# Digital ID (AGDIS) Data Standards – Feedback Template

## Digital ID (AGDIS) Data Standards

The Digital ID Data standards are composed of 4 related elements:

* Content necessary for the AGDIS Data Standard as a legislative instrument
* Schedule 1 – AGDIS Onboarding Specifications
* Schedule 2 – AGDIS OpenID Connect Profile
* Schedule 3 – AGDIS Attribute Profile.

Copies of the AGDIS Data Standards can be found on the Digital ID website.

The Digital ID Act can be found on the [Federal Register of Legislation](https://www.legislation.gov.au/C2024A00025/asmade/text).

## Have Your Say

The Digital ID (AGDIS) Data Standards have been developed from the AGDIS specific requirements in Chapters 6, 06A, 06B and 06D of Trusted Digital Identity Framework (TDIF). Developed in and refined through extensive consultation with the community and industry over several years TDIF was the precursor to the voluntary legislated Accreditation scheme established by the Digital ID Act.

Using this template for your feedback is optional. It is provided for your convenience and contains general context information and questions that you may wish to use to direct your feedback. You may fill out as little or as much of the template as you want.

Please ensure that your consultation feedback is submitted by **5:00 pm** on **Thursday, 5 August 2024,** via the submissions page on the Digital ID website. There is an attachment option for you to upload and submit your feedback via Word or PDF document.

## Template Navigation

* [Attachment A – Preamble and General Comments](#_Attachment_A:_)
* [Attachment B – AGDIS Onboarding Specification Feedback](#_Attachment_B:_AGDIS)
* [Attachment C – AGDIS OpenID Connect Profile Feedback](#_Attachment_C:_AGDIS)
* [Attachment D - AGDIS Attribute Profile Feedback Table](#_Attachment_D:_AGDIS)

# Your details

|  |  |
| --- | --- |
| Organisation or Agency Name: |  |
| Contact Name: |  |
| Contact Email: |  |
| The name of the attachment/s you provided feedback in |  |

#

# Attachment A: Legislative Instrument content and General Comments Table

This table serves as a structure for gathering general feedback on the Digital ID (AGDIS) Data Standards. This approach ensures that your feedback is systematically documented and can be effectively reviewed and considered during the consultation process.

However should you wish to provide more detailed feedback on the Digital ID (AGDIS) Data Standards, please refer to Attachment B, C and D below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule |   | Page No. | Explanation  | Your Feedback |
| The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are drawn from, and interpreted in accordance with the Internet Engineering Taskforce’s Request For Comment 2119. As a legislative instrument that needs to balance readability by a technical audience with enforceability and certainty for compliance and enforcement audiences, is the mechanism as currently drafted in the AGDIS Data Standards workable? |
| Digital ID Standards  | Page No. | Part No. | Section | Your Feedback |
| Eg: Digital ID Data Standards | 1 | 4 | Definitions - (e) Australian Government Digital ID System; | <Insert your comments> |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |

# Attachment B: AGDIS Onboarding Specifications Feedback

Pease ensure you provide your feedback against the correct rule number, include the relevant page number and have completed the ‘your details’ section.

