Australian Government

Digital Identity

06A Federation Onboarding Guidance

Trusted Digital Identity Framework

Release 4.8 – Feb 2023

PUBLISHED VERSION

Department of Finance (Finance)

Licence

Use of the Coat of Arms

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

Conventions

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

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

Contact us

Finance 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 digitalid@finance.gov.au

Document management

Finance has reviewed and endorsed this document for release.

Change log

Document Version	Release Version	Date	Author	Description of the changes
0.1		Dec 2019	AV	Initial version
0.2		Feb 2019	AV	Updated to incorporate feedback provided during the third consultation round on TDIF Release 4
1.0	4.0	May 2020		Published version
1.1	4.4	June 2020	AV	CRID0018 – Technical Requirements guidance changes
1.2	4.6	March 2022		Update of defined terms to align with Release 4.6 of the TDIF Requirements
NA	4.7	June 2022		No changes to document
NA	4.8	Feb 2023		No changes to document

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

Contents

List of Figures

Introduction

This document has been developed to inform *Applicants* undergoing *Accreditation* what is required to meet the *TDIF 06 Federation Onboarding Requirements* and encompasses:

- Technical requirements guidance.
- Guidance for *Attribute Service Providers*.
- Guidance for *Identity Exchanges*.
- Technical integration guidance

The intended audience for this document includes:

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

Australian Government Digital Identity System Overview

The *TDIF* sets out the framework within which the *Australian Government Digital Identity System* operates. The *Australian Government Digital Identity System* is a brokered model of an *Identity federation*, with an *Identity Exchange* brokering interactions between *Relying Parties* and *Digital Identity Providers*.

The architecture of the *Australian Government Digital Identity System* has several key aspects, including:

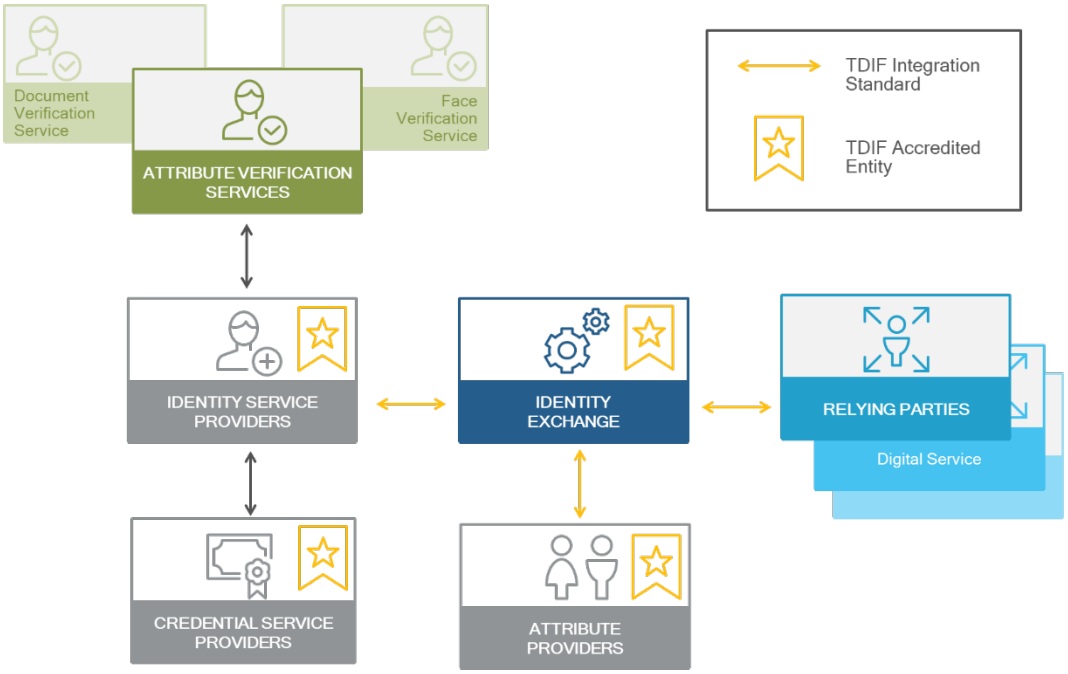
- *Identity Exchanges* which mediate all interactions between *Identity Service Providers*, *Attribute Service Providers* and *Relying Parties*. The *Identity Exchange* enables the use of multiple providers of identity services through a single point of integration for the *Relying Parties* it onboards.
- The presence of an *Identity Exchange* results in the creation of a *double blind*. The separation of the *Relying Parties* from the providers of identity services limits the ability for providers to conduct unauthorised tracking and profiling of information across the services they access as neither party can identify the other

during an interaction. This provides a privacy barrier between *Identity Service Providers* and *Relying Parties*.

