Australian Government
Digital Transformation Agency

Attribute Profile

Trusted Digital Identity Framework
March 2019, version 1.4

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

Conventions

TDIF documents refenced by this document are denoted in italics. For example, *TDIF: Overview and Glossary* is a reference to the TDIF document titled Overview and Glossary.

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *TDIF: Overview and Glossary.*

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties accessing this document or have questions or comments regarding this document please email the Director, Digital Identity Policy at identity@dta.gov.au.

Document Management

The TDIF Accreditation Authority has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Jan 2018	TM	Initial version
0.2	Jan 2018	TM	Revision prior to release for comment.
0.3	Feb 2018	TM	Revision to align with Trust Framework release 2.
0.3	Feb 2018	TM	Revision from internal review.
0.5	Mar 2018	TM	Added auth_time, tdif_audit_id attributes. Revised examples.
0.6	Mar 2018	TM	Moved to updated TDIF template.
0.7	Jun 2018	TM	Revision following consultation with key stakeholders.
1.0	Aug 2018		Approved for release by the Commonwealth GovPass Authority
1.1	Aug 2018	TM	Added business authorisations attributes.
1.2	Aug 2018	TM	Updates following internal review. Added verified other names attribute.
1.3	Dec 2018	TM	Added verified document details attributes.
1.4	Mar 2018	TM	Incorporated feedback from stakeholders and public consultation.

Contents

1 Introduction

Agencies and organisations that apply to be accredited under the TDIF undergo a series of rigorous evaluations across all aspects of their identity service operations. The *TDIF: Accreditation Process* requires Applicants to demonstrate their identity service is usable, privacy enhancing and is secure and resilient to cyber threats. The intent of these evaluations is to determine whether the Applicant's identity service meets the TDIF Guiding Principles[1] and whether it is suitable to join the identity federation.

This document forms part of the technical integration requirements that Applicants are required to meet in order to achieve and maintain TDIF accreditation.

The intended audience for this document includes:

Applicants and Accredited Providers.
Relying Parties.
TDIF Accreditation Authority.

1.1 Purpose

The purpose of this document is to provide:

- The logical attributes that are shared between Relying Parties (RP) and Identity Providers (IdP) via an Identity Exchange.
- Any policies that govern the sharing of these attributes, such requirements for user consent.
- The technical specifications for these logical attributes.
- The mapping of these attributes to the federation standards that used to share these attributes.

The document provides attribute mappings for OpenID Connect 1.0 and SAML 2.0.

[1] See *TDIF: Overview and Glossary* for further information on the TDIF guiding principles.

1.2 Relationship to other TDIF documents

This document should be the read in conjunction with the following TDIF documents:

- *TDIF: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.
- *TDIF: Architecture Overview,* which provides an architecture overview that describes the functions of the participants and how they interact with each other.
- *TDIF: Technical Requirements,* which provides the core technical requirements for each participant in the TDIF architecture.
- *TDIF: OpenID Connect 1.0 Profile* specifies how the OpenID Connect 1.0 standards can be used to support authentication interactions.
- *TDIF: SAML 2.0 Profile* specifies how the SAML 2.0 standards can be used to support authentication interactions.

The functional requirements for an Identity Service Provider are defined in the *TDIF: Identity Proofing Requirements.*

2 Logical Attribute Profile

2.1 Overview

The core attributes of a person's identity are their full name and date of birth. Core attributes are populated from the identity documents that used by an IdPto verify the identity attributes. An IdP will generally also use a validated email address and/or mobile phone number to manage contact with a person and these may also be shared with RPs.

Some attributes are mandatory and must be provided by an IdP, some attributes are optional. Additional attributes will be added in the future to support the needs of RPs, subject to the consultation processes that support the development of the TDIF. Examples of additional attributes for future consideration may include:

- Computed attributes (i.e. attribute assertions).
- Additional attributes to support RPs that have a clear and justifiable need to establish uniqueness of identity in their service provision context.
- Additional name attributes to improve the effectiveness of identity matching at RPs.
- Additional contact details attributes.

2.2 Attributes

2.2.1 Core Attributes

Table 1 lists the core attributes that defined by the TDIF. These attributes are sourced by an IdP from the Evidence of Identity (EOI) that was used to achieve the Legitimacy Objective of the *TDIF: Identity Proofing Requirements*.