| Rule |  | Page No. | Explanation  | Your Feedback |
| --- | --- | --- | --- | --- |
| Not all elements of TDIF 06 Federation Onboarding Requirements (TDIF 06) have been transitioned to the Schedule 1 (AGDIS Onboarding Specifications). Features that are currently not active on the system, or do not have viable solutions have been deliberately excluded from these data standards to avoid compliance risks for AGDIS participants at commencement. The federation protocol mappings have been moved to the Schedule 2 (AGDIS OpenID Connect profile). A new section has been introduced outlining Identity Service Provider specific requirements. |
| Chapter 1—Common Requirements for Participating Accredited Entities |
| 1.1 Security Considerations |  | Was section 2.1.2 of TDIF 06, the intent of these requirements is unchanged. |  |
| 1.2 Identity Resolution |  | New elements include the introduction of an additional unique identifier type that only can be used by ISPs, and the formalised the use of sector identifiers.Features of TDIF 06 with no active implementation, like deduplication, have not been transitioned to the data standards to avoid compliance issues. No change from TDIF. |  |
| 1.2.1 General Purposes Identifiers |  |  |
| 1.2.2 Pairwise Identifiers |  |  |
| 1.2.3 Sector Identifiers |  |  |
| 1.3 Data Sharing |  | The intent of the data sharing requirements aligned with the those outlined in TDIF 06 section 5. |  |
| The Identity Exchange Provider (IXP) requirements currently not supported in the AGDIS have not been transitioned to the data standards for commencement, including SAML protocol support and deduplication. |
| Chapter 2—Identity Exchange Provider |
| 2.1 Technical Integration Requirements |  | Technical requirements previously outlined in TDIF 06 section 2 are now presented specifically for each accredited role. |  |
| 2.1.1 Protocol Requirements |  | The intent of these requirements in unchanged from TDIF 06. Please note that the optional requirements to support SAML have not been transitioned. |  |
| 2.1.2 Audit Requirements |  | Audit Identifier requirements have been transitioned from the TDIF 06 with the intent of maintaining the current requirements. |  |
| 2.1.3 Levels of Assurance |  | The levels of assurance used in the AGDIS will remain unchanged for commencement. Please provide feedback on if and when you would like the URNs updated to use Assurance Levels (AL) instead of Credential Level (CL).. |  |
| 2.1.4 Identity Resolution |  | New requirements to introduced to align the standards with how Sector Identifiers are currently used in the AGDIS, other the intention to implement a prohibition on single identifiers is maintained. |  |
| 2.1.5 Authenticated Sessions |  | Session management requirements have been transitioned from TDIF 06 with the intent to maintain current requirements.We invite you to provide feedback on alternative approaches to session management e.g. back-channel methods. |  |
| 2.1.6 Single Sign-On |  |  |
| 2.1.7 Single Logout |  |  |
| 2.1.8 Attribute Service Provider Integration |  | Redrafted with the intent of maintaining existing requirements whilst adding the option for an IXP to support the use of digital ID in existing ASP and PRP data sharing mechanisms. |  |
| 2.1.9 Federation Protocol Brokering |  | Simplified with the detailed federation protocol details moved to Schedule 2 (AGDIS OpenID Connect profile). |  |
| 2.2 Identity Provider Selection |  | Intent of these requirements is unchanged and aligned to the objective providing individuals with choice when access services connected to the AGDIS. |  |
| 2.2.1 Blinding |  | New requirements introduced to gather feedback during this consultation on the proposal to transition the AGDIS to a single blind where the ISP is blinded and the PRP is informed of which ISP authenticated the individual.We invite your feedback on these new requirements. Please outline your concerns or the opportunities you see from moving to a single blind. |  |
| 2.3 User Dashboard |  | No changes to the intent of the User Dashboard requirements have been introduced. |  |
| 2.4 Data Requirements |  | The intent of the data requirement is unchanged from the IXP role equivalent requirements TDIF 06. |  |
| 2.4.1 Attribute Requirements |  |  |
| 2.4.2 Computed attributes |  |  |
| 2.4.3 Attribute sharing policy |  |  |
| 2.4.4. Data representation |  |  |
| A newly introduced section bringing together the Identity Service Provider (ISP) specific requirements previously spread across TDIF 06. Please note that the requirements outlined in this section are not new and have the intent of their equivalent requirements outlined in TDIF 06. |
| Chapter 3—Identity Service Provider |
| 3.1 Technical Integration Requirements |  | Technical requirements previously outlined in TDIF 06 section 2 are now presented specifically for each accredited role. |  |
| 3.1.1 Protocol Requirements |  | Intent of these requirements in unchanged noting that the optional requirements to support SAML have not been transitioned. |  |
| 3.1.2 Identity Resolution |  | Current TDIF requirements have been transitioned with the addition requirements to permit the use of General Purposes Identifiers. |  |
| 3.1.3 Single Sign-On |  | Session management requirements have been transitioned from TDIF 06 with the intent to maintain current requirements. |  |
| 3.1.4 Single Logout |  |  |
| 3.2 Data Requirements |  | No changes to the intent of the data sharing requirements outlined in TDIF 06 section 5. |  |
| 3.2.1 Attribute Requirements |  |  |
| 3.2.2 Computed Attributes |  |  |
| Attribute Service Provider requirements have been redrafted with the intent of introducing terminology that is agnostic of specific technologies. The objective has been to introduce no breaking changes for existing ASPs whilst not limiting the scope for innovating approaches to facilitate attribute sharing via the AGDIS. |
| Chapter 4—Attribute Service Provider |
| 4.1 Technical Integration Requirements |  | Technical requirements previously outlined in TDIF 06 section 2 are now presented specifically for each accredited role. |  |
| 4.1.1 Protocol Requirements |  | The intent of these requirements unchanged from TDIF 06. |  |
| 4.1.2 Access Channels |  | A new concept introduced to focus the requirements on facilitating the sharing attributes across the AGDIS, and to declutter the requirements of technology specific terms. |  |
| 4.2 Audit Logging |  | The intent of these requirements in unchanged from the TDIF 06. |  |
| 4.3 Attribute Schema |  | A updated to the existing requirement the will require review as new governance requirements for the AGDIS are established. |  |