- An *Identity Exchange* provides a central point of user *Consent* and visibility of identity *Attributes* to the user.
- An *Identity Exchange* provides an identifier mapping service that provides a stable, anonymous, identifier for a user that is unique for each *Relying Party*.
- *Identity Service Providers* are responsible for identity *Attribute Verification* by implementing *Identity Proofing* processes that conform to the standards in the *TDIF 05 Role Requirements*. *Identity Service Providers* use *Attribute Verification* services to validate the authenticity of *Identity Documents* against the document source.
- *Identity Service Providers* use a *Credential Service Provider* for the issuance and management, of *Credentials*, and *Authentication*
- An *Identity Exchange* may mediate interactions with additional *Attribute Service Providers* to support the sharing of *Attributes* that are in addition to the core identity attributes available for *Individuals* from *Identity Service Providers*.
- *Attribute Service Providers* manage *Attributes* relating to people and *non-person entities*, verifying special attributes relating to authorisations, qualifications or entitlements, which can then be provided to *Relying Parties* via an *Identity Exchange* with the *User's Consent*.

The conceptual architecture for the *Australian Government Digital Identity System* is set out in Figure 1.

Figure 1: *Australian Government Digital Identity System Conceptual Architecture.*



Key digital identity interactions

The key digital identity interactions that the *Australian Government Digital Identity System* supports are:

- *User Authentication*. *User Authentication* occurs when a *User* accesses a digital service at a *Relying Party* that requires *Authentication* and may also require verified *Attributes*.
- *Identity Proofing*. *Identity Proofing* may occur as part of an *Authentication* interaction with a *Relying Party*.
- *Credential Management*.
- *Identity Management*.

For further details regarding *Credential Management, Identity Management, Identity Proofing*, see both the requirements in the *TDIF 05 – Role Requirements* and the guidance present in the *TDIF 05A – Role Guidance*.

User Authentication

The *User Authentication* interaction is the primary interaction that touches all the components in the *Australian Government Digital Identity System*. At a high level it occurs via the *Relying Party* sending an *Authentication* request to an *Identity Exchange*, which then brokers the request to an *Identity Service Provider*, before returning the response, along with any *Attributes* received from an *Attribute Service Provider* back to the Relying Party. The *Identity Exchange* acts as a *Federation Proxy* and proxies the original request from a *Relying Party* to the *User's* selected *Identity Service Provider*.

Figure 2 and Figure 3 show the sequence of interactions which take place during a *User Authentication*. The sequence of interactions depicted in these figures is agnostic of the *Federation Protocol* used to make the requests. Where the *User* is transferred between entities via the user agent, the interaction is annotated with the `<<Front Channel Transfer>>` label.

Figure 2: User Authentication Sequence Diagrams (steps 1 to 5).