An IdP:
MUST provide a mandatory attribute.
MAY provide an optional attribute.
An Identity Exchange **MUST** support the sharing of all attributes.

Table 1: 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

2.2.2 Validated Contact Details Attributes

Table 2 Lists the validated contact details attributes that defined by the TDIF. These attributes are sourced from an IdP.

An IdP:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.
- An Identity Exchange **MUST** support the sharing of all attributes.

Table 2: 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

2.2.3 Other Verified Names Attributes

Table 3 lists the other verified name attributes that defined by the TDIF. These attributes are sourced by an IdP from the Evidence of Identity (EOI) documents that was used to achieve the Legitimacy Objective of the *TDIF: Identity Proofing 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:

- Approved CoI documents.
- Approved Photo ID documents.
- Approved Linking documents.

An IdP:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.
- An Identity Exchange **MUST** support the sharing of all attributes.

Table 3: 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 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

2.2.4 Verified Document Attributes

Table 4 lists the other verified document attributes that defined by the TDIF. These attributes are sourced by an IdP from the Approved Evidence of Identity (EOI) documents of the *TDIF: Identity Proofing Requirements*. These attributes are only sourced from the following document types:

- Approved CoI documents.
- Approved Photo ID documents.
- Approved UitC documents.
- Approved Linking documents.

An IdP:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.
- An Identity Exchange **MUST** support the sharing of all attributes.

Table 4: 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 attributes that a document provides. Table 5 details the attributes contained in this collection. There can be multiple instances of the Verified Documents attribute.

Table 5: 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 verification.	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. Each document identifier is a Type-Value Tuple as described in **Table 7**.	Mandatory
Document Names	Document names are the person names as recorded on the document. The format varies according to the document type. The sub-attributes for document names are described in **Table 6**	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. Each document attribute is a Type-Value Tuple as described in **Table 7**.	Optional

Table 6: 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

Attribute	Description	Mandatory/ 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

Table 7: 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

2.2.5 Additional Identity Exchange Attributes

Additional attributes are supplied by an Identity Exchange to support the operation of the digital identity ecosystem.

Table 8 lists the additional attributes that an Identity Exchange may provide to a RP in response to a request. Table 9 details the data representation of TDIF attributes.

An Identity Exchange:

- **MUST** provide a mandatory attribute.
- **MAY** provide an optional attribute.

Table 8: 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

2.2.6 Attribute Data Representation

Table 9: Trust Framework 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
Core Attributes Last Updated	Datetime	Date and time in Coordinated Universal Time (UTC) format	
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	
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	
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	
Verified Documents	Complex	Detailed in **Table 10**	
Authentication Time	Datetime	Date and time in Coordinated Universal Time (UTC) format	
RP Audit Id	String	Universally Unique Identifier (UUID) conforming to RFC 4122 RFC4122	36

Table 10: Trust Framework Verified Documents attribute data representation.

Attribute/sub-attribute	Type	Format	Maximum Length
Document Type Code	String	URN for the document type. See Annex B Verified Documents for the supported document types.	
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-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	

2.2.7 Attribute Sets

Not all attributes are requested individually by a RP. 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. This description 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 11: 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	Common attributes that are not specific to an Attribute Set. These attributes support the use of attributes by Relying Parties.

2.2.8 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 a RP. The key element of these policies relate to the operation of user consent. The different types of consent are detailed in Table 12. User consent requirements must be explicitly met for each RP that requests attributes, in other words the user provides the required consent per RP. The TDIF may require additional policy requirements that must be met. An example is attributes that are only available to specific RPs. The additional policy requirements may also further qualify the operation of user consent by specifying the maximum duration for which a user consent can be remembered.

An Identity Exchange acts as an enforcement point for Attribute Sharing Policies. An accredited provider of attributes, such an Identity Provider or Attribute Provider, can rely on an Identity Exchange to implement the required Attribute Sharing Policies for the attributes it provides.

Table 12: 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..

An Identity Exchange **MUST** implement the attribute sharing policies that are detailed in Table 13. The policies described apply to all the attributes in the Attribute Set regardless of whether the RP has requested an Attribute Set and any of the attributes are contained in an Attribute Set. If RP request an Attribute Set then user consent must be provided for the entire collection of attributes that it contains.