# Attachment C: AGDIS OpenID Connect Profile Feedback Table

Pease ensure you provide your feedback against the correct rule number, include the relevant page number and have completed the ‘your details’ section.

|  | Page No.  | Explanation  | Your feedback |
| --- | --- | --- | --- |
| **Aside from the departure from the TDIF requirements approach the AGDIS OpenID Connect Profile has only introduced clarifications based an initial review of these Data Standards by key participants. We invite your feedback on the approach to drafting, and any additional changes you would like to see in the profile.****Where the term client is used in the Data Standards, is it sufficient to be enforced** |
| **Chapter 1—Participating Identity Exchange** |
| **1.1 Authorisation Grant Types** |  | The intent of these requirements is unchanged from TDIF 06B OpenID Connect Profile (TDIF 06B). |  |
| **1.2 Client Types** |  | The intent of these requirements is unchanged from TDIF 06B, except for the inclusion of the Direct Access Client type. The Direct Access Client type has been introduced to support additional service and connectivity for ASPs |  |
| **1.2.1 Full Client with User Delegation** |  |  |
| **1.2.2 Native Client with User Delegation** |  |  |
| **1.2.3 Direct Access Client** |  |  |
| **1.3 Client Registration** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **1.4 Redirect URI** |  |  |
| **1.4.1 Native Client Applications** |  |  |
| **1.5 Connection to the Authorisation Server** |  |  |
| **1.4.1 Client Keys** |  |  |
| **1.6 Grant Types** |  |  |
| **1.7 Relying Party Profile** |  | Whilst the intent of the IXP Relying Party Profile requirements is unchanged from TDIF 06B, we invite feedback on this section to help us clarify ambiguities and improve them upon.  |  |
| **1.7.1 Requests to the Authorisation Endpoint** |  |  |
| **1.7.2 Request to the Token Endpoint** |  |  |
| **1.7.3 Token Response** |  |  |
| **1.7.3.1 ID Tokens** |  |  |
| **1.7.4 Request to the UserInfo Endpoint** |  |  |
| **1.7.5 Request Object** |  |  |
| **1.7.6 Discovery** |  |  |
| **1.8 Identity Exchange OpenID Connect Provider Profile** |  | Whilst the intent of the IXP OpenID Connect provider profile requirements are unchanged from TDIF 06B, we invite feedback on this section to help us clarify ambiguities and improve upon them. |  |
| **1.8.1 Connecting to Clients** |  |  |
| **1.8.1.1 Grant Types** |  |  |
| **1.8.1.2 Client Authentication** |  |  |
| **1.8.1.3 Dynamic Registration** |  |  |
| **1.8.1.4 Discovery** |  |  |
| **1.8.1.5 PKCE** |  |  |
| **1.8.2 Response to Authorisation Requests** |  |  |
| **1.8.2.1 Authentication Error Response** |  |  |
| **1.8.2.2 Responding to Invalid Claims** |  |  |
| **1.8.3 Token Response** |  |  |
| **1.8.4 User Info Endpoint** |  |  |
| **1.8.4 User Info Endpoint** |  |  |
| **1.8.5 Request Objects** |  |  |
| **1.8.6 Authentication Context** |  |  |
| **1.9 Entity Information** |  |  |
| **1.9.1 Claims Supported** |  |  |
| **1.9.2 Scope Profiles** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **1.10 User Consent** |  |  |
| **1.11 Privacy Considerations** |  |  |
| **1.12 Security Considerations** |  |  |
