Australian Government

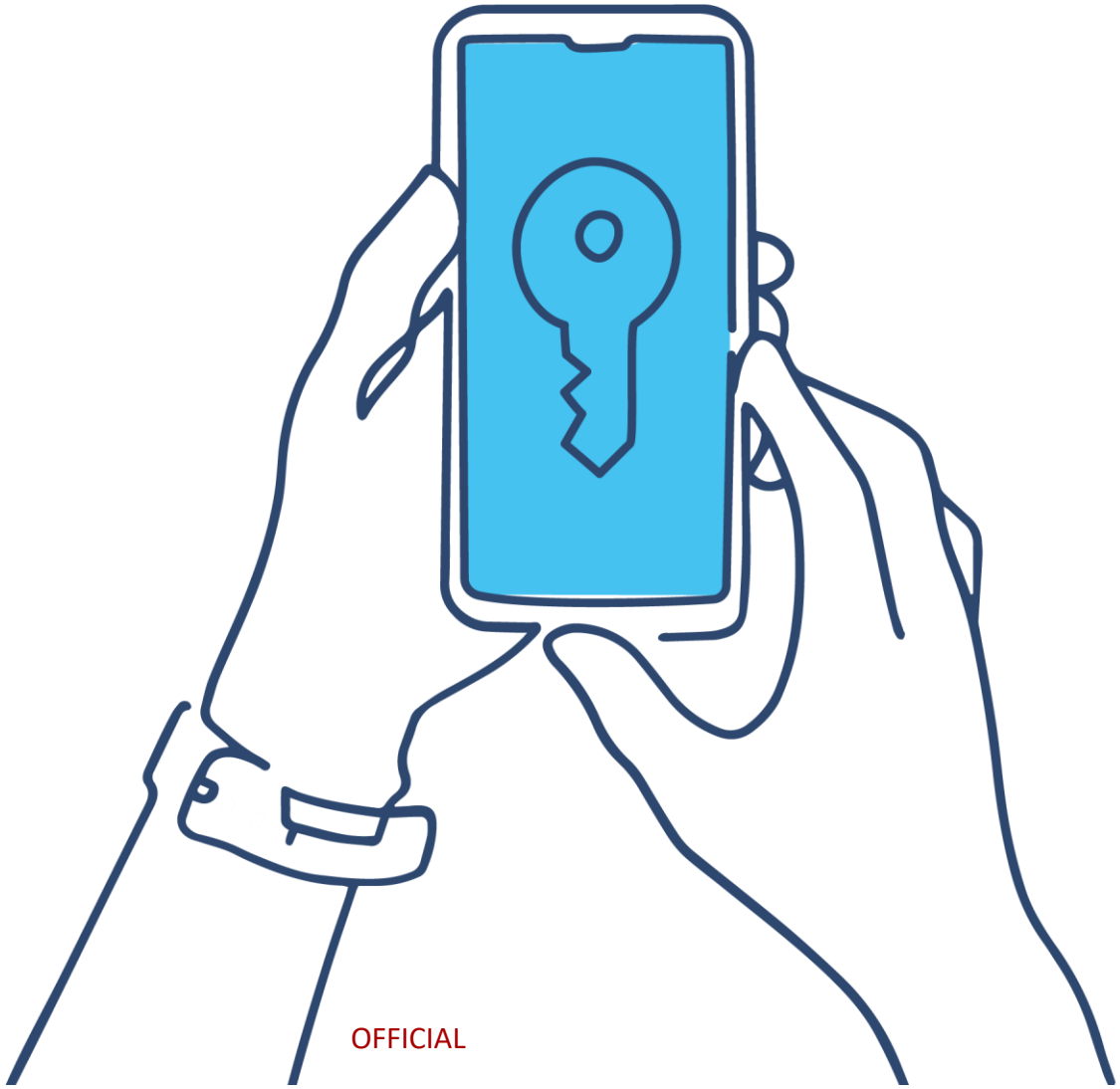
Digital Identity

06D Attribute Profile

Trusted Digital Identity Framework

Release 4.6 – March 2022

PUBLISHED VERSION



Digital Transformation Agency (DTA)

Licence

Use of the Coat of Arms

The terms under which the Commonwealth Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Conventions

References to *TDIF* documents, abbreviations and key terms (including the words *MUST*, *MUST NOT*, and *MAY)* are denoted in italics are to be interpreted as described in the current published version of the *TDIF: 01 – Glossary of Abbreviations and Terms.*

TDIF requirements and references to *Applicants* are to be read as also meaning *Accredited Providers*, and vice versa. The scope of *TDIF* requirements are to be read as applying to the identity system under *Accreditation* and not to the organisation's broader operating environment.

Contact us

The *DTA* is committed to providing web accessible content wherever possible. This document has undergone an accessibility check however, if you are having difficulties with accessing the document, or have questions or comments regarding the document please email digitalidentity@dta.gov.au

Document management

The *DTA* has endorsed this document for release.

Change log

Document Version		Date	Author	Description of the changes
0.1		Jan 2020	AV	Initial version
0.2		Mar 2020	AV	Minor updates to align with the TDIF Release 4 structure.
1.0	4.0	May 2020		Published version
1.1	4.4	June 2021	AV	CRID0018 – Changes to structure of document and addition of additional name *Attributes.*
1.2	4.5	Oct 2021	AV	CRID0026 – Emergency Changes to correct Business Authorisations Attribute Example
1.3	4.6	Mar 2022	AV	CRID0029 - Minor text update (Table 30, Page 12)

All changes made to the TDIF are published in the TDIF Change Log which is available at https://www.digitalidentity.gov.au/privacy-and-security/trusted-digital-identity-framework.

Contents

List of tables

Introduction

This document defines all *Attributes* that can be requested by *Participants* of the *Australian Government Digital Identity System*. This document will be updated with additional *Attributes* and *Federation protocols* as the *Australian Government Digital Identity System* expands.

The intended audience for this document includes:

- *Accredited Participants.*
- *Applicants*.
- *Assessors.*
- *Relying Parties*.

To the extent of any conflict between any requirement in the *TDIF 05 – Role Requirements* and this document regarding *Attributes* available in the *Australian Government Digital Identity System*, the *TDIF 06D – Attribute Profile* takes precedence.

Attribute Sets

2.1 *Attribute Sets*

The *Attributes* passed through the *Australian Government Digital Identity System* are split into *Attribute Sets*. *Attribute Sets* correspond to the logical sets of *Attributes* that an *RP* will typically ask for as a collection, and that a *User* will provide consent for as a collection. Some *Attribute Sets* will contain a single attribute, and some will contain several *Attributes*. The presence of *Attribute Sets* does not preclude *Attributes* being requested individually by an *RP* to support the principle of only releasing the minimum *Attributes* required.

Table 1 sets out how the *Attributes* described in this document are split into *Attribute Sets*.

Table 1: Trust Framework *Attribute Sets*.

Attribute Set	*Attributes*	Description
Core	Full Name Family Name Given Names Middle Names Preferred Name Date of Birth Core *Attributes* Last Updated	The core *Attributes* – name and date of birth.
Validated Email	Validated Email Validated Email Last Updated	Validated email address.
Validated Phone	Mobile Phone Number Validated Mobile Phone Number Last Updated.	Validated mobile phone number.
Verified Other Names	Verified Other Names Verified Other Names Last Updated	Verified other names that the user has used.
Verified Documents	Verified Documents	Verified *Attributes* from documents used to conduct *Identity Proofing*. These are *Restricted Attributes*.

Attribute Set	*Attributes*	Description
Common	RP Audit Id Authentication Time TDIF EDI Identity Proofing Level Credential Level *Digital Identity* (user identifier) Last Updated	Common *Attributes* that are not specific to an *Attribute Set*. These *Attributes* support the use of *Attributes* by Relying Parties.
myGov Link	myGov LinkID	*Attributes* used to link a myGov account to a myGov member service for a particular user at the Relying Party which requested the authentication.
Business Authorisations	Unique Relationship ID Entity ID Entity Type Entity Name Contact Emails Relationship Type Relationship Start Time Relationship End Time Roles Entitlements *Attributes* Last Updated	All *Attributes* that specify a business authorisation. For more detail see section 5.1.2.