Table 13: 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	Single-use	**Relying Party Restricted Attribute**. Relying Party must be authorised to request verified documents. This authorisation may be restricted to specific document types.
Common	Not Applicable	Not Applicable

2.2.8.1 Relying Party Restricted Attributes

Attribute sets that contain significant sensitive personal information, or represent potential privacy and security risks due to a unauthorised access are available on a restricted basis to Relying Parties that can demonstrate:

- An existing policy mandate. The Relying Party is able to provide evidence of their legislative and legal requirements and how they will be satisfied by receiving these additional attributes.
- An existing business need to collect and/or use these attributes. The attributes disclosed to the Relying Party cannot exceed those normally collected by the IdP during its normal course of business.
- Existing security risk mechanisms are in place to manage and protect these attributes.

The TDIF requirements to be satisfied with regard to Relying Party Restricted Attributes is available in *TDIF: Accreditation Process* (v1.3, Mar 2019) at Annex F. The ability for a Relying Party to request and receive these restricted attributes will be managed by the TDIF Oversight Authority.

2.2.9 Computed Attributes (Attribute References)

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 a person's age or an indicator that person is above at certain age. This need can be supported by providing a Computed Attribute that is derived from the person's date of birth attribute.

Computed attributes are supplied by an IdP, by an Attribute Provider, or by 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.

An Identity Exchange, Attribute Provider, or IdP **MAY** define support for additional computed attributes that derived from the attributes in an Attribute Set. The attribute sharing policies for a computed attribute must be consistent with the attribute sharing policies of the attributes that it is derived from.

In accordance with the *TDIF: Privacy Requirements*, an Identity Exchange **MUST** only disclose the minimum requirements for the Relying Party transitions. An Identity

Exchange **MUST** support additional computed attributes in order to meet this requirement. An Identity Exchange **MAY** source the computed attribute from an Attribute Provider or IdP.

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."*

2.2.10 Levels of Assurance

Levels of Assurance (LoA) are special attributes used to describe the level of assurance described in the TDIF. Levels of Assurance are commonly used mechanism to describe the degree of confidence in an authentication process. The TDIF describes 2 Levels of Assurance.to represent the degree of confidence in the identity proofing process and the degree of confidence in the credentials used to share attributes.

Table 14: Trust Framework Levels of Assurance.

LofA	Description
Identity Proofing Level (IP)	Level of identity assurance associated with the core attributes. There are four levels of identity proofing assurance defined in the TDIF.
Credential Level (CL)	Levels indicate the strength of the credential used to authenticate. There are three levels of credential assurance defined in the TDIF.

In federation protocols LoAs are typically represented using values of an Authentication Context Class Reference, commonly referred to as an acr. The concept of Authentication Context Class is defined in both the SAML 2.0 and OpenID Connect 1.0 standards. In the TDIF technical integration standards URNs are used to define each of the assurance levels. The URNs are the permissible combinations of the Identity Proofing LoA and Credential Level LoA defined by the TDIF. A request for a valid combination in the table below is also satisfied by any combination that is ranked higher than it.

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

Table 15: Level of Assurance Combinations.

Identity Proofing Level	Credential Level	URN	Ranking (Lowest to Highest)
IP1	CL1	`urn:id.gov.au:tdif:acr:ip1:cl1`	1
	CL2	`urn:id.gov.au:tdif:acr:ip1:cl2`	2
	CL3	`urn:id.gov.au:tdif:acr:ip1:cl3`	3
IP2	CL2	`urn:id.gov.au:tdif:acr:ip2:cl2`	4
	CL3	`urn:id.gov.au:tdif:acr:ip2:cl3`	5
IP3	CL2	`urn:id.gov.au:tdif:acr:ip3:cl2`	6
	CL3	`urn:id.gov.au:tdif:acr:ip3:cl3`	7
IP4	CL3	`urn:id.gov.au:tdif:acr:ip4:cl3`	8

3 Technical Attribute Profiles

The technical attribute profiles provide the mapping of the logical attributes to the federation protocols used by the TDIF technical integration requirements. Attribute profiles are provided for the following standards:

- OpenID Connect 1.0 (OIDC).
- SAML 2.0.

3.1 OpenID Connect 1.0 Attribute Profile

3.1.1 Mapping attributes to OIDC

Broadly speaking:

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

3.1.2 Design Goals

The design goals for mapping the Attribute Profile to the OIDC specification are summarised for IdPs and RPs below:

3.1.2.1 Design goals for IDPs

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.

3.1.2.2 Design goals for RPs

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.

3.1.3 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.

Table 16: 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.