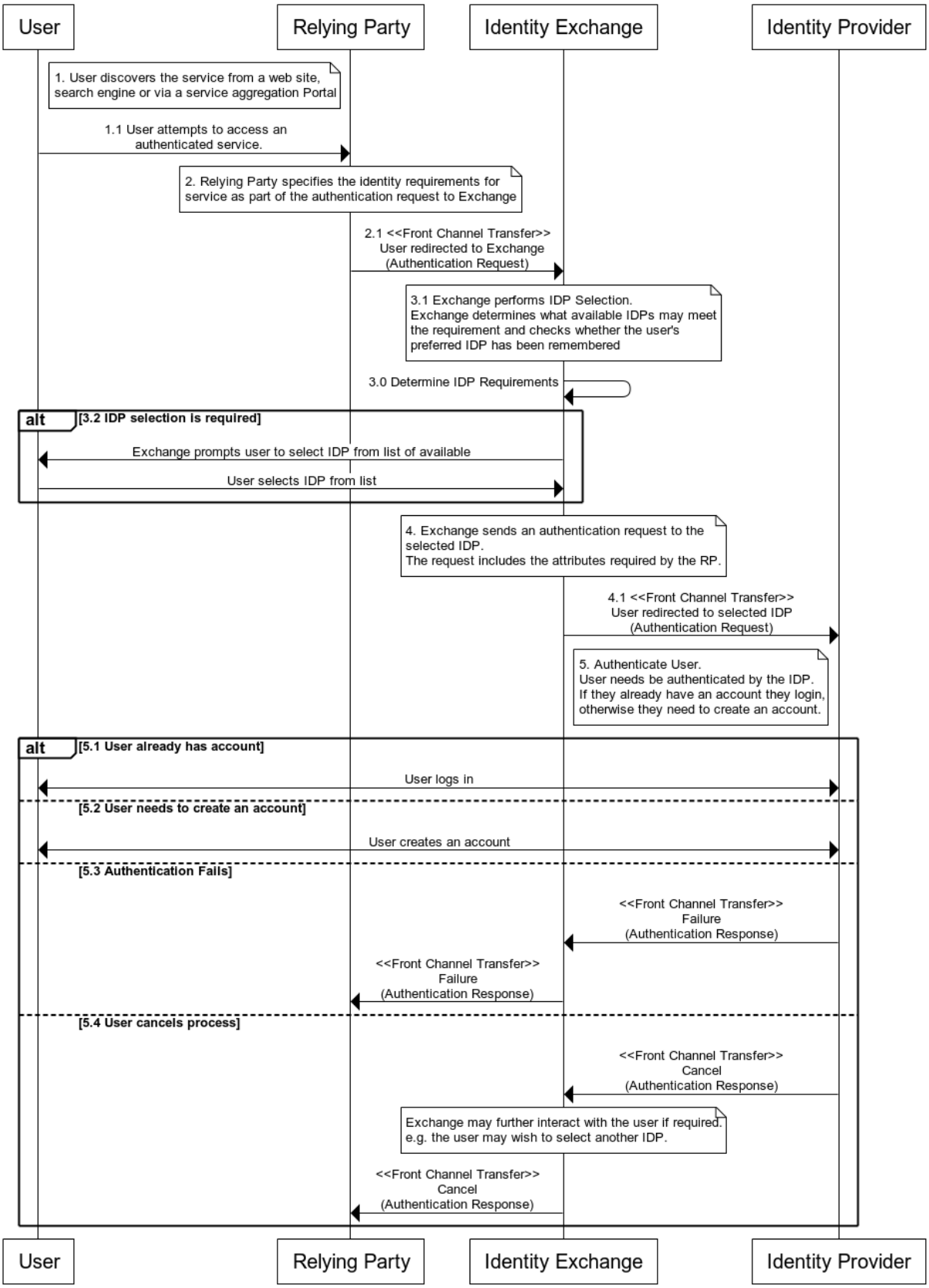
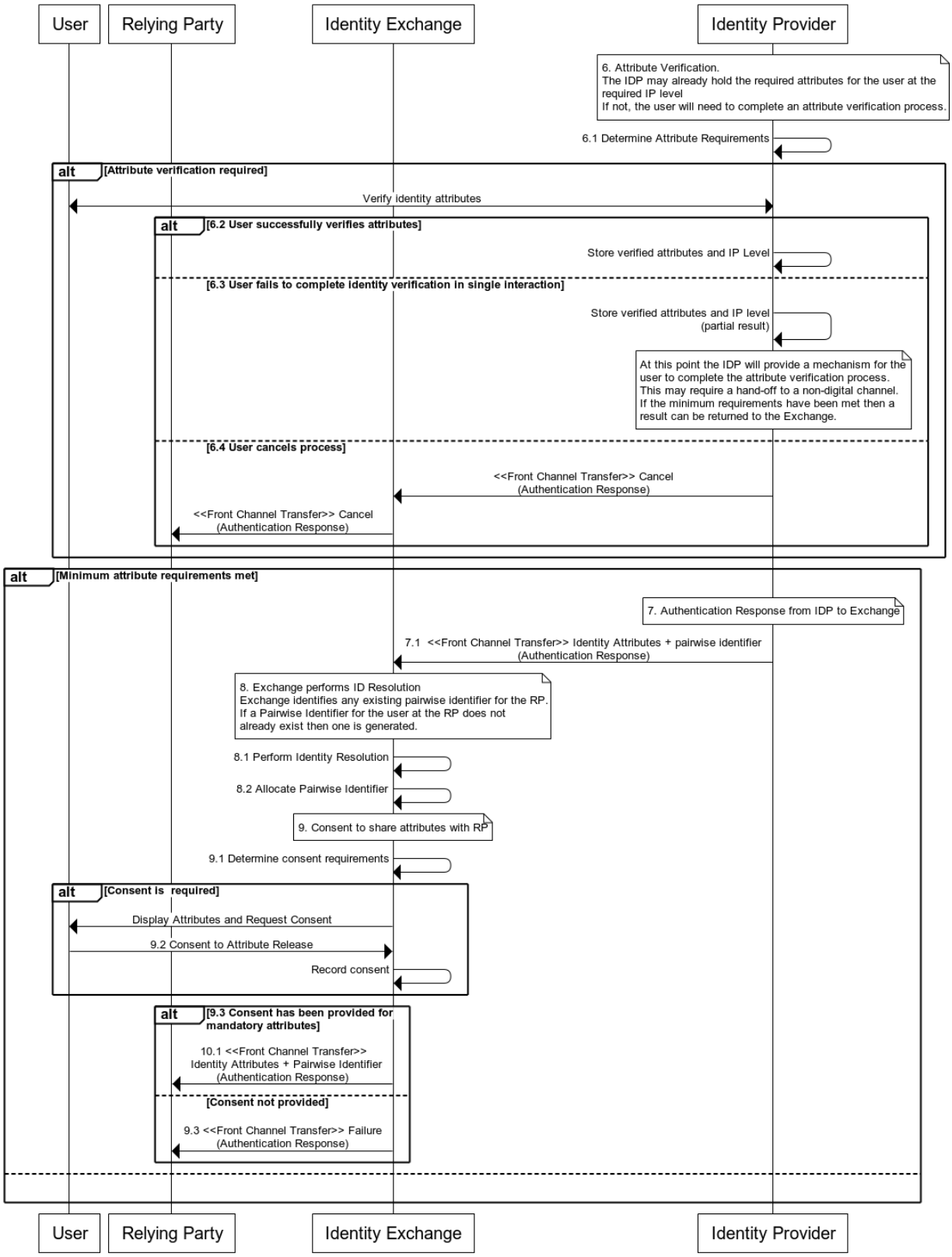