2.2 Attribute Sharing Policies

Attribute Sharing Policies are applied to all *Attributes* that are contained in an *Attribute Set*. These policies describe the rules that must be applied when sharing these *Attributes* with an *RP*. The key element of these policies relate to the operation of user consent.

Table 2: Trust Framework attribute sharing policies.

Attribute Set	Consent Requirement	Additional Policy Requirements
Core	Every Change	None
Validated Email	Every Change	None

Attribute Set	Consent Requirement	Additional Policy Requirements
Validated Mobile Phone Number	Every Change	None
Verified Other Names	Every Change	None
Verified Documents	Every Change	*Restricted Attributes*. A *Relying Party* must be authorised by the *Oversight Authority* to request verified documents. This authorisation may be restricted to specific document types.
Common	Not required	Not Applicable
myGov Link	Not required	Only available for a relying party which is a myGov member service.
Business Authorisations	Every Change	None

Table 3 sets out the meanings of each *Consent* type that is prescribed for *Attribute Sets* in the *TDIF*.

Table 3: Trust Framework consent types.

Consent Type	Description
Not required	User consent is not required for the *Attributes*. In general, this applies to technical *Attributes* that support the operation of the *Australian Government Digital Identity System* rather than *Attributes* that describe an *Individual*.
Single-use	*Express Consent* is required for the *Attributes* every time a user authenticates to a *Relying Party*.
Ongoing	*Express Consent* for the *Attributes* is required at least the first time it is shared with a Relying Party. The *User* then has the option for this consent to be remembered. The *User* must be provided with a mechanism to revoke this consent.
Every Change	This consent type extends the Ongoing consent type by requiring *Express Consent* for the *Attributes* every time an attribute has changed. To meet this requirement the attribute have a date time attribute associated with it that that enable the *Identity Exchange* to determine if the attribute has changed since the last time that *Express Consent* was provided.

2.3 Authorised *Attribute Sets*

Table 4: *TDIF* authorised *Attribute Sets*.

Attribute Set	Relying Parties authorized to request
Core	All
Validated Email	All
Validated Mobile Phone Number	All
Verified Other Names	All
Verified Documents	*Relying Parties* approved to request Verified documents as *Restricted Attributes* by the *Oversight Authority*.[1]
Common	Not required.
myGov Link	myGov Member Services
Business Authorisations	All

[1] *Relying Parties* can apply to the *Oversight Authority* for permission to receive *Restricted Attributes*.

Core *Attribute* Profile

The Core *Attributes* are the *Attributes* shared in the *Australian Government Digital Identity System* independent of any *Attribute Service Providers*. It includes the following *Attribute Sets*:

- Core
- Validated Email
- Validated Phone
- Verified Other Names
- Verified Documents
- Common

3.1 Mutual *Attributes*

These are the *Attributes* which both *IdPs* and *Identity Exchanges* are required to support.

3.1.1 Core *Attributes*

The core *Attributes* of a *Person*'s identity are their full name and their date of birth. Core *Attributes* are populated from the identity documents used by an IdP to verify the *Attributes* of the *Individual* if they have verified a document. A *User* may also provide their Preferred Name to an *IdP*, but it is not a verified attribute. Preferred Name may accompany the core attributes but should not be relied upon for name matching by a *Relying Party*.

Table 5: Trust Framework core *Attributes*.

Attribute	Description	Mandatory/ Optional
Full Name	*Person*'s Full Name. This will be one or more names separated by a space. This is generated from the Given Names, Middle Names and Family Names.	Optional

Attribute	Description	Mandatory/ Optional
Family Name	*Person*'s family name. Where the *Person* has a single name it is used as the family name.	Mandatory
Given Names	*Person*'s given names. There may be zero or more names separated by a space.	Mandatory
Middle Names	*Person*'s middle names. There may be zero or more names separated by a space. Note that in some cultures, middle names are not used.	Mandatory
Preferred Name	*Person*'s Preferred Name. This is a name which the *User* can indicate is the preferred name by which they are to be addressed at a *Relying Party*.	Optional
Date of Birth	*Person*'s date of birth.	Mandatory
Core *Attributes* Last Updated	Date and time of when the core *Attributes* for a *Person* were last updated.	Mandatory

3.1.2 Validated contact details *Attributes*

Table 6 lists the validated contact details *Attributes* that defined by the TDIF. These *Attributes* are sourced from an IdP, which in turn gathers them from the Identity Proofing process. IdPs are required to validate the mobile phone number and email address as per the guidance in section 2.5 of the *TDIF 05A Role-Specific Guidance*.

Table 6: Trust Framework validated contact details *Attributes*.

Attribute	Description	Mandatory/ Optional
Validated Email	Validated Email address.	Optional
Validated Email Last Updated	Date and time of when the validated email address was last updated.	Optional
Validated Mobile Phone Number	Validated Mobile Phone Number.	Optional

Attribute	Description	Mandatory/ Optional
Validated Mobile Number Last Updated	Date and time of when the validated mobile phone number was last updated.	Optional

3.1.3 Verified Other Names *Attributes*

These *Attributes* are sourced by an *IdP* from the *Evidence of Identity* (*EOI*) documents that was used to achieve *Identity Proofing Levels* according to the *TDIF 05 Role Requirements*. These *Attributes* include the variations of the *Person*'s name from those recorded in the core *Attributes* and are only sourced from the following document types:

- *CoI documents.*
- *Photo ID documents.*
- *Linking documents.*

Table 7: Trust Framework other verified names *Attributes*.

Attribute	Description	Mandatory/ Optional
Other Verified Names	Collection of Family Name, Middle names and Given Names tuples for each of the *Person*'s other verified names. The Family Name, Middle Names and Given Names *Attributes* are as defined in the TDIF core *Attributes*.	Optional
Other Verified Names *Attributes* Last Updated	Date and time of when the other verified names *Attributes* for a *Person* where last updated.	Optional

3.1.4 Verified Document *Attributes*

Table 8 lists the other verified document *Attributes* that defined by the *TDIF*. These *Attributes* are sourced by an IdP from the *Evidence of Identity* (*EOI*) documents listed in *Appendix A* of the *TDIF 05 Role Requirements*. These *Attributes* are only sourced from the following document types:

- *CoI documents.*

- *Linking documents.*
- *UitC documents.*
- *Photo ID documents.*

Verified Documents are *Restricted Attributes* and will only be returned to a Relying Party if they are approved to receive these *Attributes*.

Table 8: Trust Framework verified document *Attributes*.

Attribute	Description	Mandatory/ Optional
Verified Documents	Collection of verified documents including document metadata, document identifiers, document names and date of birth, and additional *Attributes* specific to a document type.	Mandatory

The Verified Documents *Attribute* is a collection of the verified documents that a user has used to conduct *Identity Proofing*. There can be multiple instances of a Verified Document within the Verified Documents attribute. Table 9: Trust Framework Verified Documents collection. details the sub-*Attributes* contained as part of a Verified Document.

Table 9: Trust Framework Verified Documents collection.

Attribute	Description	Mandatory/ Optional
Document Type Code	A URN representing the type of document.	Mandatory
Document Verification Method	The TDIF verification method by which the document was verified. “S”=Source Verification, “T”=Technical Verification, “V”=Visual Verification.	Mandatory
Document Verification Date	The date and time that the document was verified.	Mandatory
Document Issuer State	For state-based documents the state code (‘NSW’, “QLD”, “VIC”, “TAS”, “WA”, “SA”, “ACT”, “NT”) is a required attribute.	Optional
Document Identifiers	Document Identifiers. This a multi-valued attribute.	Mandatory

Attribute	Description	Mandatory/ Optional
Document Names	Document names are the names recorded on the document. The format varies according to the document type.	Optional
Document Date of Birth	The *Person*'s date of birth as recorded on the document.	Optional
Document *Attributes*	*Attributes* that are specific to a document type. This is a multi-valued attribute.	Optional

Table 10: Trust Framework Document Names.