3.1.4 OIDC Attribute Mapping

Table 17 describes the mapping of the TDIF attributes to OIDC claims. All claims are standard OIDC claims with the exception of claims that are prefixed with `tdif`. For standard claims a reference to the applicable section of the OpenID Connect 1.0 Core standard is provided.

Table 17*:* 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_last_updated`	`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`	

Attribute	OIDC Claim	JSON Type	OIDC Standard Reference
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`	
Last Updated	`updated_at`	`number`	Section 5.1

The `tdif_other_names` claim is a JSON array that contains 1 or more occurrences of the sub-attributes specified in Table 18. Unless specified otherwise all sub-attributes listed below are as specified in Table 17.

Table 18: tdif name sub-attributes.

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

The `tdif_doc` claim is a JSON array that contains 1 or more occurrences of the sub-attributes specified in Table 19.

Table 19: 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 State	`state`	`strong`	
Document Identifiers	`identifiers`	`complex`	
Document Names	`names`	`complex`	
Document Date of Birth	`birthdate`		

Sub-attribute	JSON attribute name	JSON Type	Schema Reference
Document Attributes	attributes	complex	

The names claim is a complex JSON type that contains the sub-attributes. 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 20

Table 20: 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 21: Tdif type-value sub-attribute.

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

3.1.4.1 OIDC Attribute Profile for RPs

3.1.4.1.1 RP OIDC Scopes

Table 22 maps the TDIF attribute sets to the standard OIDC scopes that a RP may use to request identity attributes from an Identity Exchange. This 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 attribute profile may restrict the availability of these claims if required.

An Identity Exchange **MUST** support all these scopes.

Table 22: 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

In addition to the standard OIDC scopes defined in Table 22, an Identity Exchange **MUST** support all the scopes defined for IdPs in section 3.1.4.2.1 . This makes the full set of attributes available to RPs in addition to the standard OIDC attributes.

3.1.4.2 OIDC Attribute Profile for IdPs

3.1.4.2.1 IdP OIDC Scopes and Claim Requests

Table 23 maps the TDIF attribute sets to the scopes that an Identity Exchange may use to request identity 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.

Claims will generally be available via both endpoints, future iterations of this attribute profile may restrict the availability of claims if required.

An Identity Provider **MUST** support all these scopes.

Table 23: 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.

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.

An Identity Provider **MUST** support individual claim requests for the following claims:

- `tdif_doc.` An Identity Provider must also support individual claim request for a specific document type using the standard OIDC members in the JSON object that requests the claim as specified in Table 24. The valid values for type_code are specified in Annex B Verified Documents attributes

Table 24 Individual claim requests for specific document types.

JSON Object Member	Value	Matching rule
value	A `type_code` URN	This requests the `tdif_doc claim` is returned for all verified documents that match the value of the `document_type_code`
values	A set of `type_code` URNs	This requests the `tdif_doc claim` is returned for all verified documents that match any of the `document_type_code` values.

An example of a request for single document type:

```
"tdif_doc": {"value": "urn: id.gov.au.tdif:doc:type_code:MD"}
```

An example for a request for multiple document types:

```
"tdif_doc": {"value": ["urn: id.gov.au.tdif:doc:type_code:BC",
"urn:id.gov.au.tdif:doc:type_code:IM", "urn: id.gov.au.tdif:doc:type_code:CC",
"urn:id.gov.au.tdif:doc:type_code:VI"]}
```

3.2 SAML 2.0 Attribute Profile

3.2.1 Mapping attributes to SAML 2.0

The SAML 2.0 Attribute Profile defines the expression of TDIF attributes as SAML attribute names and values.

3.2.2 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.

3.2.3 SAML 2.0 Attribute Mapping

This profile defines the mapping of the TDIF attributes into specific attribute names. 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 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]**.

An Identity Exchange **MUST** support all attributes, with the exception of the RP Audit Id attributes.

An IdP **MUST** support all attributes.

Table 25: 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 3.2.3.1
Verified Other Names Last Updated	urn:id.gov.au:tdif:verified_other_names_updated_at	verified_other_names_updated_at	dateTime

Attribute	SAML Attribute Name	FriendlyName	XML Type

Verified Documents	`urn:id.gov.au:tdif:verified_documents`	`verified_documents`	`complex`
			`see Section 3.2.3.1`

Authentication Time	`AuthnInstant`		`dateTime`

3.2.3.1 Mapping complex objects to SAML attributes

It is difficult to map complex objects to SAML attributes in a way that can be guaranteed to be interoperable with Relying Parties as many implementations can only handle elements that contain simple XML types, not nested XML elements.