| **Chapter 2—Participating Identity Service Provider** |
| **2.1 Client Types** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **2.1.1 Full Client with User Delegation** |  |  |
| **2.2 Client Registration** |  |  |
| **2.3 Redirect URI** |  |  |
| **2.4 Client Keys** |  |  |
| **2.5 Grant Types** |  |  |
| **2.6 Technical Replying Party Profile** |  | Whilst the intent of these requirements is unchanged from TDIF 06B, to avoid terminology collisions with the Digital ID Act’s definition of a relying party, we have introduced the term technical relying party. The new term facilitates a description of an IXP’s role as an OpenID Connect relying party to its connected ISPs and is used more generally through Schedule 2 (AGDIS OpenID Connect Profile). |  |
| **2.6.1 Audit Logging** |  |  |
| **2.6.2 Request to the Authorisation Endpoint** |  |  |
| **2.6.3 Request to the Token Endpoint** |  |  |
| **2.6.4 Request to the User Info Endpoint** |  |  |
| **2.6.5 ID Tokens** |  |  |
| **2.6.6 Request Objects** |  |  |
| **2.6.7 Discovery** |  |  |
| **2.7 Identity Provider Profile** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **2.7.1 Audit Logging** |  |  |
| **2.7.2.1 Grant Types** |  |  |
| **2.7.2.2 Client Authentication** |  |  |
| **2.7.2.3 Dynamic Registration** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **2.7.2.4 Discovery** |  |  |
| **2.7.3 Requests to the Authorisation Endpoint (Authentication Request)** |  |  |
| **2.7.4 User Consent** |  |  |
| **2.7.5 Response to Authorisation Requests** |  |  |
| **2.7.5.1 Authentication Error Response** |  |  |
| **2.7.6 Token Response** |  |  |
| **2.7.6.1 ID Token** |  |  |
| **2.7.7 User Info Endpoint** |  |  |
| **2.7.8 Request Object** |  |  |
| **2.7.9 Authentication Context** |  |  |
| **2.8 Entity Information** |  | The intent of these requirements is unchanged from TDIF 06B. Noting that the ACR claim values will still use the legacy levels of assurance defined under the TDIF at commencement. |  |
| **2.8.1 Claims Supported** |  |  |
| **2.8.2 Scope Profiles** |  |  |
| **2.8.3 Valid ACR Claims** |  |  |
| **2.9 Privacy Requirements** |  | The intent of these requirements is unchanged from TDIF 06B. |  |
| **2.10 Security Considerations** |  |  |
| **Chapter 3—Protocol Brokering** |
| **3.1 Entity’s Obligation** |  | These requirements have been transitioned from TDIF 06 to the Schedule 2 (AGDIS OpenID Connect Profile). The intent of these requirements remains unchanged.  |  |
| **3.1.1 Mapping Claims and Scopes** |  |  |
| **3.1.2 Handing of Subject ID** |  | These requirements have been transitioned from TDIF 06 to the Schedule 2 (AGDIS OpenID Connect Profile). The intent of these requirements remains unchanged.  |  |
| **3.1.3 Mapping Assurance Levels** |  |  |
| **3.1.4 Prompt Parameter** |  |  |
| **3.1.5 ID Token Hint Parameter** |  |  |
| **Chapter 4—Attributes** |
| **4.1 Restricted Attributes** |  | The requirements have been introduced to clarify handling of restricted attributes for participants using OpenID Connect. |  |
| **4.2 OIDC Attribute Mapping** |  | The intent of these requirements is unchanged from TDIF 06B. |  |

