Australian Government
Digital Transformation Agency

Attribute Provider Requirements

Trusted Digital Identity Framework
March 2019, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

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

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	Sep 2018	PH	Initial version
0.2	Jan 2019	PH	Incorporated feedback from stakeholders.
0.3	Feb 2019	PH	Incorporated feedback from public consultation.
1.0	Mar 2019		Endorsed for release by the TDIF Accreditation Authority.

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 defines requirements for Applicants who undergo TDIF accreditation as an Attribute Provider.

The intended audience for this document includes:

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

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

2 What is an Attribute Provider?

Attribute Providers are TDIF-accredited organisations or government agencies that manage attributes relating to people and non-person entities. The role of an Attribute Provider is to represent an authoritative source for a selected set of authorisation, qualification or entitlement Attributes under the TDIF.

Attributes are provided to Relying Parties on behalf of a person or non-person entity to support their decision-making processes.

Attribute Providers differ from Identity Service Providers in that they assert one or more Attributes about a person or non-person entity relating to authorisations, qualifications or entitlements, rather than about a person's identity information. Whereas an Identity Provider verifies the identity attributes of a person (e.g. I am Sue Jones), an Attribute Provider verifies specific attributes relating to entitlements, qualifications or characteristics of that person (e.g. this Sue Jones is authorised to act on behalf of business xyz in a particular capacity).

Table 1 below provides information regarding the different types of Attributes that can be provided by Service Providers operating under the TDIF.

Table 1: Attribute Types

Attribute Type	Description	Authoritative Source	Issued by
Identity	A piece of data relating to a person's identity. E.g. name, date of birth	Document and credential issuing bodies.	Identity Service Provider
Authorisation	Person is authorised to act on behalf of another entity. E.g., person is authorised to act on behalf of a business.	Authorisation bodies	Attribute Provider
Qualification	A person has studied at and graduated from an educational institution e.g. gained a university degree A person completed and passed a test e.g. driver licence	Education Providers, assessment bodies, registration bodies, licencing authorities	Attribute Provider
Entitlement	A thing you can have. E.g. a concession card, seniors card A person registers and is granted permission to perform a task	Federal, State & territory Government agencies	Attribute Provider

NOTE: The Attribute Provider Requirements defined in this document still apply where an Attribute type has not been identified in this table.

3 Attribute Provider Requirements

3.1 General Requirements

An Attribute Provider **MUST** either be:

- The Authoritative Source of the Attributes that they provide. E.g. if the Attribute is a licence and the Attribute Provider is the licencing authority for that licence, or

- Have the approval of the Authoritative Source to act as an Attribute Provider under the TDIF. E.g. if the Attribute is a qualification, the Attribute Provider will be the educational institution that issues that qualification or is authorised by that educational institution to act as an Attribute Provider on their behalf.

All Attributes contained within the database managed by the Attribute Provider **MUST** be uniquely identifiable and distinguishable from each other.

The Attribute Provider **MUST:**

- Use an up-to-date and accurate authoritative data source to register, link or verify Attributes.

- Verify the digital identity of the Attribute Holder prior to issuance or linking of an Attribute.

- Where the attribute is bound to a digital identity, verify that the digital identity has been proofed to at least Identity Proofing Level 2 before they can apply to be an Attribute Holder.

- Clearly identify:
    - Attribute Type, and where appropriate, Identity Proofing level required to access them and their validity periods. An Attribute Provider might check or provide multiple Attributes for an Attribute Holder. It is important that all Attribute Types are identified to the Exchange and or the Relying Party for this reason.

- entity types (e.g. person, business etc.) and their role in the context of Attribute issuance and/or
- roles assigned to the Attribute Holder in the context of the Attribute.

The Attribute Provider **MUST:**

- Ensure that where an attribute relates to a person, it is bound to a person who is has a digital identity registered with an Identity Service Provider.
- Ensure that the Attribute issued is unique (in the context of the service and this includes Attributes previously issued and that are now deactivated).
- Verify that requests to deactivate Attributes come from authenticated and authorised Attribute Holders.
- Have documented processes for management of attributes.

The Attribute Provider **MUST** publish its policies and practices for issuing and managing its attributes. At a minimum, the policies and practices **MUST** specify:

- The application process for attributes and requirements to issue attributes including the identity proofing level required, how the person is notified of the issuing of an Attribute and what obligations they accept by doing so.
- How a person's identity is bound to an Attribute and how it may need to be re-proven.
- How a person or a non-person entity gives consent for the use of their Attribute with Relying Parties
- How Attributes are renewed, replaced, revoked, suspended, and deactivated including how requests are authenticated and authorised.
- Establish and maintain an Attribute Provider Operations Manual, which at a minimum includes the following information:
  - Roles and responsibilities of the Attribute Provider and associated staff (i.e. Attribute Provider operators).
  - Processes, procedures and workflows used to support the Attribute Provider's lifecycle management functions (i.e. access control, storage, backup, archive and retrieval, disaster recovery, business continuity and records management)
  - Procedures used to register, create, bind, renew, modify, suspend, revoke and delete attributes.