Attribute	Description	Mandatory/ Optional
Family Name	*Person*'s family name as recorded on the document.	Optional
Given Names	*Person*'s given names as recorded on the document.	Optional
Family Name 2	Additional family name as recorded on the document. This is currently used by Linking documents that contain two names.	Optional
Given Name 2	Additional given names as recorded on the document. This is currently used by Linking documents that include a previous and new name.	Optional
Middle Name	*Person*'s middle name as recorded on the document.	Optional
Full Name	*Person*'s full name as recorded on the document.	Optional

Both the Document *Attributes* and Document Identifiers sub-*Attributes* are multi-valued *Attributes* comprised of Type-Value Tuples as set out in **Table 11**.

Table 11: Trust Framework Type-Value Tuple.

Attribute	Description	Mandatory/ Optional
Type	The "type" of the attribute. Where the *Attribute* is sourced from a document type that can be verified using DVS then the type should be the	Mandatory

Attribute	Description	Mandatory/ Optional
	name of the DVS Field Name defined in the relevant DVS Match Specification.	
Value	The value of the *Attribute* as a string.	Mandatory

3.1.5 Identity System Metadata

This section refers to the *Identity System Metadata Attributes* which are shared by an *Identity System* to support its operation. These *Attributes* are generated by a *Participant*. These *Attributes* are not a part of an *Attribute Set*.

Table 12: *Identity System Metadata Attributes*

Attribute	Description	Mandatory/ Optional
Digital Identity (user identifier)	The *User's* identifier at the party requesting the *Attribute*. This is assigned by the supplier of the *Attribute* and is required to be a *pairwise identifier*. For further detail as to the requirements around generation and sharing of this *Attribute*, see section 2.3.1.1 of the *TDIF 06 – Federation Onboarding Requirements*.	Mandatory
Authentication Time	Date and time when the *Person* was authenticated at the *Identity Service Provider*.	Mandatory
Identity Proofing Level	The *Identity Proofing Level* of the *Digital Identity*.	Mandatory
Credential Level	The *Credential Level* of the *Credentials* used in an *Authentication*.	Mandatory
Last Updated	Date and time that any of the *Individual's Attributes* were last updated.	Mandatory

3.2 IdP Specific *Attributes*

This section refers to *Attributes* which the *IdPs* are required to be able to share if requested by the *Identity Exchange*, but the *Identity Exchange* is not required to share.

Table 13: IDP specific *Attributes*.

Attribute	Description	Mandatory/ Optional
TDIF EDI	Evanescent Deterministic Identifier used by an exchange for the purposes of Deduplication.	Mandatory

3.3 Exchange Specific *Attributes*

Additional *Attributes* are supplied by an *Identity Exchange* to support the operation of the *Australian Government Digital Identity System*.

Table 14 lists the additional *Attributes* that an *Identity Exchange* may provide to a *Relying Party* in response to an *Authentication* request.

Table 14: Trust Framework additional *Identity Exchange Attributes*.

Attribute	Description	Mandatory/ Optional
RP Audit Id	A unique identifier for every logical interaction between a Relying Party and an *Identity Exchange* to enable an audit trail. This *Attribute* is generated by an *Identity Exchange*, made available to a Relying Party. It is never shared with an Identity Provider.	Mandatory
myGov LinkID	The pairwise identifier used to link a myGov account to a myGov member service for a particular user at the Relying Party which requested the authentication.	Optional

3.4 Computed *Attributes*

A *Computed Attribute* is an *Attribute* that is dynamically derived from the *Attributes* in an *Attribute Set* using an algorithm. Using *Computed Attributes* supports privacy outcomes by only releasing the minimum required set of *Attributes* to *RPs* to meet the need of the service being accessed. For example, a *RP* may need to know an *Individual's* age or an indicator that *Individual* is above at certain age. This need can

be supported by providing a *Computed Attribute* that is derived from the *Individual's* date of birth.

Computed Attributes can be supplied by an *IdP*, an *Attribute Service Provider*, or an *Identity Exchange*. In a federation where there are multiple *IdPs*, an *Identity Exchange* can more readily adapt to support the needs of the *RPs* that it supports.

The *Attribute* sharing policies for a *Computed Attribute* must be consistent with the *Attribute* sharing policies of the *Attributes* that it is derived from.

Computed Attributes are synonymous with *Attribute References* defined in the *NIST* digital identity standards[2]. An *Attribute* reference is defined by NIST as:

> *A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December."*

There are currently no *Computed Attributes* shared in the *Australian Government Digital Identity System*. When *Computed Attributes* are added to the federation they will be described in this section.

3.5 *Assumed Self-asserted Attributes*

Assumed Self-asserted Attributes are *Attributes* provided by an *Individual* that can assist with service delivery, such as prefilling online forms. It is optional for an *IdP* to support the disclosure of *Assumed Self-asserted Attributes* .

[2] https://pages.nist.gov/800-63-3/sp800-63-3.html

Table 15: *Assumed Self-Asserted Attributes*.

Attribute	Description	Mandatory/ Optional
Preferred name(s)	*Person*'s Preferred Name. This is a name which the user can indicate is the preferred name by which they are to be addressed at a Relying Party. This is included in the Core *Attribute Set*.	Optional
Residential address	*Person's* residential address, as asserted by them.	Optional
Postal address	*Person's* postal address, as asserted by them.	Optional
Other address	*Person's* other addresses, as asserted by them (e.g. second residential address).	Optional
Other phone number (e.g. landline)	Any other unvalidated phone numbers of a *Person*, as asserted by them.	Optional
Place of Birth	*Person's* place of birth.	Optional
Titles (e.g. Dr. Mr, Ms)	*Person's* title. This is the preferred title of the *Person* as indicated by them.	Optional

Apart from Preferred name(s) the SAML and OIDC mappings for the above *Attributes* have not been specified. When they are specified, the mapping will be incorporated into this profile.

Federation Protocol Mappings

4.1 OIDC *Attribute* Mapping

Broadly speaking:

- *Attributes* correspond to claims in *OIDC*.
- *Attribute Sets* correspond to scopes in *OIDC*.

The following tables describe the mapping of the *TDIF Attributes* to *OIDC* claims. All claims are standard *OIDC* claims except for claims that are prefixed with `tdif.` For standard claims a reference to the applicable section of the OpenID Connect 1.0 Core [OpenIDCore] is provided.

The key design goals for the *OIDC Attribute* mapping for *IdPs* are:

- Conform to standards.
- Use custom claims and scopes for *TDIF*-specific *Attributes* to avoid conflicts with any other uses of the *Attributes*, and limit the data being returned from an IdP.
- Support extensibility by allowing additional claims and scopes can be easily added as the *Attributes* handled by an *Identity Exchange* is expanded.

The key design goals for the *OIDC Attribute* mapping for *RPs* are:

- Maximise interoperability to simplify onboarding of *RPs*.
- Use commonly implemented features of the standards.
- Minimise the use of extensions to the standards.

4.1.1 *Attribute* Mapping

Table 16 sets out the mapping of the *Attributes* described in section 3 of this document to the *OIDC* claims which represent those *Attributes*. It also outlines the maximum set of *Attributes* it is expected that *Identity Service Providers* and *Identity Exchanges* can support provision of via their *OIDC* interface.

Table 16: OIDC *Attribute* mapping.

