Australian Government
Digital Transformation Agency

06D - Attribute Profile

Trusted Digital Identity Framework Release 4
May 2020, version 1.0

PUBLISHED VERSION

dta

Digital Transformation Agency

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 Participants*, 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 Digital Transformation Agency 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 the Director, Digital Identity Policy at identity@dta.gov.au.

Document management

The *DTA* has endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Jan 20	AV	Initial version
0.2	Mar 20	AV	Minor updates to align with the TDIF Release 4 structure.
1.0	May 20		Published version

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a *TDIF* change management document and published to the *DTA* website.

Contents

List of tables

1 Introduction

This document defines all *Attributes* that can be requested by *Participants* of the *Australian Government's identity federation*. This document will be updated with additional *Attributes* and protocols as the *Australian Government's identity federation* expands in the future.

The intended audience for this document includes:

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

2 Attribute Sets

2.1 Attribute Sets

The *Attributes* passed through the federation are split into Attribute sets. Attribute sets correspond to the logical sets of attributes that a 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 a number of 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	Family Name Given 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 for documents used to verify an identity. Availability of this attribute set may be restricted to specific document types.
Common	RP Audit Id Authentication Time TDIF EDI	Common attributes that are not specific to an Attribute Set. These attributes support the use of attributes by Relying Parties.

Attribute Set	Attributes	Description
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
Validated Mobile Phone Number	Every Change	None
Verified Other Names	Every Change	None
Verified Documents	Every Change	**Relying Party Restricted Attribute.** Relying Party must be authorised to request verified documents. This

Attribute Set	Consent Requirement	Additional Policy Requirements
		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 digital identity eco-system rather than attributes that describe an individual.
Single-use	User consent is required for the attributes every time a user authenticates to a Relying Party.
Ongoing	User 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 user 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 user consent was provided.

2.3 Authorised Attribute Sets

Table 4: Trust Framework attribute sharing policies.

Attribute Set	Relying Parties authorized to request
Core	All
Validated Email	All

Attribute Set	Relying Parties authorized to request
Validated Mobile Phone Number	All
Verified Other Names	All
Verified Documents	Relying Parties approved to request Verified documents as restricted attributes under section 3.6.1 of the *TDIF: 05 Role Requirements*.
Common	Not required.
myGov Link	myGov Member Services
Business Authorisations	All

3 Core Attribute Profile

The Core Attributes are the attributes shared in the federation independent of any attribute providers. It includes the following attribute sets:

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

3.1 Mutual attributes

These are the attributes which both IDPs and 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 identity attributes of the individual.

Table 5: Trust Framework core attributes.

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
Date of Birth	Person's date of birth.	Mandatory
Core Attributes Last Updated	Date and time of when the core attributes for a person where last updated.	Mandatory
Authentication Time	Date and time when the person was authenticated at the Identity Provider.	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
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, Given Names tuples for each of the person's other verified names. The Family Name and Given Names	Optional

	attributes are as defined in the TDIF core attributes.	
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 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.*

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 verify their identity. Table 9: Trust Framework Verified Documents collection. Table 10 details the attributes contained as part of a Verified Document. There can be multiple instances of a Verified Document within the Verified Documents attribute. There can only be one collection attribute (Verified Documents) and within this multiple Verified Documents, each a collection of the verified attributes that a document provides.

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
Document Names	Document names are the person names as 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

Attribute	Description	Mandatory/ Optional
Full Name	Person's full name as recorded on the document.	Optional

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 name of the DVS Field Name defined in the relevant DVS Match Specification.	Mandatory
Value	The value of the attribute as a string.	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 12: 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's identity federation*.

Error! Reference source not found. lists the additional attributes that an Identity Exchange may provide to a RP in response to a request.

Table 13: 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 Link	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[1]. An attribute reference is defined by NIST as:

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

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's identity federation*. When *Computed Attributes* are added to the federation they will be described in this section.

3.5 Self-Asserted Attributes

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

Table 14: Self-Asserted Attributes.

Attribute	Description	Mandatory/ Optional
Preferred name(s)	The preferred name of the user	Optional
Physical Address	The physical address of the user, as asserted by them.	Optional

4 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 attribute mapping contained in this section can also be found in the *TDIF: 06B OpenID Connect 1.0 Profile* [TDIF.OIDC]. Where there is inconsistency between this document and [TDIF.OIDC] refer to this document for the authority on what the mappings between attributes are.

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 the 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 15: OIDC attribute mapping.

Attribute	OIDC Claim	JSON Type	OIDC Standard Reference
Family Name	family_name	string	Section 5.1
Given Names	given_name	string	Section 5.1
Date of Birth	birthdate	string	Section 5.1
Core Attributes Last Updated	tdif_core_updated_at	number	
Validated Email	email	string	Section 5.1
Email Validated Indicator	email_verified The value of this claim must always be true	boolean	Section 5.1
Validated Email Last Updated	tdif_email_updated_at	number	
Validated Mobile Phone Number	phone_number	string	Section 5.1
Mobile Phone Number Validated Indicator	phone_number_verified The value of this claim must always be true	boolean	Section 5.1
Validated Mobile Phone Last Updated	tdif_phone_number_updated_at	number	
Verified Other Names	tdif_other_names	complex type	
Verified Other Names Last Updated	tdif_other_names_updated_at	number	
Verified Documents	tdif_doc	complex type	
Authentication Time	auth_time	number	Section 2
RP Audit Id	tdif_audit_id	string	
TDIF EDI	tdif_edi	string	
myGov LinkID	mygov_link_id	string	
Last Updated	updated_at	number	Section 5.1

Table 16: tdif name sub-attributes.