Where the object is multi-valued, but each value is a simple XML type, then multiple <AttributeValue> elements are to used for each value. An example is shown below:

JSON example:

```
"example_attr": [
   "value1",
   "value2"
]
```

SAML equivalent:

```
<saml:Attribute
NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
Name=”urn.id.gov.au:tdif:example_attr” FriendlyName=”example_attr”>
   <saml:AttributeValue xsi:type="xs:string">value1</saml:AttributeValue>
   <saml:AttributeValue xsi:type="xs:string">value2</saml:AttributeValue>
</saml:Attribute>
```

The following approach MUST be used for complex objects that have nested elements:

- Where there is at most one instance of the complex object, then the contents of the complex object may be flattened into separate SAML attributes where the name of the attribute is qualified with xml namespace that is the extension namespace for TDIF attributes. See an example of this approach at http://www.simplecloud.info/specs/draft-scim-saml2-binding-02.html#anchor5
- Where there is one or more instances of the complex object then the JSON representation of the component object as defined by this specification may be included as the <AttributeValue> element as a XML string.

These approaches are illustrated in the following examples:

JSON example:

```
"example_attr": {
  "attr1":"value1",
  "attr2": {
    "childattr1": "value2"
  }
}
```

SAML Equivalent using flattened attributes.

```
<saml:AttributeStatement
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:tdif="urn:id.gov.au:tdif">
   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified" Name="TDIF.example_attr.attr1">
      <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">value1</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified" Name="TDIF.example_attr.attr2.childattr1">
      <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">value2</saml:AttributeValue>
   </saml:Attribute>
</saml:AttributeStatement>
```

SAML Equivalent using embedded JSON object as a string. Not that the string must be encoded.so that XML special characters are escaped.

```
<saml:Attribute
NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”
Name=”urn.id.gov.au:tdif:exmaple_attr” FriendlyName=”example_attr”>
   <saml:AttributeValue
xsi:type="xs:string">{&quot;attr1&quot;:&quot;value1&quot;,&quot;attr2&quot;:{&quot;
childattr1&quot;:&quot;value2&quot;}}</saml:AttributeValue>
</saml:Attribute>
```

3.3 SAML 2.0 and OpenID Connect 1.0 Attribute Equivalents

Table 26 details the equivalent attributes in SAML 2.0 and OpenID 1.0 Connect for the TDIF attributes.

Table 26: 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

Attribute	OIDC Claim Name	SAML Attribute Name
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

4 Authorisation Attributes

4.1 Overview

Broadly speaking, in the TDIF authorisation refers to the ability for an authenticated person to act on behalf of another entity. Types of authorisations include:

- The authorisation for person to act on behalf of a non-person or organisational entity.
- The authorisation for a non-person or organisational entity to act on behalf of a person.
- The authorisation for a person to act on behalf of another person.

This version of the *TDIF: Attribute Profile* only considers the authorisation for a person to act on behalf of a non-person or organisational entity. It specifically deals with entities that are a registered business on the Australian Business Register (ABR) and have been issued with an Australian Business Number (ABN).

In general:

- Authorisation attributes are managed by an accredited Attribute Provider.
- An Attribute Provider is integrated with an Identity Exchange as a Relying Party. This enables a person to authenticate to the Attribute Provider using their chosen Identity Provider in order to:
  - Establish authorisation attributes and associate them to their digital identity.
  - Manage authorisation attributes.
- An Identity Exchange is integrated with the Attribute Provider to enable the retrieval of the authorisation attributes. These authorisation attributes can then be shared with Relying Parties so that the authorisation can be used by the person to access services at the Relying Party.

The technical integration of the Identity Exchange and Attribute Provider is outside the scope of this document. This details the authorisation attributes that may be shared with Relying Parties.

Detailed requirements relating to Attribute Providers is defined in *TDIF: Attribute Provider Requirements.*

Technical requirements that relate to Attribute Providers and their integration with an Identity Exchange is defined in *TDIF: Technical Requirements.*

4.2 Logical Attributes

4.2.1 Logical Attribute Data Representation for Authorisations

Table 27 provides a logical representation of the attributes that describe authorisation that a person has to act on behalf of an organisational or non-person entity. The term relationship refers to the association between the person and the entity.