Attribute	OIDC Claim	JSON Type	Can be requested from *Identity Exchanges*[3]	Can be requested from *Identity Service Providers*[4]	OIDC Standard Reference
Digital Identity (user identifier)	sub	string	**Yes**	**Yes**	Section 2, Section 8
Full Name	name	string	**Yes**	**Yes**	Section 5.1
Family Name	family_name	string	**Yes**	**Yes**	Section 5.1
Given Names	given_name	string	**Yes**	**Yes**	Section 5.1
Middle Names	middle_name	string	**Yes**	**Yes**	Section 5.1
Preferred Name	preferred_username	string	**Yes**	**Yes**	Section 5.1
Date of Birth	birthdate	string	**Yes**	**Yes**	Section 5.1
Core *Attributes* Last Updated	tdif_core_updated_at	number	**Yes**	**Yes**	
Validated Email	email	string	**Yes**	**Yes**	Section 5.1
Email Validated Indicator	email_verified The value of this claim must always be true	boolean	**Yes**	**Yes**	Section 5.1

[3] This refers to the attributes which a *Relying Party* can request from an *Identity Exchange* using *OIDC*. The *Identity Exchange* does not store this information but retrieves it from *Identity Service Providers* and *Attribute Service Providers*, as per the requirements for *Identity Exchanges* outlined in the *TDIF 04 – Functional Requirements*.

[4] This refers to the *Attributes* that an *Identity Exchange* can request from an *Identity Service Provider*.

Attribute	OIDC Claim	JSON Type	Can be requested from *Identity Exchanges*[3]	Can be requested from *Identity Service Providers*[4]	OIDC Standard Reference
Validated Email Last Updated	tdif_email_updated_at	number	**Yes**	**Yes**	
Validated Mobile Phone Number	phone_number	string	**Yes**	**Yes**	Section 5.1
Mobile Phone Number Validated Indicator	phone_number_verified The value of this claim must always be true	boolean	**Yes**	**Yes**	Section 5.1
Validated Mobile Phone Last Updated	tdif_phone_number_updated_at	number	**Yes**	**Yes**	
Other Verified Names	tdif_other_names	complex type	**Yes**	**Yes**	
Other Verified Names Last Updated	tdif_other_names_updated_at	number	**Yes**	**Yes**	
Verified Documents	tdif_doc	complex type	**Yes**	**Yes**	
Identity Proofing Level and *Credential Level*	acr	string	**Yes**	**Yes**	Section 2
Authentication Time	auth_time	number	**Yes**	**Yes**	Section 2
RP Audit Id	tdif_audit_id	string	**Yes**	**No**	
TDIF EDI	tdif_edi	string	**No**	**Yes**	
myGov LinkID	mygov_link_id	string	**Yes**	**No**	
Last Updated	updated_at	number	**Yes**	**Yes**	Section 5.1

The acr claim is returned as a string specifying one of the values described in section 4.2.1 of the *TDIF 06 – Federation Onboarding Requirements*.

The tdif_doc claim is returned as a complex JSON type containing an array of zero or more occurrences of a tdif_doc, each of which will be comprised of the following sub-*Attributes* described in **Table 17**.

Table 17: Tdif doc sub-*Attributes*.

Sub-attribute	JSON *Attribute* name	JSON Type	Schema Reference
Document Type	type_code	string	
Document Verification Method	verification_method	string	
Document Verification DateTime	verification_date	string	
Document Issuer State	issuer_state	string	
Document Identifiers	identifiers	complex	
Document Names	names	complex	
Document Date of Birth	birthdate	string	
Document *Attributes*	attributes	complex	

The Document Names sub-*Attribute* is a complex *JSON* type that contains the sub-*Attributes* listed in Table 18.

Table 18: Tdif document names sub-*Attributes*.

Sub-attribute	JSON *Attribute* name	JSON Type	Schema Reference
Family Name	family_name	string	
Given Names	given_name	string	
Family Name2	family_name_2	string	
Given Names2	given_name_2	string	
Middle Name	middle_name	string	
Full Name	full_name	string	

The Document identifiers and Document Attributes sub-*Attributes* are complex *JSON* types that contain an array of zero or more occurrences of the type-value tuple

specified in Error! Not a valid bookmark self-reference.. The list of possible types of identifiers for each document is described in **Table 39** in Annex B of this document. The list of possible types of *Attributes* can found in **Table 39** in Annex B. An example of a tdif_doc *Attribute* being returned can be found in **Table 38**.

Table 19: Tdif type-value sub-attribute.

Sub-attribute	JSON *Attribute* name	JSON Type	Schema Reference
Type	type	string	
Value	value	string	

4.1.1.1 Additional OIDC Attributes

The following additional *Attributes* are defined to support interoperability using the standard claims defined in the OpenID Connect 1.0 Core specification [OpenIDCore].

Table 20: Additional OIDC *Attributes*.

Attribute Set	*Attributes*	Description
Validated Email	Email Validated Indicator	Email address indicator as to whether it has been validated.
Validated Phone	Mobile Phone Number Validated Indicator	Mobile phone number indicator as to whether it has been validated.
Common	Last Updated	The time that any of the end-user's information was last updated

4.1.2 RP OIDC Scopes and Claims

A *Relying Party* can request *Attributes* from an *Identity Exchange* as per the *Relying Party* to *Identity Exchange* profile defined in section 2 of the *TDIF 06B – OpenID Connect 1.0 Profile*.

Under this profile, a *Relying Party* using OIDC can obtain *Attributes* by either requesting claims as part of a scope, or as individual claims as per section 5.5.1 of the OpenID Connect Core 1.0 standard using the `claims` parameter. The claims available to a *Relying Party* are defined in **Table 16**. The *Relying Party* may also

make requests for scopes and claims provided by *Attribute Service Providers* as described in section 5 of this document.

The following *OIDC* scopes are available to *Relying Parties*:

- `openid`
- `profile`
- `email`
- `phone`
- `tdif_doc`

Table 21 contains the mapping of these scopes to *Attribute Sets* and the claims that will be returned if the scopes are requested.

Table 21: OIDC *Attribute* Profile for RPs.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
Common	openid	sub tdif_audit_id auth_time acr	ID Token UserInfo	Standard *OIDC* scope. These *Attributes* are returned for any scope requested
Core	profile	name family_name given_name middle_name preferred_username birthdate updated_at tdif_core_updated_at	ID Token UserInfo	Standard scope. Only the claims noted are returned.
Validated Email	email	email email_verified tdif_email_updated_at	ID Token UserInfo	
Validated Phone	phone	phone_number phone_number_verified tdif_phone_number_updated_at	ID Token UserInfo	
Verified Other Names	No scope for request.	tdif_other_names tdif_other_names_updated_at	UserInfo	Custom claims, which can only be requested via an individual claim request.
Verified Documents	tdif_doc	tdif_doc	UserInfo	Custom scope

Any Claims requested will be made available as follows:

- Via an ID Token from the Token Endpoint.
- Via the UserInfo Endpoint.

Claims will generally be available via both endpoints; however some claims are only available from certain endpoints as described above in **Table 21**. Additional

parameters may be returned as part of the authorisation response as per the *Relying Party* to *Identity Exchange* profile defined in section 2 of the *TDIF 06B – OpenID Connect 1.0 Profile*.

4.1.3 IdP OIDC Scopes and Claim Requests

An *Identity Exchange* can request *Attributes* from an *Identity Service Provider* using the *Identity Exchange* to *Identity Service Provider* profile described in section 3 of the *TDIF 06B – OpenID Connect 1.0 Profile.*

Under this profile, an *Identity Exchange* using OIDC can obtain *Attributes* by either requesting claims as part of a scope, or as individual claims as per section 5.5.1 of the OpenID Connect Core 1.0 standard using the `claims` parameter. The claims available to an *Identity Exchange* from *Identity Service Providers* are defined in **Table 16**.

The following scopes are available to an *Identity Exchange* to request from an *Identity Service Provider*:

- `openid`
- `tdif_core`
- `tdif_email`
- `tdif_phone`
- `tdif_other_names`
- `tdif_docs`

These scopes are custom scopes as they have a richer set of *Attributes* than the standard *OIDC* scopes. **Table 22** contains the mapping of these scopes to *Attribute Sets* and the claims that will be returned if the scopes are requested.