Figure 3: User Authentication Sequence Diagrams (steps 6 to 11).



Each step in the above diagrams is described below.

1. *User* discovers the digital service.

    1.1. *User* attempts to access an authenticated digital service.

        - The *User* discovers the digital service at a *Relying Party*. This can be from content on an unauthenticated web site, a search engine, or from within a service aggregation portal.
        - The *User* accessing the service triggers the Authentication process by choosing to log on with their *Digital Identity* and any required verification of identity *attributes* can occur as a part of this *Authentication*.

2. *Authentication Request* from *Relying Party* to an *Identity Exchange*.

    2.1. User redirected to an *Identity Exchange* by the *Relying Party* using an *Authentication Request*.

        - The *Relying Party* specifies the requirements to access the digital service as part of the *Authentication Request*. The request includes the required *Credential Level, Identity Proofing Level, Attributes* and other parameters supported by the *Identity Exchange*.[1]
        - The *Relying Party* specifies the minimum levels of assurance. The minimum *a*ssurance level is specified as mandatory or optional. If the specified minimum IP level is mandatory it must be reached for a successful *Authentication* response to be returned to the *Relying Party*.
        - The *Attributes* are specified as optional or mandatory. If a mandatory attribute cannot be returned (not available or consent not provided) then the authentication response will be a failure.[2]

3. *Identity Service Provider* Selection.