- Procedures used by the Attribute Provider to manage a cyber security incident[2] (refer to the TDIF Protective Security Requirements for more information on management of cyber security incidents).
- Procedures used by the Attribute provider to meet TDIF Privacy Requirements (refer to the TDIF Privacy Requirements for more information about Privacy).
- Procedures used by the Attribute Provider to manage fraud (refer to the TDIF Fraud Control Requirements for more information about fraud control).
- Processes, procedures and workflows used to support system logging and the types of events captured.

The Attribute Provider **MUST** accommodate the following:

- Issuing multiple Attributes and attribute types to a person.
- Issuing multiple Attributes relating to the same entity to a person.
- Linking multiple people to the same Attribute/entity.
- Linking multiple digital identities for the same person to their Attribute.

The operation TDIF Attribute Provider by an organisation **MUST** be kept administratively and logically separated from other systems operated by the organisation.

An Attribute Provider **MUST NOT:**

- Store additional identity information outside of an Accreditation Authority approved Attribute Schema in an Attribute Profile
- Share identity information that is not part of the approved Attribute Schema, with Relying Parties.

3.2 Attribute Registration

An Attribute in the context of these Requirements may be obtained in a number of ways including:

- a registration process (e.g. a birth certificate, registering a car).
- validation of a claim or assertion (e.g. a business authorisation, a working with children check).

[2] 'Cyber security incident' is defined in the *TDIF: Overview and Glossary*.

- a once-off test (e.g. a hunting licence).
- a course of study (e.g. a first aid certificate).
- multiple courses of study (e.g. university degree).

Once an attribute has been obtained, an Attribute registration process with a TDIF-accredited Attribute Provider, consisting three steps can take place:

Step 1: Identifying the person who is registering for the Attribute (i.e. the Attribute Holder).
Step 2: Attribute identification.
Step 3: Linking the digital identity to the Attribute.

3.2.1 Identifying the person who is registering the attribute

A person needs to establish their Identity with a TDIF accredited IdP to the minimum level required to access their Attribute (Identity Proofing Level 2 or above).

3.2.2 Attribute identification

An attribute **MUST** be identified through either self-nomination, or by an Approved Attribute Holder.

Self-nomination

A self-nomination process **MUST** comprise the following:

- Identification of the attribute type (e.g. authorisation, qualification, entitlement)
- How the Attribute is issued (digitally, manual process)
- Identification of the entities relating to the attribute.
- If applicable, identification of roles, level or any sub-categories relating to the attribute.
- Context-specific information relating to the attribute.
- Contact information for the person requesting the attribute.

Authorised and Approved Attribute Holders

An Authorised Attribute Holder is a person or system authorised to appoint nominated Attribute Holders and for the registration of attributes. E.g. If the Authorised Attribute Holder is a business owner, they can authorise someone else to transact on behalf of their business. Alternatively, if the Attribute Holder is an education provider, they can confirm a student's academic record and advise Relying Parties of the associated qualification achieved by that student.

The Approved Attribute Holder process **MAY** compromise the following:

- The activities listed in the Self-nomination process above.
- Identity information of the Authorised Attribute Holder (where appropriate): e.g. name, role, authorisation level, contact information.
- Outcome of the identity verification if the Authorised Attribute Holder is a person.

3.2.3 Linking the nominee's identity to an attribute

A nominated Attribute Holder **MUST** consent to their digital identity being linked to an Attribute.

At a minimum the following information is collected when an attribute is registered:

- Identification of attribute type (e.g. authorisation, qualification, entitlement)
- Identification of the entities relating to the Attribute.
- If applicable, identification of roles, level or any sub-categories relating to the Attribute.
- Context-specific information relating to the Attribute.
- Contact information for the person requesting the Attribute.
- Other entities associated with the attribute (e.g. business, education provider, licensing authority).
- How the Attribute is issued (digitally, manual process)

Refer to the *TDIF: Attribute Profile* for guidance about information that that can be included in an Attribute Schema.

4 Attribute Management

4.1 Attribute lifespan

The lifespan of an attribute is dependent on the requirements and limitations placed on it by the Authoritative Source. Some attributes may be valid indefinitely, while others are valid for a defined period. E.g. if an attribute has a five-year validity period, the Attribute Provider cannot assert the attribute is valid beyond this period.

If an Attribute expires, the Attribute Provider **MUST:**

- Deactivate or suspend the Attribute.
- Remove the binding a digital identity.

4.2 Managing and editing Attribute information

The Attribute Provider **MUST** provide the Approved Attribute Holder:

- A way to securely view and manage their attributes and manage/update their contact and other information where appropriate.
- The ability to correct inaccurate information.
- The ability to de-link or de-associate an Attribute from the entity that they are authorised to manage.
- The ability to cancel their Attribute where appropriate.

The Attribute Provider **MUST:**

- Maintain a record all changes made to an Attribute.
- Re-verify the Digital Identity of an Attribute whenever an Attribute is changed.

Depending on the attribute type and context in which the Attribute is being used, the Attribute Provider and the Exchange **SHOULD** give the Attribute Holder the option to be advised whenever their Attribute is used or when their Attribute is used to transact with a new Relying Party.