Table 22: OIDC Profile for IdPs.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
Common	openid	sub auth_time	ID Token UserInfo	Standard *OIDC* scope.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
		acr		These *Attributes* are returned for any scope requested
Core	tdif_core	name family_name given_name middle_name preferred_username birthdate updated_at tdif_core_updated_at	ID Token UserInfo	Custom scope.
Validated Email	tdif_email	email email_verified tdif_email_updated_at	ID Token UserInfo	Custom scope
Validated Phone	tdif_phone	phone_number phone_number_verified tdif_phone_number_updated_at	ID Token UserInfo	Custom scope
Verified Other Names	tdif_other_names	tdif_other_names tdif_other_names_updated_at	ID Token UserInfo	Custom scope
Verified Documents	tdif_doc	tdif_doc	UserInfo	Custom scope.
	Not applicable	tdif_edi	ID Token	tdif_edi is requested as an individual claim as per section 5.5.1 of the **[OpenID.Core]**

Claims are made available as follows:

- Via an ID Token from the Token Endpoint.
- Via the UserInfo Endpoint.

Claims will generally be available via both endpoints; however some claims are only available from certain endpoints as described above in Table 21. Additional

parameters may be returned as part of the authorisation response as per the *Identity Exchange* to *Identity Service Provider* profile defined in section 3 of the *TDIF 06B – OpenID Connect 1.0 Profile*.

4.2 SAML 2.0 *Attribute* Mapping

The *Attribute* mapping contained in this section can also be found in the *TDIF: 06C SAML 2.0 Profile* [TDIF.SAML]. Where there is inconsistency between this document and [TDIF.SAML] refer to this document for the authority on what the mappings between *Attributes* are.

4.2.1 Design Goals

The design goals for the *SAML* 2.0 *Attribute* mapping are summarised below:

- Simplify protocol translation between *OIDC* and *SAML* by an *Identity Exchange*. Provide straightforward correspondence between the *OIDC* and *SAML* profile.
- Simplify interoperability. Avoid the use of custom *SAML* extensions, use standard built-in XML schema types, and where possible use the *XML* string data type.
- Provide the same functionality for *RPs* regardless of the protocol being used.

4.2.2 SAML *Attribute* Mapping

The following section describes the mapping of *Attributes* described in this document to *SAML* claims. There is no concept of a scope in *SAML* 2.0.

In general, *Attributes* are included in *SAML* 2.0 assertion about a subject in an `<AttributeStatement>` that contains an `<Attribute>` element for each attribute. See Section 2.7.3.1 of the *SAML* core specification [SAMLCore]. The following rules applies for the *Attributes* returned as `<Attribute>` elements:

- The NameFormat XML *Attribute* in `<Attribute>` elements must have the value `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

- A value of the XML *Attribute* FriendlyName is provided for each of the *SAML* 2.0 *Attributes* in this profile. This is only defined for the purposes of readability, it is optional, and it plays no role in processing.
- The XML schema type of the contents of the `<AttributeValue>` must be drawn from one of the types defined Section 3 of [Schema2]. The xsi:type must be present and given the appropriate value.

The Authentication Time *Attributes* uses the standard *SAML* `AuthnInstant` *Attribute* in authentication responses. The time value is encoded in UTC. See Section 2.7.2 of the SAML core specification [SAMLCore].

Table 23: SAML 2.0 *Attribute* Mapping.

Attribute	SAML *Attribute* Name	FriendlyName	XML Type
Full Name	urn:id.gov.au:tdif:name	name	string
Family Name	urn:id.gov.au:tdif:family_name	family_name	string
Given Names	urn:id.gov.au:tdif:given_name	given_name	string
Middle Names	urn:id.gov.au:tdif:middle_name	middle_name	string
Preferred Name	urn:id.gov.au:tdif:preferred_username	preferred_name	string
Date of Birth	urn:id.gov.au:tdif:birthdate	birthdate	string
Core *Attributes* Last Updated	urn:id.gov.au:tdif:core_updated_at	core_updated_at	
Validated Email	urn:id.gov.au:tdif:validated_email	validated_email	string
Validated Email Last Updated	urn:id.gov.au:tdif:validated_email_updated_at	validated_email_updated_at	dateTime
Validated Mobile Phone Number	urn:id.gov.au:tdif:validated_phone_number	validated_phone_number	string
Validated Mobile Phone Number Last Updated	urn:id.gov.au:tdif:validated_phone_number_updated_at	validated_phone_number_updated_at	dateTime
Other Verified Names	urn:id.gov.au:tdif:verified_other_names	verified_other_names	complex

			see Section 3.1.3
Other Verified Names Last Updated	urn:id.gov.au:tdif:verified_other_names_updated_at	verified_other_names_updated_at	dateTime
Verified Documents	urn:id.gov.au:tdif:verified_documents	verified_documents	complex see Section 3.1.4
Authentication Time	AuthnInstant		dateTime
TDIF EDI	urn:id.gov.au:tdif:tdif_edi	tdif_edi	string
myGov LinkID	urn:id.gov.au:tdif:mygov_link_id	mygov_link_id	string

4.3 Mappings between protocols

4.3.1 SAML 2.0 and OpenID Connect 1.0 *Attribute* Mappings

Table 24 details the equivalent *Attributes* in *SAML* 2.0 and OpenID 1.0 Connect for the *TDIF Attributes*.

Table 24: SAML 2.0 and OIDC *Attribute* Equivalents.

Attribute	OIDC Claim Name	SAML *Attribute* Name
Full Name	name	urn:id.gov.au:tdif:name
Family Name	family_name	urn:id.gov.au:tdif:family_name
Given Names	given_name	urn:id.gov.au:tdif:given_name
Middle Names	middle_name	urn:id.gov.au:tdif:middle_name
Preferred Name	preferred_username	urn:id.gov.au:tdif:preferred_username
Date of Birth	birthdate	urn:id.gov.au:tdif:birthdate
Core *Attributes* Last Updated	tdif_core_updated_at	urn:id.gov.au:tdif:core_updated_at
Validated Email	email email_verified=true	urn:id.gov.au:tdif:validated_email
Validated Email Last Updated	tdif_email_updated_at	urn:id.gov.au:tdif:validated_email_updated_at

Validated Mobile Phone Number	phone_number phone_number_verified=true	urn:id.gov.au:tdif:validated_phone_number
Validated Mobile Phone Number Last Updated	tdif_phone_number_updated_at	urn:id.gov.au:tdif:validated_phone_number_updated_at
Other Verified Names	tdif_other_names	urn:id.gov.au:tdif:verified_other_names
Other Verified Names Last Updated	tdif_other_names_updated_at	urn:id.gov.au:tdif:verified_other_names_updated_at
Authentication Time	auth_time	AuthInstant *Attribute* in the <AuthnStatement> element
RP Audit Id	tdif_audit_id	urn:id.gov.au:tdif:tdif_audit_id

Attribute Service Provider Profiles

Attribute Service Providers

Table 25 lists the *Attribute Service Providers* that are currently accredited under the TDIF to provide *Attributes*.

Table 25: Trust Framework Authorisation *Attribute Service Provider*s.

Attribute	*Attribute Service Provider* System/Component	Description
Business Authorisations	RAM. RAM is the system that manages business authorisations. RAM is operated by the Australian Taxation Office (ATO) and is integrated with the ABR that is also operated by the ATO.	RAM manages the authorisation for a *Person* to act on behalf of a business entity that is registered with the Australian Business Register (ABR) and issued with an Australian Business Number (ABN)

5.1 Authorisation *Attributes*

Broadly speaking, in the *TDIF* authorisation refers to the ability for an authenticated *Person* to act on behalf of another entity. For guidance on this *Attribute* class, refer to section 5.1 of the *TDIF: 05A – Role-specific Guidance*.