Sub-attribute	JSON attribute name	JSON Type	Schema Reference
Family Name	family_name	string	
Given Names	given_name	string	

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		
Document Attributes	attributes	complex	

The `names` claim is a complex *JSON* type that contains the sub-attributes listed in Table 18. The identifiers and attributes claims are a *JSON* array that contains zero or more occurrences of the complex *JSON* type that represents a type-value tuple as specified in Table 19

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	

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	Date that any of the core or validated contact details were last updated.

4.1.2 RP OIDC Scopes and Claims

The mapping of attributes to the standard *OIDC* scopes that a *RP* may use to request identity attributes from an *Identity Exchange* is a minimalist attribute profile to maximise interoperability for *RPs* that have simple needs for identity attributes.

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 TDIF attribute profile may restrict the availability of these claims if required. A *Relying Party* can also make requests for individual claims as per section 5.5.1 of the OpenID Connect Core 1.0 standard using the `claims` parameter. This includes making an individual claim request for any restricted attributes that the *Relying Party* has been

authorised to request. The *Relying Party* may also make requests for scopes and claims to be provided by *Attribute Service Providers* as described in section 5 of this document.

Table 21: OIDC Attribute Profile for RPs.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
Core	profile	family_name given_name birthdate	ID Token UserInfo	Standard scope. Only the claims noted are returned.
Validated Email	email	email email_verified	ID Token UserInfo	
Validated Phone	phone	phone_number phone_number_verified	ID Token UserInfo	
Common	Not applicable	tdif_audit_id	ID Token	These attributes are returned for any scope requested
Verified Documents	tdif_doc	tdif_doc	UserInfo	Restricted Attributes. Will only be returned if the Relying Party is approved to receive these attributes.

4.1.3 IdP OIDC Scopes and Claim Requests

Table 22 maps the *TDIF Attribute Sets* to the scopes that an *Identity Exchange* may use to request *Attributes* from an *IdP*. These scopes are custom scopes as they have a richer set of *Attributes* than the standard *OIDC* scopes.

Claims are made available as follows:

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

Requests for individual claims can be made as per section 5.5.1 of the OpenID Connect Core 1.0 standard using the `claims` parameter.

Table 22: OIDC Profile for IdPs.

Attribute Set	OIDC Scope	OIDC Claims	OIDC Claims Support	Comments
Core	tdif_core	family_name given_name birthdate 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.
Common	Not applicable	tdif_edi	ID Token	Requested as an individual claim as per section 5.5.1 of the **[OpenID.Core]**

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
Family Name	urn:id.gov.au:tdif:family_name	family_name	string
Given Names	urn:id.gov.au:tdif:given_name	given_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
Verified Other Names	urn:id.gov.au:tdif:verified_other_names	verified_other_names	complex see Section 3.1.3
Verified Other 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 Link ID	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
Family Name	family_name	urn:id.gov.au:tdif:family_name
Given Names	given_name	urn:id.gov.au:tdif:given_name
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
Verified Other Names	tdif_other_names	urn:id.gov.au:tdif:verified_other_names
Verified Other 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

5 Attribute Provider Profiles

Attribute Providers

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

Table 25: Trust Framework Authorisation Attribute Providers.

Authorisation Context	Attribute 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 Provider to support common use-cases and the responsibility and accountability for managing these roles must be clearly defined by the Attribute 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-attributes may be added in future.

Business authorisations are returned to a Relying Party using a single complex claim that contains all the business authorisation attributes. These attributes are retrieved from the Attribute Provider.

The `tdif_business_authorisation` claim is a complex JSON type that contains the sub-attributes specified in section 6.3.1 of the *TDIF: 06 Federation Onboarding Requirements*. Unless specified otherwise all sub-attributes 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-attributes

Sub-attribute	JSON attribute name	JSON Type
Unique Relationship ID	id	string
Entity ID	subjectId	string
Entity Type	subjectType	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",
	"subjectType": "ABN",
	"subjectName": "Business Name",
	"email": "theowner@abusiness.com",
	"roles": "administrator",
	"relationshipType": "ASSOCIATE",
	"startTimestamp": "2018-06-08T00:00:00+10:00",
	"endTimestamp": "2018-06-28T00:00:00+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": "2018-06-08T00:00:00+10:00"
	}

6 Attribute Data Representation

The *TDIF* relies on standards and protocols to communicate between the participants in the federation. 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
Family Name	String	1 or more characters	100
Given Names	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
Attributes 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.	
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	

Attribute	Type	Format	Maximum Length
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
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-	10

Attribute/sub-attribute	Type	Format	Maximum Length
		MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	
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
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 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.	

Attribute	Type	Format	Maximum Length
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": [{"verification_method": "S", "verification_date": "2010-01-23T04:56:22Z", "type_code": "urn:id.gov.au.tdif:doc:type_code:MD", "identifiers": [{"value": "123456789", "type": "Card Number"}, {"value": "1", "type": "Individual Ref Number"}], "attributes": [{"value": "G", "type": "Card Type"}, {"value": "2018-09", "type": "Card Expiry"}, {"value": "John A Citizen", "type": "Full Name 1"}] }]
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
Document Attributes			
		Date of Event	MC
		Acquisition Date	CD, 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