# Attachment D: AGDIS Attribute Profile Feedback Table

Pease ensure you provide your feedback against the correct rule number, include the relevant page number and have completed the ‘your details’ section.

| Standard  | Page No.  | Explanation | Your feedback |
| --- | --- | --- | --- |
| The redrafting of TDIF 06D Attribute Profile into Digital ID (AGDIS) Data Standards has seen a significant change in previous approach to the presentation of requirements, and how attribute sharing policies are specified. The objective of the change has been to reduce ambiguity for all participating entities on the AGDIS. We invite feedback on the effectiveness of this new approach and welcome your suggestions to improve it further. |
| Chapter 1 —Operation of Attributes |  |
| To facilitate the use of attributes effective across the AGDIS the concept of an attribute sharing policy has been formalised in the opening chapter of attribute profile. Please provide feedback on the consent types, fulfillment requirements, access policy types, and the data representation requirements. |
| 1 Attributes and Attribute Sets |  | Outlines what attributes are on the AGDIS. |  |
| 1.2 Attribute Sharing Policy |  | Outlines the key features of an attribute sharing policy. |  |
| 1.2.1 Consent Types |  | Consent type have been defined by of the current models used under the TDIF, with refinement from the requirements of the Act. |  |
| 1.2.2 Fulfillment Requirements |  | A replacement for the previously ambiguous use of the MANDATORY and OPTIONAL keywords. |  |
| 1.2.3 Access Policy |  | Defines the rules that can be applied to the fulfillment of attribute or attribute set to determine if an accredited participant. |  |
| 1.2.4 Data Representation |  | Provider requirements that each attribute sharing policy must fulfill to ensure the data types for each attribute set are known by AGDIS participants. |  |
| Chapter 2 — Core Attributes |  |
| The presentation of attribute requirements is significant transition from the previous approach evolved for the TDIF. For each attribute or attribute set we define an attribute sharing policy that includes attribute handling requirements for each accredited participant. To progress the data minimisation objectives Identity Proofing levels requirements are also defined to limit access to attributes by participating relying parties. |
| 2.1 Mutual Attributes |  | Outlines the attribute sharing policies for the core attributes and system metadata that is shared across the AGDIS. |  |
| 2.1.1 Core |  | Attribute sharing policies for Core Digital Identity Attributes that are available on the AGDIS – name(s) and date of birth. New requirement IP1 Plus minimum to fulfill core attribute requests. |  |
| 2.1.2 Validated Contact Details |  | Validated contact details attribute sharing policy is outlined in this section. Note this attribute is available at all IP Levels. |  |
| 2.1.3 Verified Other Names |  | Verified Other Names comes from linking or EoI documents. A new requirement for these attributes limits fulfilment of attribute requests for verified other names to IP2 or higher. |  |
| 2.1.4 Verified Documents |  | Verified documents remain a restricted attribute, with additional restriction introduced. Attribute requests can only be fulfilled based upon the IP level associated with the attribute request.The data representation in this section enumerates values that are used in the federation protocol. |  |