5.1.1 Logical *Attribute* Data Representation for Authorisations

Table 26 describes the standard *Attribute* profile for authorisations. This lists the *Attributes* which comprise an authorisation in the system. When there is a reference to an entity, this is the *Person*, company, or group that an individual is being authorised to act on behalf of,

Table 26: Logical *Attribute* Data Representation for Authorisations.

Attribute	Format	Mandatory/ Optional
Schemas	List of URNs for the schemas that specify the *Attributes* that describe authorisations. A default value may be specified, in which case this *Attribute* may be optional.element in the response to a Relying Party.	Optional
Unique Relationship ID	Unique identifier for the relationship between the *Person* and the entity. This identifier must uniquely identify the *Person* at the entity.	Mandatory
Entity ID	Unique identifier for the entity	Mandatory
Entity Type	The type of entity.	Mandatory
Entity Name.	The name of the entity. Information about the entity may be separately available from an authoritative entity using the Entity ID.	Optional.
Family Name	The last name for the *Person* at the entity. Required where there is a need to support a *Person* having a name at the entity that is different to the name *Attributes* in their verified identity.	Optional
Given Names	The given names for the *Person* at the entity. Required where there is a need to support a *Person* having a name at the entity that is different to the name *Attributes* in their verified identity.	Optional
Contact Emails	Emails addresses that are specific to the *Person* at the entity. Email addresses MUST conform to RFC 5322 [RFC 5322] address syntax. Depending on the requirements of the authorisation context, an indicator on whether the email address is validated may be included.	Optional
Contact Phone Numbers	Phone numbers that are specific to the *Person* at the entity. Phone numbers. Phone numbers MUST be in E.164 [E.164] format. . Depending on the requirements of the authorisation context, an indicator on whether the phone number is validated may be included	Optional
Contact Addresses	Physical mailing addresses that are specific to the *Person* at the entity. Australian addresses	Optional

Attribute	Format	Mandatory/ Optional
	should be recorded in an AS4590 compliant manner.	
Relationship Type	A literal that identifies the type of the relationship. Each relationship type must have the same process for managing the relationship and the use the same CL and IP levels (or a have defined common minimum. This is analogous to the levels of assurance for creds/identity. It informs the Relying Party on how the *Attributes* were verified and how they were bound to the authentication user.	Mandatory
Relationship Start Time	Date and time in Coordinated Universal Time (UTC) format (ISO 8601) for the commencement of the relationship.	Optional
Relationship End Time	Date and time in Coordinated Universal Time (UTC) format (ISO 8601) for when the relationship will end.	Optional
Roles	List of literals to describe the roles that an authorised *Person* at the entity may perform, e.g. Administrator. These roles are standard roles defined by the *Attribute Service Provider* to support common use-cases and the responsibility and accountability for managing these roles must be clearly defined by the *Attribute Service Provider*.	Optional
Entitlements	Additional access that the *Person* may possess when acting on behalf of the entity. This may be specific to the Relying Party in some authorisation contexts.	Optional
Attributes Last Updated	Date and time in Coordinated Universal Time (UTC) format (ISO 8601) for when the relationship *Attributes* were last updated.	Mandatory

5.1.2 Business authorisations

As a subset of Authorisation *Attributes*, the *TDIF* currently supports the provision of Business Authorisations by an *Attribute Service Provider*. Business Authorisations represent the ability for a *Person* to act on behalf of a business entity that is

registered with the Australian Business Register (ABR) and issued with an Australian Business Number (ABN). A Business Owner is an Authorised *Person* for the business entity that is registered on the ABR. A Business Owner may appoint additional Authorised *Persons*. An Authorised *Person* may appoint additional Business Representatives to act on behalf of the business entity.

The specification of the business *Attributes* that represent business authorisation is based on a pre-existing schema for the RAM system implemented by the ATO.

5.1.2.1 Attribute Profile

The *Attributes* which comprise a business authorisation correspond to those described in the standard *Attribute* profile for an authorisation. The description of each *Attribute* can be found in Table 26.

Table 27: Business authorisations *Attribute Set*

Authorisation Context	*Attribute Set*	*Attributes*	Description
Business Authorisations	Business Authorisations	Unique Relationship ID Entity ID Entity Type Entity Name Contact Emails Relationship Type Relationship Start Time Relationship End Time Roles Entitlements *Attributes* Last Updated	All *Attributes* that specify a business authorisation.

5.1.2.2 Attribute Sharing Policy

Table 28: TDIF *Attribute* sharing policies.

Attribute Set	Consent Requirement	Additional Policy Requirements
Business Authorisations	Every Change	None

5.1.2.3 OIDC Attribute mapping

Table 29 and Table 30 describe the claims and scopes which can be used by a Relying Party to request a Business authorisation as part of an OIDC authentication request.

Claims are made available as follows:

- Via an ID Token from the Token Endpoint.
- Via the UserInfo Endpoint.

Claims will generally be available via both endpoints, future iterations of this *Attribute* profile may restrict the availability of these claims if required. Additional sub-*Attribute*s may be added in future.

Business authorisations are returned to a Relying Party using a single complex JSON Object or String that contains all the business authorisation *Attribute*s. These *Attribute*s are retrieved from the *Attribute Service Provider*.

The `tdif_business_authorisation` claim will be returned by default as a complex JSON type format holding the sub-Attributes specified in section 5.1 of the TDIF: 06D Attribute Profile. Alternatively, the Relying Party can request that it be returned as a string, in which case the attribute is returned as a complex claim in a JSON string representation containing the sub attributes specified in section 5.1 of the TDIF: 06D Attribute Profile. Unless specified otherwise all sub-*Attribute*s listed below are specified by the following schema URN:
`urn:id.gov.au:tdif:authorisations:business:1.0`

Table 29: OIDC business authorisations *Attribute* Profile for RPs.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
Business Authorisations	tdif_business_authorisations	tdif_business_authorisations	ID Token UserInfo	All claims are returned.

Table 30: tdif_business_authorisation claim sub-*Attribute*s

Sub-*Attribute*	JSON *Attribute* name	JSON Type
Unique Relationship ID	id	string
Entity ID	subjectId	string
Entity ID Type	subjectIdType	string
Entity Name	subjectName	string
Contact Details	email	string
Relationship Type	relationshipType	string
Relationship Start Time	startTimestamp	string
Relationship End.Time	endTimestamp	string
Attributes	attributes	tuple array
Roles	roles	string array
Entitlements	permissions	string array
Attributes Last Updated	lastModified	string

The *Attributes* sub-*Attribute* is an array of tuples, with each being a name-value tuple, as described in Table 31.

Table 31: TDIF name-value sub-attribute.

Sub-attribute	JSON *Attribute* name	JSON Type	Schema Reference
Name	name	string	
Value	value	string	

5.1.2.4 Business Authorisations Attribute Example

Table 32 is an example of the `tdif_business_authorisation` claim. All values are indicative only.

Table 32: Business Authorisations *Attribute* Example.

Attribute	Examples

Business Authorisations	Example OIDC Value:
	"tdif_business_authorisations": {
	"id": "2819c223-7f76-453a-919d-413861904646",
	"subjectId": "12123456789",
	"subjectIdType": "ABN",
	"subjectName": "Business Name",
	"email": "theowner@abusiness.com",
	"roles": ["administrator"],
	"relationshipType": "ASSOCIATE",
	"startTimestamp": "2021-07-08T00:00:00+10:00",
	"endTimestamp": "2021-07-28T00:00:00+10:00",
	“attributes”:[
	{
	“name”: “pid”
	“value”:”1234”
	},
	{
	"name": "subId",
	"value": "ABRP:45001242137_50"
	},
	{
	"name": "previousPid",
	"value": null
	},
	{
	"name": "previousSubId",
	"value": null
	}
	],
	"permissions": [
	"TAX_AND_SUPER_SERVICES_PERMISSION/FULL"
	],
	.."lastModified": "2021-07-08T04:58:21.8349992Z"
	}

Attribute Data Representation

The *TDIF* relies on standards and protocols to communicate between the participants in the *Australian Government Digital Identity System*. This requires parties to represent data using the same standardised formats, and these formats are specified below.