    3.1. The *Identity Exchange* conducts *IdP Selection*, displaying the *Identity Service Providers* that will meet the requirements of the *Authentication Request* from

[1] For further detail on what can be requested, refer to the *TDIF 06B - OpenID Connect 1.0 Profile, TDIF 06C - SAML 2.0 Profile*, *TDIF 06D – Attribute Profile.*

[2] The *TDIF 06 Federation Onboarding Requirements* does not currently specify any attributes that may be requested as Mandatory by a Relying Party. In general, an authentication response should always be returned to the Relying Party as per the point above. This is consistent with the requests for claims in the OIDC standard, see https://openid.net/specs/openid-connect-core-1_0.html section 5.5.1.

the *Relying Party* to the *User*. It will also check whether a preferred *Identity Service Provider* for the *User* has already been remembered.

3.2. If more than one *Identity Service Provider* is available then the *User* will be prompted to select an *Identity Service Provider* from a list. This selection may be remembered to streamline further interactions.

3.3. *User* cancels process. An authentication response indicating the cancellation of the process is sent back to the *Relying Party*.

4. *Authentication Request* from an *Identity Exchange* to an *Identity Service Provider*.

4.1. The *Identity Exchange* redirects the *User* to the selected *Identity Service Provider* using an *Authentication Request*. The request includes the *Attributes*, *Credential Levels* and *Identity Proofing levels* that will satisfy the original request by the *Relying Party*.

- The *Identity Exchange* will map the request from the *Relying Party* to the *Federation Protocol* supported by the *Identity Service Provider* in accordance with the requirements found in section 4.2.2 of the *TDIF 06 - Federation Onboarding Requirements*. .

5. *Authenticate User*. The user will either login to an existing account at the *Identity Service Provider*, create a new one, fail to authenticate or cancel the process of logging in.

5.1. *User* already has an account at the *Identity Service Provider*.

- The *User* logs into the *Identity Service Provider* using their existing *Credentials*. If the existing *Credentials* do not meet the required *Credential Level* the *User* will need to enrol additional *Credentials*.

5.2. *User* does not have an account at the *Identity Service Provider*.

- The *User* creates an account and is issued with *Credentials* at the required Credential *Level*.

5.3. *Authentication* fails.

- If the *User* fails to authenticate at the required *Credential Level* then an *Authentication* response indicating the *Authentication* failure is sent back to the *Identity Exchange*. The *Identity Exchange* then sends the same *Authentication* response back to the *Relying Party*.

5.4. *User* Cancels Process.

- An *Authentication* response indicating the cancellation of the process is sent back to the *Identity Exchange*. The *Identity Exchange* may interact with the *User* to determine if an alternate pathway is required to complete the process, e.g. to select a different *Identity Service Provider*. The *Identity Exchange* then sends the same *Authentication* response back to the *Relying Party* if there is no identified alternate pathway.

6. Verify *Attributes*. The *Identity Service Provider* interacts with the *User* to verify *Attributes* at the required *Identity Proofing Level*, as described in the section 3 of the *TDIF 05 Role Requirements*¸ unless the *User* has already verified the required *Attributes*.

6.1. *Identity Service Provider* determines *Attribute* requirements.

- The *Identity Service Provider* checks the *Attributes* already held for the *User* and determine if any further *Attribute* verification is required. If *Attribute* verification is required then steps 6.2 to 6.4 are possible paths.

6.2. User successfully verifies *Attributes*.

- The *User* is able to successfully verify *Attributes* at the required level.

6.3. The user is unable to complete the *Attribute* verification process to the desired *Identity Proofing Level* in a single digital interaction.

- The *Identity Service Provider* will store the partial result and provide a process for the *User* to complete the *Attribute* verification. This may require a hand-off to a non-digital channel. If the *Relying Party* originally specified a minimum *Identity Proofing Level* that has been met then a response can be returned to the *Relying Party*, otherwise this sequence of interactions end here.

6.4. *User* Cancels Process.

- An *Authentication* response indicating the cancellation of the process is sent back to the *Identity Exchange*. The *Identity Exchange* then sends the same *Authentication* response back to the *Relying Party* if there is no identified alternate pathway.