Table 27: 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. To avoid conflict with the *TDIF Privacy Requirements*, a different value for this identifier must be sent to each Relying Party, i.e. it must be pairwise unique.[3] [4]	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.

[3] See *TDIF Privacy Requirements*, section 2.11 Government Identifiers

[4] This appears to be in conflict with some existing practices that relate to the use of the AUSkey credentials to enable access to government services. At the time of writing, a Privacy Impact Assessment covering the use of these business authorisation attributes has not been completed so no permissible variation to this requirement for pairwise uniqueness, and any additional policy conditions that may govern its use, has been established.

Attribute	Format	Mandatory/ 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 should be recorded in an AS4590 compliant manner.	Optional
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 for the commencement of the relationship.	Optional
Relationship End Time	Date and time in Coordinated Universal Time (UTC) format 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 for when the relationship attributes were last updated.	Mandatory

This logical representation is implemented by an Attribute Provider that provides authorisations for a specified collection of entities and relationships. The collection of entities and relationships that an Attribute Provider supports is termed the Authorisation Context.

The Attribute Provider may provide additional attributes to support the needs of the Authorisation Context that it supports.

4.2.2 Authorisation Contexts.

Table 28 Defines the Authorisation Contexts that are supported by the Trust Framework.

Table 28: Trust Framework Authorisation Contexts.

Authorisation Context	Description
Business Authorisations	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.

An Authorisation Context is supported by only one Attribute Provider. This does not preclude another provider supporting the same collection of entities and relationship, just that for the purposes of this specification only one Attribute Provider implements a defined Authorisation Context.

4.3 Attribute Providers

Table 29 lists the Attribute Providers that are accredited under the TDIF to provide authorisation attributes.

Table 29: 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)

4.4 Business Authorisation Attribute Profile

4.4.1 Attributes

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

Table 30: Trust Framework 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)	

4.4.2 Attribute Sets

Consistent with Section 0, Attribute Sets are defined for the attributes that support an Authorisation Context.

Table 31: Trust Framework attribute sets.

Authorisation Context	Attribute Set	Attributes	Description
Business Authorisations	Business Authorisations	All attributes	All attributes that specify a business authorisation.

4.4.3 Attribute Sharing Policies

A person may represent more than one registered business. This version of the Attribute Profile assumes that a single business authorisation relationship (i.e. one ABN) is shared with a Relying Party during an authentication interaction. Support for the sharing a multiple business relationship (multiple ABNs) is under consideration for future releases.

To enable this, the Identity Exchange provides a mechanism for the person to view and select the business entity that they are wishing to represent when accessing a Relying Party. This selection is effectively providing the user consent for the business attributes to be shared with the Relying Party.

Additional attribute sharing policy requirements are detailed below:

The Attribute Provider **MUST** ensure that only business authorisations attributes that are relevant to Relying Party that has requested the business authorisation attributes are shared with the Relying Party. This requirement requires filtering the business attributes that are provided to the Identity Exchange to exclude:

- Entire business authorisation relationship that are not relevant, i.e. filtering out business relationships for business entities that have no interactions or relevance to the Relying Party.
- Any specific attribute values that may be Relying Party-specific. For example, values of the Entitlements attribute will generally be specific to a Relying Party.

4.4.4 Relationship Types, Roles and Levels of Assurance

An Attribute Provider is required to provide a practice statement for the attributes that it provides to the identity federation. For business authorisations this practice statement describes the business process that is used by the Attribute Provider to establish and maintain each type of relationship and the associated levels of credential and identity assurance that are used in this process.

The following table is non-normative and is indicative only of the relationship types that may be supported. It is included in this document only to illustrate the operation of the business authorisation attributes.

Table 32: Business Authorisation Relationship Types (Illustrative Only).

Relationship Type	Description	Levels of Assurance
Business Owner	The owner of a registered business authentication using a digital identity and their verified identity attributes is matched against the business owner details recorded on the ABR for the claimed ABN	The Business Owner is authentication with a minimum identity assurance level of IP2.
Business Representative	An Authorised Person authenticates and grants a business representative the right to act on behalf of the ABN. RAM generates a short-lived, single-use authorisation code that is provided out-of-band to the business representative. The business representative authenticates using their digital identity and provides the authorisation code. The verified identity attributes of the business representative are used to confirm that the intended person has accepted the authorisation.	The Authorised Person is an authenticated with a minimum identity assurance level of IP2. The Business Representative is authenticated with a minimum identity assurance level of IP2.

