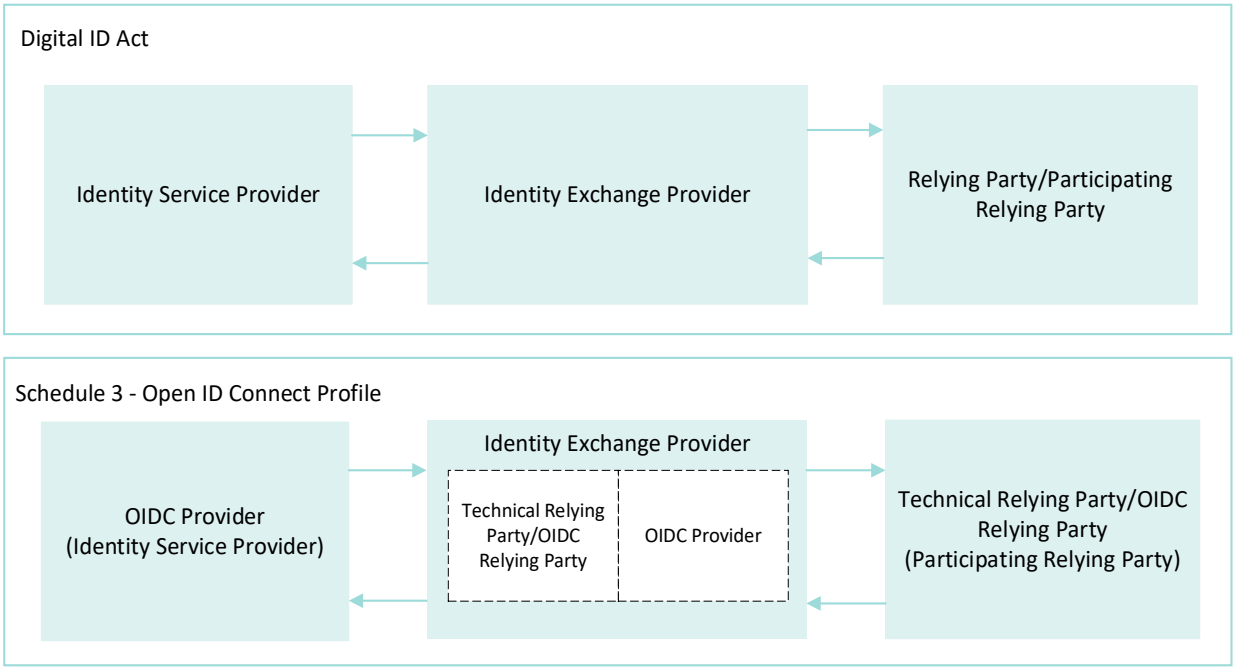


Figure 1 – TRP Context Diagram

Audience

Participating relying parties should use this document along with the AGDIS Onboarding Specification, and the AGDIS Attribute Profile as **guidance** to determine OIDC obligations for onboarding to the AGDIS.

The Identity Service Provider (ISP) profiles outline the specifications an ISP must implement as an OpenID Connect provider for connectivity to an IXP that implements this profile.

An Attribute Service Provider should implement relevant elements of this profile to ensure it can operate effectively as an AGDIS participating relying party.

Accredited Participants should treat these data standards as **requirements**, in addition to their obligations outlined in the Digital ID Act and the accreditation rules and data standards.

Schedule 3 – AGDIS Attribute Profile

Introduction

The AGDIS Attribute Profile outlines requirements and definitions for the available attributes and attribute set on the AGIDS. The profile outlines role-based requirements for the handling and fulfillment of attribute requests, along with normative definitions mapping AGDIS attributes and system metadata to the OpenID Connect profile.

The Attribute profile is relevant to both accredited and non-accredited entities seeking to participate or presently participating in the AGDIS.

Drafting of the AGDIS Data Standards has been informed by the Digital ID Act, the retired TDIF 06D Attribute (release 4.8), and feedback gathered from AGDIS participants.

Terminology

The AGDIS Attribute Profile retains terminology from TDIF 06D. However, it does formalise definitions for attribute sharing policies, consent types, fulfillment requirements, and detailed data representation.

Attribute requirements are now assigned specifically to roles, along with restrictions based on identity proofing level that are applied when fulfilling an attribute request. The Attribute Profile also formalise specifications for assumed self-asserted attributes that were previously missing in TDIF 06D.

Audience

Participating Relying Parties should use the attribute profile as **guidance** to determine what attribute they require, and how they will process them.

Accredited participants must treat these data standards as **requirements**, in addition to their obligations outlined in the Digital ID Act and the accreditation rules and data standards.