7. *Authentication* response is sent back to the *Identity Exchange*.

7.1. The *Authentication* response from the *Identity Service Provider* includes:

- Achieved *ACR* level.
- A *Pairwise Identifier* for the *User* at the *Identity Service Provider*.
- *Attributes*.
- Any other parameters requested by the *Identity Exchange* allowed by the applicable *Federation Protocol TDIF* profile.

8. *Identity Exchange* performs identity resolution.

- *Identity Exchange* identifies any existing mapping between the *IP Link* sent by the *Identity Service Provider* and an *RP Link* at the *Relying Party*. If a mapping does not already exist then one is generated.

8.1. Perform identity resolution.

- If there is already an *RP link* mapped to the *IP Link* from the *Identity Service Provider* then the *Identity Exchange* will use that *RP link*.

8.2. Allocate *Pairwise Identifier*

- If required, an *RP Link* is generated for the User which is unique for that user at that *Relying Party*.

9. *Consent* to share attributes.

9.1. Determine *Consent* requirements.

- *Identity Exchange* determines the user *Consent* requirements for the *Attributes* requested by the *Relying Party*. It will include checking for any ongoing *Consent* for sharing the *Attributes* with the *Relying Party*.

9.2. Consent to *Attribute* release.

- If *User Consent* is required, the *Identity Exchange* will interact with the *User* to gather *Consent* to release the *Attributes* to the *Relying Party*. The *Identity Exchange* will record the provided *Consent* and the *User's* preference for remembering this.

9.3. *Consent* not provided.

- If *Consent* is not provided then these *Attributes* are not returned in the *Authentication* response to the *Relying Party*.
- If *Consent* is not provided for any mandatory *Attribute* then a failure *Authentication* response is returned to the *Relying Party*.

10. *Authentication* response to *Relying Party*.

10.1. *Authentication* response is sent back to the *Relying Party*.

- The response includes:
  - Achieved *ACR* level.
  - *Pairwise Identifier* for the *User* at the *Relying Party*.
  - *Attributes* for which *Consent* has been provided.

11. User accesses digital service.

11.1. Relying Party uses the *Attributes* to enable the *User* to access the digital service.

- The first time the *User* accesses a *Relying Party*, the *Relying Party* may need to determine if there is an existing customer record by using the identity *Attributes*. Where a *Relying Party* performs *Identity* matching, the *Relying Party* is responsible for ensuring that the matching process is sufficient to manage risks of authorised access to a person's record and is accountable for any privacy breach that may occur as a result of improper matching. Once a customer record has been located or created at the *Relying Party* the *Pairwise identifier* is stored by the *Relying Party*, subsequent interaction by the user with the digital service will simply use the *Pairwise Identifier* to locate the customer record.

- Note: some transactions are one-off and will not require the above process.

Technical Requirements Guidance

Common Functional Requirements

Technical Integration Standards

*Relates to TDIF requirements **FED-02-01-01** to **FED-02-01-05** of section 2.1.1 in the TDIF 06 – Federation Onboarding Requirements.*

To support the operation of the *Australian Government Digital Identity System,* the *TDIF* defines requirements for implementing specific *Federation Protocols*. These requirements specify the *Federation Protocols* that *Accredited Participants* are required to implement according to the role they are performing in the *Australian Government Digital Identity System*.

For an *Identity Exchange*, it will need to support both receiving requests from a *Relying Party* and making requests to *Identity Service Providers*. Each of these interactions is an instantiation of the *Federation Protocols*, with the *Identity Exchange* being responsible for maintaining the correspondence between them. In each scenario (either receiving requests, or making them) the *Identity Exchange* acts as a different entity in terms of the *Federation Protocols*:

- *Relying Party* to *Identity Exchange*: The *Identity Exchange* acts as an *Identity Service Provider*.
- *Identity Exchange* to *Identity Service Provider*: The *Identity Exchange* acts as a *Relying Party*.

With more advanced *Identity Exchanges*, this process includes a translation in the *Federation Protocol* used. For example, a *Relying Party* connecting to an *Identity Exchange* using the *SAML Federation Protocol* has their requests serviced by the *Identity Exchange* performing a protocol translation to provide *Authentication* from an *Identity Service Provider* that uses the OpenID Connect 1.0 *Federation Protocol*.