The authoritative source of the supported relationship types and the associated assurance levels is the practice statement published by the Attribute Provider. Additional relationship types may be added to the illustrative ones described above. An example is the use of a digital identity at IP3 by the business owner to register a business entity. This would result in an increased level of assurance for business owner relationship type and thus it may need to be identified as a distinct relationship type so that Relying Parties can recognise the increased level of trust in the business authorisation attributes.

4.5 Business Authorisation Technical Attribute Provider Profile

4.5.1 Overview

This profile specifies that attributes that are made available to Relying Parties via the Identity Exchange. For this version only an OpenID Connect 1.0 profile is provided.

An Identity Exchange may provide an XML equivalent schema for Relying Parties that integrate using the SAML 2.0 standard.

4.5.2 OIDC Attribute Mapping

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

Table 33: OIDC Business Authorisations Attribute Mapping.

Attribute	OIDC Claim	JSON Type
Business Authorisations	`tdif_business_authorisations`	`Complex type`

The `tdif_business_authorisation` claim is a complex JSON type that contains the sub-attributes specified in Table 34. 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 34: tdif_business_authorisation claim sub-attributes

Sub-attribute	JSON attribute name	JSON Type	Schema Reference
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`	

Sub-attribute	JSON attribute name	JSON Type	Schema Reference
Relationship End.Time	endTimestamp	string	
Roles	Roles	string array	
Entitlements	permissions	string array	
Attributes Last Updated	lastModified	string	

Additional sub-attributes may be added in future.

A Relying Party **MUST NOT** throw an error if additional sub-attributes are returned.

The Attribute Provider **MUST** publish the JSON schema for any attributes it provides. This schema must enumerate the valid values for any attributes that have a defined set of values, for example, the valid values for the `relationshipType` attribute.

4.5.3 RP OIDC Scopes

Table 35 maps the TDIF attribute sets to the standard OIDC scopes that a RP may use to request Business Authorisation attributes from an Identity Exchange.

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.

An Identity Exchange that integrates with the Attribute Provider for Business Authorisations **MUST** support all these scopes.

Table 35: OIDC 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.

4.5.4 Business Authorisations Attribute Example

Table 36 is an example of the `tdif_business_authorisation` claim. All values are indicative only.

Table 36: 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": "Business Owner",`
	`  "startTimestamp": "2018-06-08T00:00:00+10:00",`
	`  "endTimestamp": "2018-06-28T00:00:00+10:00",`
	`  "permissions": [`
	`    "TAX_AND_SUPER_SERVICES_PERMISSION/FULL"`
	`  ],`
	`.."lastModified": "2018-06-08T00:00:00+10:00"`
	`}`

Annex A – Attribute examples

Table 37 below provides an example of each TDIF attribute in SAML 2.0 and OIDC.

Table 37: SAML and OIDC attribute examples.

Attribute	Examples

Family Name	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:family_name” FriendlyName=”family_name”> <saml:AttributeValue xsi:type="xs:string">Moore</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"family_name": "Moore"`

Given Names	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:given_name” FriendlyName=”given_name”> <saml:AttributeValue xsi:type="xs:string">Trentino Bici</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example JWT Value:
	`"given_name": "Trentino Bici"`

Date of Birth	Example OIDC Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:birthdate” FriendlyName=”birthdate”> <saml:AttributeValue xsi:type="xs:string">1972-05-06</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"birthdate": "1972-05-06"`

Core Attributes Last Updated	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:core_updated_at” FriendlyName=”core_updated_at”> <saml:AttributeValue xsi:type="xs:dateTime">2018-03-05T03:20:48Z </saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_core_updated_at": 1520220048`

Attribute	Examples

Validated Email	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:validated_email” FriendlyName=”validated_email”> <saml:AttributeValue xsi:type="xs:string">tmoore@adomain.com.au</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Values:
	`"email": "tmoore@adomain.com.au"`
	`"email_verified": true`

Validated Email Last Updated	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:validated_email_updated_at” FriendlyName=”validated_email_updated_at”> <saml:AttributeValue xsi:type="xs:dateTime">2018-03-05T03:20:48Z </saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_email_updated_at": 1520220048`