Table 33: TDIF *Attribute* data representation.

Attribute	Type	Format	Maximum Length
Full Name	string	1 or more characters	100
Family Name	string	1 or more characters	100
Given Names	string	0 or more characters	100
Middle Names	string	0 or more characters	100
Preferred Name	string	0 or more characters	100
Date of Birth	string	ISO 8601:2004 [ISO 8601:2004] format: YYYY-MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	10
Last Updated	datetime	Date and time in Coordinated Universal Time (UTC) format (ISO 8601).	
Validated Email	string	Email address conforming to RFC 5322 [RFC 5322] address syntax. Maximum length is determined by RFC 2821.	254
Validated Email Last Updated	datetime	Date and time in Coordinated Universal Time (UTC) format (ISO 8601).	
Validated Mobile Phone Number	string	Mobile phone number in E.164 [E.164] format	15
Validated Mobile Phone Number Last Updated	datetime	Date and time in Coordinated Universal Time (UTC) format (ISO 8601).	
Other Verified Names	complex	Multi-valued *Attribute* containing Family Name, Given Names tuples.	

Attribute	Type	Format	Maximum Length
Other Verified Names *Attributes* Last Updated	datetime	Date and time in Coordinated Universal Time (UTC) format (ISO 8601).	
Verified Documents	complex	Multi-valued *Attribute* Detailed in Table 34	
Digital Identity (user identifier)	string	1 or more characters	255
Identity Proofing Level and *Credential Level*	string	1 or more characters. Must be one of the values listed in Table 4 of the *TDIF 06 – Federation Onboarding Requirements*.	
Authentication Time	datetime	Date and time in Coordinated Universal Time (UTC) format (ISO 8601).	
RP Audit Id	string	Universally Unique Identifier (UUID) conforming to RFC 4122 RFC4122	36
TDIF EDI	complex	List of EDIs which are each a string of 1 or more characters.	

6.1 Verified Documents

Table 34: TDIF Verified Documents *Attribute* data representation.

Attribute/sub-attribute	Type	Format	Maximum Length
Document Type Code	String	URN for the document type.	
Document Verification Method	String	Values are “S”, “T”, “V”	1
Document Verification Date	String	Date and time in Coordinated Universal Time (UTC) format	
Document Issuer State	String	Values are “NSW’, “QLD”, “VIC”, “TAS”, “WA”, “SA”, “ACT”, “NT”	3
Document Identifiers	Complex	Multi-valued *Attribute* containing Type-Value tuples	
Type	String	1 or more characters	50
Value	String	0 or more characters	50

Attribute/sub-attribute	Type	Format	Maximum Length
Document Names	Complex	Complex object containing 1 or more of the following sub-*Attributes*.	
Family Name	String	1 or more characters	100
Given Names	String	0 or more characters	100
Family Name 2	String	1 or more characters	100
Given Names 2	String	0 or more characters	100
Middle Name	String	0 or more characters	50
Full Name	String	1 or more characters	100
Document Date of Birth	String	ISO 8601:2004 [ISO 8601:2004] format: YYYY-MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	10
Document *Attributes*	Complex	Multi-valued *Attribute* containing Type-Value tuples	
Type		1 or more characters	
Value		0 or more characters	

Table 35: Document Type Code.

Document Type	Verification Authority	Document Type Code URN	Verification Authority Document Type Code
Birth Certificate	DVS	urn:id.gov.au:tdif:doc:type_code:BC	BC
Change of Name Certificate	DVS	urn:id.gov.au:tdif:doc:type_code:NC	NC
Marriage Certificate	DVS	urn:id.gov.au:tdif:doc:type_code:MC	MC
Citizenship Certificate	DVS	urn:id.gov.au:tdif:doc:type_code:CC	CC
Registration by Descent Certificate	DVS	urn:id.gov.au:tdif:doc:type_code:RD	RD
Immi Card	DVS	urn:id.gov.au:tdif:doc:type_code:IM	IM

Document Type	Verification Authority	Document Type Code URN	Verification Authority Document Type Code
Visa	DVS	urn:id.gov.au:tdif:doc:type_code:VI	VI
Australian Driver Licence	DVS	urn:id.gov.au:tdif:doc:type_code:DL	DL
Medicare Card	DVS	urn:id.gov.au:tdif:doc:type_code:MD	MD
Australian Travel Document	DVS	urn:id.gov.au:tdif:doc:type_code:PP	PP
Centrelink Concession Card	DVS	urn:id.gov.au:tdif:doc:type_code:CO	CO

Table 36: Additional Document Type Codes

Document Type	Document Type Code URN	Jurisdiction/ Sub Type
Australian Driver Licence	urn:id.gov.au:tdif:doc:type_code:DL.NSW	New South Wales
	urn:id.gov.au:tdif:doc:type_code:DL.VIC	Victoria
	urn:id.gov.au:tdif:doc:type_code:DL.QLD	Queensland
	urn:id.gov.au:tdif:doc:type_code:DL.WA	Western Australia
	urn:id.gov.au:tdif:doc:type_code:DL.SA	South Australia
	urn:id.gov.au:tdif:doc:type_code:DL.TAS	Tasmania
	urn:id.gov.au:tdif:doc:type_code:DL.ACT	Australian Capital Territory
	urn:id.gov.au:tdif:doc:type_code:DL.NT	Northern Territory

6.2 *Attribute Service Provider Attribute* data representation

6.2.1 Authorisations

6.2.1.1 Business Authorisations

Table 37: Business Authorisations *Attribute* data representation.

Attribute	Type	Format	Maximum Length
Unique Relationship ID	String	1 or more characters	256
Entity ID	String	Value is the ABN	11
Entity Type	Datetime	Value is “ABN”	3
Entity Name	String	Registered Business Name as recorded on the ABR.	200
Contact Emails	String	Only a single email is provided.	256
Relationship Type	String	1 or more characters.	
Relationship Start Time	String	Date and time in Coordinated Universal Time (UTC) format (ISO 8601)	
Relationship End Time	String	Date and time in Coordinated Universal Time (UTC) format (ISO 8601)	
Roles	List of String	List of strings, where each string is 1 to 256 characters.	
Entitlements	List of String	List of strings, where each string is 1 to 256 characters.	
Attributes Last Updated	String	Date and time in Coordinated Universal Time (UTC) format (ISO 8601)	

Annex A – *Attribute* examples

Table 38: OIDC *Attribute* examples.

Attribute	Examples
Family Name	Example OIDC Value: "family_name": "Moore"
Given Names	Example JWT Value: "given_name": "Trentino Bici"
Date of Birth	Example OIDC Value: "birthdate": "1972-05-06"
Core *Attributes* Last Updated	Example OIDC Value: "tdif_core_updated_at": 1520220048
Validated Email	Example OIDC Values: "email": "tmoore@adomain.com.au" "email_verified": true
Validated Email Last Updated	Example OIDC Value: "tdif_email_updated_at": 1520220048
Validated Mobile Phone Number	Example OIDC Value: "phone_number": “+61444888222” "phone_number_verified": true
Validated Mobile Phone Number Last Updated	Example OIDC Value: "tdif_phone_number_updated_at": 1520220048
Verified Other Names	Example OIDC Value: "tdif_verified_other_names": [{"family_name": "Moore","given_name": "Trentino"},{"family_name": "Moore","given_name": "Trentino Vino"}]
Verified Other	Example OIDC Value: "tdif_verified_other_names_updated_at": 1520220048