| 2.1.4.1 Verified Birth Certificate Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.2 Verified Change of Name Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.3 Verified Marriage Certificate Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.4 Verified Citizenship Certificate Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.5 Verified Immigration Card Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.6 Verified Visa Request Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.7 Verified Driver License Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.8 Verified Medicare Card Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.9 Verified Passport Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.1.4.10 Verified Centrelink Concession Card Schema |  | Aligns to DVS match specifications, no breaking changes. |  |
| 2.2 Identity System Metadata |  | Outline the attribute sharing policies for AGDIS system metadata. |  |
| 2.2.1 Common |  | Outlines system metadata that is shared to facilitate the general operation of the AGDIS. These values are not attributes of an individual. |  |
| 2.2.1.1 Digital ID Identifier |  | No change from TDIF. |  |
| 2.2.1.2 Authentication Time |  | No change from TDIF. |  |
| 2.2.1.3 Assurance Level |  | No change from TDIF. |  |
| 2.2.1.4 Authentication Method |  | Proposed for introduction to support the changes to blinding policy. |  |
| 2.2.1.5 Last Updated |  | No change from TDIF. |  |
| 2.2.2 Audit |  | No change from TDIF. |  |
| 2.2.2.1 RP Audit Identifier |  |  |
| 2.3 Assumed Self-Asserted Attributes |  | Existed under TDIF however the attributes are now formally defined in this schedule. To avoid breaking changes assumed self-asserted attributes are only recommended and not required for commencement. The fulfillment of these attributes is done a best-effort basis. |  |
| 2.3.1 Preferred Name |  | An alternative or nickname an individual may provide. |  |
| 2.3.2 Addresses |  | An address or addresses supplied by the individual. The data representation mirrors the format defined in the OpenID Connect Core 1.0 specification. |  |
| 2.3.3 Other Email Addresses |  | One or more additional email address that conform the requirements of a validated email address (see 2.1.2 above). Additionally, they also have a contact type (based on the RFC 6350 vCard Format Specification).  |  |
| 2.3.4 Other Phone Numbers |  | One or more additional phone numbers that conform to the validated phone requirements (see 2.1.2 above). We also outline requirement for the telephony type, and a contact type (based on RFC 6350 vCard Format Specification). |  |
| 2.3.5 Place of Birth |  | Individual’s birthplace may be self-asserted or extracted from a Birth Certificate. Noting that this field is not available for verification when documents are submitted to the DVS. |  |
| 2.3.6 Audit |  | Self-asserted personal, professional, or culturally significant title. |  |
| 2.3.7 RP Audit Identifier |  | No change from TDIF. |  |
| 2.4 Computed Attributes  |  | Whilst no computed attributes are defined on the AGIDS this section has been provided to outline requirements that any computed attributes must meet. |  |
| Chapter 3 — Attribute Service Provider Profiles |  |
| 3.1 Business Authorisations |  | Attributes that are managed and supplied by the Australian Tax Office’s Relationship Authorisation Manager (RAM). |  |
| 3.2 MyGov Link Identifier |  | An attribute that is supplied to myGov member services that are also AGDIS participating relying parties. |  |
| Chapter 4 — OpenID Connect Attribute Profile |  |
| 4.1 Attribute Mapping |  | The attribute mapping defines how the AGDIS Attribute Profile maps to the AGDIS OpenID Connect Profile for each accredited participants role. |  |
| 4.1.1 Identity Exchange Provider Replying Party Mapping |  | Mappings of the attributes to the OpenID Connect scopes and claims that are available for participating relying parties to request. |  |
| 4.1.2 Identity Provider Scopes and Claims |  | Mappings of the attributes to the OpenID Connect scopes and claims that an Identity Service Provider makes available to an Identity Exchange Provider. |  |