Validated Mobile Phone Number	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:validated_mobile_phone_number” FriendlyName=”validated_mobile_phone_number”> <saml:AttributeValue xsi:type="xs:string">+61444888222</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"phone_number": “+61444888222”`
	`"phone_number_verified": true`

Validated Mobile Phone Number Last Updated	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:validated_phone_number_updated_at” FriendlyName=”validated_phone_number_updated_at”> <saml:AttributeValue xsi:type="xs:dateTime">2018-03-05T03:20:48Z </saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_phone_number_updated_at": 1520220048`

Attribute	Examples

Verified Other Names	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:verified_other_names” FriendlyName=”verified_other_names”> <saml:AttributeValue xsi:type="xs:string">[{&quot;family_name&quot;: &quot;Moore&quot;,&quot;given_name&quot;: &quot;Trentino&quot;},{&quot;family_name&quot;: &quot;Moore&quot;,&quot;given_name&quot;: &quot;Trentino Vino&quot;}]</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_verified_other_names": [{"family_name": "Moore","given_name": "Trentino"},{"family_name": "Moore","given_name": "Trentino Vino"}]`

Verified Other Names Last Updated	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:verified_other_names_updated_at” FriendlyName=”verified_other_names_updated_at”> <saml:AttributeValue xsi:type="xs:dateTime">2018-03-05T03:20:48Z </saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_verified_other_names_updated_at": 1520220048`

Attribute	Examples

Verified Documents	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri”`
	`Name=”urn.id.gov.au:tdif:verified_documents”`
	`FriendlyName=”verified_documents”>`
	`<saml:AttributeValue xsi:type="xs:string> [{`
	`&quot;verification_method&quot;: &quot;S&quot;,`
	`    &quot;verification_date&quot;: &quot;2010-01-`
	`23T04:56:22Z&quot;,`
	`    &quot;type_code&quot;:`
	`&quot;urn:id.gov.au.tdif:doc:type_code:MD&quot;,`
	`    &quot;identifiers&quot;: [`
	`      {&quot;value&quot;: &quot;123456789&quot;,`
	`       &quot;type&quot;: &quot;Card Number&quot;},`
	`      {&quot;value&quot;: &quot;1&quot;,`
	`       &quot;type&quot;: &quot;Individual Ref Number&quot;}],`
	`    &quot;attributes&quot;: [`
	`      {&quot;value&quot;: &quot;G&quot;,`
	`       &quot;type&quot;: &quot;Card Type&quot;},`
	`      {&quot;value&quot;: &quot;2018-09&quot;,`
	`       &quot;type&quot;: &quot;Card Expiry&quot;},`
	`      {&quot;value&quot;: &quot;John A Citizen&quot;,`
	`       &quot;type&quot;: &quot;Full Name 1&quot;}]`
	`  }]</saml:AttributeValue>`
	`</saml:Attribute>`
	
	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"}]`
	`  }]`

Attribute	Examples

RP Audit Id	Example SAML Value:
	`<saml:Attribute`
	`NameFormat=”urn:oasis:names:tc:SAML:2.0:attrname-format:uri” Name=”urn.id.gov.au:tdif:tdif_audit_id” FriendlyName=”audit_id”> <saml:AttributeValue xsi:type="xs:string">AA97B177-9383-4934-8543-0F91A7A02836</saml:AttributeValue>`
	`</saml:Attribute>`
	
	Example OIDC Value:
	`"tdif_audit_id": “AA97B177-9383-4934-8543-0F91A7A02836”`

Authentication Time	Example SAML Value:
	`<saml:AuthnStatement AuthnInstant="2018-03-05T03:20:48Z">`
	`<saml:AuthnContext> <saml:AuthnContextClassRef>urn:id.gov.au:tdif:acr:ip3:cl2</saml:AuthnContextClassRef>`
	`</saml:AuthnContext>`
	`</saml:AuthnStatement>`
	
	Example OIDC Value:
	`“auth_time”: 1520220048`

Annex B – Verified Documents attributes

This annexe 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 38 specifies the URN values that are used to specify Document Types Codes. Table 39 specifies additional URN that further qualify a document type. These URNs can be used as part of a request for a specific document type. For example to request verified document details for a Driver Licence issued by a specific state.

Table 38: 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 39: Additional Document Type Code.

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

Table provides a mapping of the DVS fields values defined in the DVS Match Specifications to the TDIF verified document attributes.

Table 40 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			
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
		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