Attribute	Examples
Names Last Updated	

Verified Documents	Example OIDC Value:
	"tdif_doc": [{
	/**PASSPORT**/
	"type_code": "urn:id.gov.au:tdif:doc:type_code:PP",
	"verification_method": "S",
	"verification_date": "2019-08-23T06:10:05.7072019",
	"issuer_state": null,
	"names": {
	"family_name": "THIRTYONECHARACTERFAMILYNAMEPAS",
	"given_name": "THIRTYONECHARACTERGIVENNAMEPASS",
	"family_name2": null,
	"given_name2": null,
	"middle_name": null,
	"full_name": null
	},
	"birthdate": "1990-01-01",
	"identifiers": [{
	"type": "Travel Document Number",
	"value": "PP1000013"
	}
	],
	"attributes": [{
	"type": "Gender",
	"value": "Female"
	}
	]
	}, {
	"type_code": "urn:id.gov.au:tdif:doc:type_code:DL",
	"verification_method": "S",
	"verification_date": "2019-08-23T06:10:20.629057",
	"issuer_state": null,
	"names": {
	"family_name": "THIRTYONECHARACTERFAMILYNAMEPAS",
	"given_name": "THIRTYONECHARACTERGIVENNAMEPASS",
	"family_name2": null,
	"given_name2": null,
	"middle_name": null,
	"full_name": null

Attribute	Examples

	},
	"birthdate": "1990-01-01",
	"identifiers": [{
	"type": "Licence Number",
	"value": "1234567"
	}
	],
	"attributes": []
	}, {
	/**MEDICARE**/
	"type_code": "urn:id.gov.au:tdif:doc:type_code:MD",
	"verification_method": "S",
	"verification_date": "2019-08-23T06:10:59.8267464",
	"issuer_state": null,
	"names": {
	"family_name": null,
	"given_name": null,
	"family_name2": null,
	"given_name2": null,
	"middle_name": null,
	"full_name": null
	},
	"birthdate": "1990-01-01",
	"identifiers": [{
	"type": "Card Number",
	"value": "123456789"
	}, {
	"type": "Individual Ref Number",
	"value": "2"
	}
	],
	"attributes": [{
	"type": "Card Type",
	"value": "Green"
	}, {
	"type": "Card Expiry",
	"value": "12-2020"
	}, {
	"type": "Full Name 1",
	"value": "THIRTYONECHARACTERGIVENNAMEPASS"

Attribute	Examples

	}, {
	"type": "Full Name 2",
	"value": "THIRTYONECHARACTERFAMILYNAMEPAS"
	}
	]
	}
	]
	]

RP Audit Id	Example OIDC Value: "tdif_audit_id": “AA97B177-9383-4934-8543-0F91A7A02836”
Authentication Time	Example OIDC Value: “auth_time”: 1520220048

Annex B – Verified Documents attributes

This annex provides additional guidance in relation to the population of the TDIF Verified Documents *Attributes*. Guidance is currently only provided for documents that can be verified using DVS. The DVS Matching specifications and accompanying support documents already provide guidance on how to collect the required *Attributes* from the documents.

Additional guidance for document types not currently supported by DVS can be provided in a future TDIF release.

Table 39 Mapping to DVS Field Names. provides a mapping of the DVS fields values defined in the DVS Match Specifications to the TDIF verified document *Attributes*.

Table 39 Mapping to DVS Field Names.

Attribute/sub-attribute	Description	DVS Field Name	DVS Document Type Code
Document Identifiers			
	Documents with one identifiers	ImmiCard Number	IM
		Licence Number	DL
		Travel Document Number	PP
		Stock Number	CC, RD
		Passport Number	VI
		CRN	CO
	Medicare cards have 2 identifiers	Card Number	MD
		Individual Ref Number	
	Different identifiers are used on BDM issued documents	Registration Number	BC, NC, MC
		Registration Date	
		Registration Year	
		Certificate Number	
Document Names			

Attribute/sub-attribute	Description	DVS Field Name	DVS Document Type Code
Family Name	All document types except cards use Family Name and Given Names.	Family Name	BC, NC, MC, CC, RD, IM, VI, DL, PP
Given Names		Given Name	
Family Name 2	Additional name used by Marriage Certificates	Family Name 2	MC
Given Names 2		Given Name 2	
Middle Name	Currently only used by Driver Licence.	Middle Name	DL
Full Name		Name	CO
Document Date of Birth			
		BirthDate	BC, NC, CC, RD, IM, VI, DL, MD, CO, PP
Document Attributes			
		Date of Event	MC
		Acquisition Date	CC, RD
		Country Of Issue	VI
		State of Issue	DL, MC, BC
		Gender	PP
		Card Type	MD
		CardType	CO
		Card Expiry	MD
		CardExpiry	CO
		Full Name 1	MD
		Full Name 2	MD
		Full Name 3	MD
		Full Name 4	MD

Annex C – Mapping to Role Requirements

Section 3.6 and 3.7 of the *TDIF 05 – Role Requirements* set out the restrictions on what *Attributes* an *Identity Service Provider* can collect and disclose. This annex sets out guidance for *Identity Service Providers* as to the mapping of these restrictions and *Attributes* described in the *TDIF 05 – Role Requirements* to the *Attributes* described in this document.

Some of the *Attributes* described in the *TDIF 05 – Role Requirements* are represented by multiple *Attributes* in this profile, as there may be multiple contexts the same information can be shared in. Similarly, some of the *Attributes* in this Profile may represent multiple *Attributes* described in the *TDIF 05 – Role Requirements*.

Table 40: Mapping of *Attributes* between *TDIF 05 - Role Requirements* and the *TDIF 06D - Attribute Profile*

Attribute in tables 2 & 3 of the *TDIF 05 – Role Requirements*	Corresponding *Attribute(s)* in the *TDIF 06D – Attribute Profile*	Location in section 3 of the *TDIF 06D – Attribute Profile*
All verified names	Full Name	3.1.1
	Family Name	3.1.1
	Given Names	3.1.1
	Middle Names	3.1.1
	Other Verified Names	3.1.3
	Document Names	3.1.4
Verified date of birth as recorded on the *EoI Document*	Date of Birth	3.1.1
	Document Date of Birth	3.1.4
Mobile Phone number	Validated Mobile Phone Number	3.1.2
Email address	Validated Email	3.1.2
EoI Document type name	No current attribute mapped.	
EoI Document type code	Document Type Code	3.1.4
EoI Document issuer	No current attribute mapped.	
EoI Document issuer state	Document Issuer State	3.1.4
EoI Document identifiers	Document Identifiers	3.1.4
Other *EoI Document Attributes*	Document Attributes	3.1.4
	Last Updated	3.1.5

Attribute in tables 2 & 3 of the *TDIF 05 – Role Requirements*	Corresponding *Attribute(s)* in the *TDIF 06D – Attribute Profile*	Location in section 3 of the *TDIF 06D – Attribute Profile*
Date and time Attributes last updated	Core Attributes last updated	3.1.1
	Other Verified Names Attributes Last Updated	3.1.3
Date and time email address was last validated	Validated Email Last Updated	3.1.2
Date and time mobile phone number was last validated (if collected)	Validated Mobile Number Last Updated	3.1.2
Verification method used for each *EoI document* (i.e. S, T, V)	Document Verification Method	3.1.4
Date and time the *EoI document* was verified	Document Verification Date	3.1.4
Identity Proofing Level achieved	Identity Proofing Level	3.1.5
Date and time the *Digital Identity* was created	No current attribute mapped.	
Digital Identity (user identifier)	*Digital Identity* (user identifier)	3.1.5
Preferred name(s)	Preferred name(s)	3.1.1 and 3.5
Residential address	Residential address	3.5
Postal address	Postal address	3.5
Other address (e.g second residential address)	Other address (e.g. second residential address)	3.5
Other phone number (e.g. landline)	Other phone number (e.g. landline)	3.5
Place of Birth	Place of Birth	3.5
Titles (e.g. Dr. Mr, Ms)	Titles (e.g. Dr. Mr, Ms)	3.5