| 4.2 Data Types |  | Outlines the data types used to define the payloads for each scope and claim. |  |
| 4.2.1 JavaScript Object Notation Types |  | Alignment of the primitive data types used to JSON data types.  |  |
| 4.2.2 Simple Data Types |  | Single value data types derived from JSON primitives. |  |
| 4.2.2.1 Name String |  | Used to represent optional name of an individual. |  |
| 4.2.2.2 Required Name String |  | Used to represent required name of an individual. |  |
| 4.2.2.3 Boolean |  | Convenience notation for the underlying JSON literals. |  |
| 4.2.2.4 Date |  | RFC 3339 compliant date values. |  |
| 4.2.2.5 Date Time |  | RFC 3339 compliant date-time values. |  |
| 4.2.2.6 Unix Timestamp |  | Numeric value. |  |
| 4.2.2.7 Email |  | Email address |  |
| 4.2.2.8 Phone Number |  | ITU-T E.164 compliant phone number. |  |
| 4.2.2.9 UUID |  | Used for the RP Audit ID |  |
| 4.2.3 Complex Data Types |  | JSON list or objects. |  |
| 4.2.3.1 Other Names Object |  | Used to represent the Verified Other Names attribute set |  |
| 4.2.3.2 Address Object |  | Represents a single self-asserted Address value. |  |
| 4.2.3.3 Other Email Address Object |  | An object for representing the self-asserted other email address attributes. |  |
| 4.2.3.4 Other Phone Number Object |  | An object for representing the self-asserted other phone number attributes. |  |
| 4.3 Mutual Attributes |  | Definition for the attributes defined in Chapter 2 of this Schedule that are used when fulfilling OpenID Connect attribute requests. |  |
| 4.3.1 Core |  |  |
| 4.3.2 Validated Contact Details |  |  |
| 4.3.3 Verified Other Names |  |  |
| 4.3.4 Verified Documents |  |  |
| 4.3.4.1 Document Identifiers Object |  |  |
| 4.3.4.2 Document Names Object |  |  |
| 4.3.4.3 Document Attributes Object |  |  |
| 4.4 Identify System Metadata |  |  |
| 4.4.1 Common |  |  |
| 4.4.1.1 Subject ID |  |  |
| 4.4.1.2 Authentication Time |  |  |
| 4.4.1.3 Assurance Level |  |  |
| 4.4.1.4 Authentication Method |  |  |
| 4.4.1.5 Last Updated |  |  |
| 4.4.1 Audit |  |  |
| 4.4.2.1 RP Audit Identifier |  |  |
| 4.5 Self-Asserted Attributes |  |  |
| 4.5.1 Preferred Name |  |  |
| 4.5.2 Addresses |  |  |
| 4.5.3 Other Email Addresses |  |  |
| 4.5.4 Other Phone Numbers |  |  |
| 4.5.5 Place of Birth |  |  |
| 4.5.6 Personal Titles |  |  |
| 4.6 Computed Attributes Data Definitions |  |  |
| 4.7 Attribute Service Providers |  | Definition for the attributes supplied by Attribute Service Providers that are used when fulfill OpenID Connect attribute requests. |  |
| 4.7.1 Business Authorisations |  |  |
| 4.7.2 MyGov |  |  |
| 4.8 Normative OIDC Profile Attribute Examples |  | Please review the normative examples supplied against what you current make available to participants or receive as a relying party. |  |
| 4.8.1 Core |  |  |
| 4.8.2 Validated Contact Details |  |  |
| 4.8.3 Verified Other Names |  |  |
| 4.8.4 Verified Documents |  |  |
| 4.8.4.1 Birth Certificate |  |  |
| 4.8.4.2 Centrelink Concession Card |  |  |
| 4.8.4.3 Change of Name Certificate |  |  |
| 4.8.4.4 Citizenship Certificate |  |  |
| 4.8.4.5 Registration by Descent Certificate |  |  |
| 4.8.4.6 Australian Driver License |  |  |
| 4.8.4.7 ImmiCard |  |  |
| 4.8.4.8 Marriage Certificate |  |  |
| 4.8.4.9 Medicare Card |  |  |
| 4.8.4.10 Australian Travel Document |  |  |
| 4.8.4.11 Visa |  |  |
| 4.8.5 Identity System Metadata |  |  |
| 4.8.5.1 Digital ID Pairwise Identifier |  |  |
| 4.8.5.2 Authentication Time and Updated At |  |  |
| 4.8.5.3 Authentication Method |  |  |
| 4.8.5.4 Audit Identifiers |  |  |
| 4.8.6 Sled-Asserted Attributes |  |  |
| 4.8.6.1 Addresses |  |  |
| 4.8.6.2 Other Email Addresses |  |  |
| 4.8.6.3 Other Phone Numbers |  |  |
| 4.8.6.4 Personal Title Normative Examples |  |  |
| 4.8.7 Business Authorisations  |  |  |