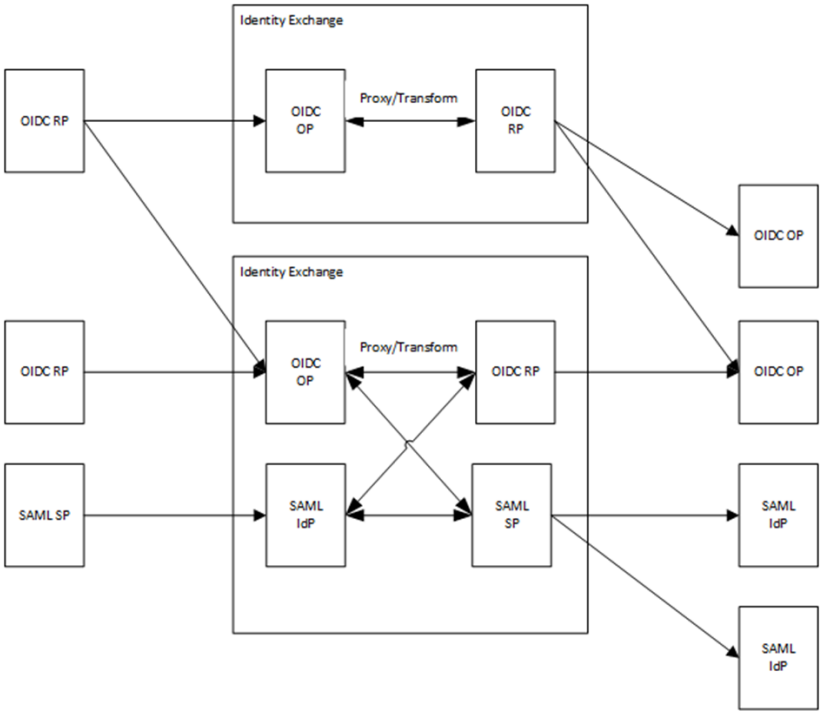
The following table notes the relationship between the terminology used in the *TDIF* and the terms used to describe entities in these federation protocols.

TDIF Term	OIDC Term	SAML Term
Relying Party (RP)	Relying Party (RP)	Service Provider (SP)
Identity Service Provider (IdP)	*OpenID Provider* (OP)	*Identity Service Provider* (IdP)

If an Applicant is required to implement OpenID Connect 1.0 then refer to the *TDIF: 06B - OpenID Connect 1.0 Profile* **[TDIF.OIDC]** for guidance and the requirements that need to be met. If an applicant is required to implement SAML 2.0 then refer to the *TDIF: 06C - SAML 2.0 Profile*.

Figure *4*: Australian Government Digital Identity System Topologies illustrates the possible *Identity Federation* topologies that exist in a mature identity eco-system. Digital services that rely on the *Australian Government Digital Identity System* can establish connections to any number of available *Identity Exchanges* that support their required *Federation Protocol*. These *Identity Exchanges* in turn can connect to any number of *Identity Service Providers* using their supported *Federation Protocols*.

Figure 4: *Australian Government Digital Identity System* Topologies



Security Considerations

*Relates to TDIF requirements **FED-02-01-06** to **FED-02-01-06a** of section 2.1.2 in the TDIF 06 – Federation Onboarding Requirements.*

See the applicable recommendations in the security considerations section of **[RFC 6749]** and those found in the OAuth 2.0 Threat Model and Security Considerations document **[RFC 6819].**

Feature-Specific Technical Integration Requirements

Identity Resolution

Identity resolution refers to the process of determining whether multiple *Digital Identities* relate to the same person or a different person, including *Digital Identity* records at one or more *Identity Service Providers* and/or *Identity Exchange's*, and/or agency records at a *Relying Party*. An *Identity Exchange* utilises *Pairwise Identifiers* and *Deduplication* to conduct identity resolution. It is also expected that *Relying*

Parties who deem it necessary will have their own identity resolution processes to avoid duplicate accounts.

Pairwise Identifiers

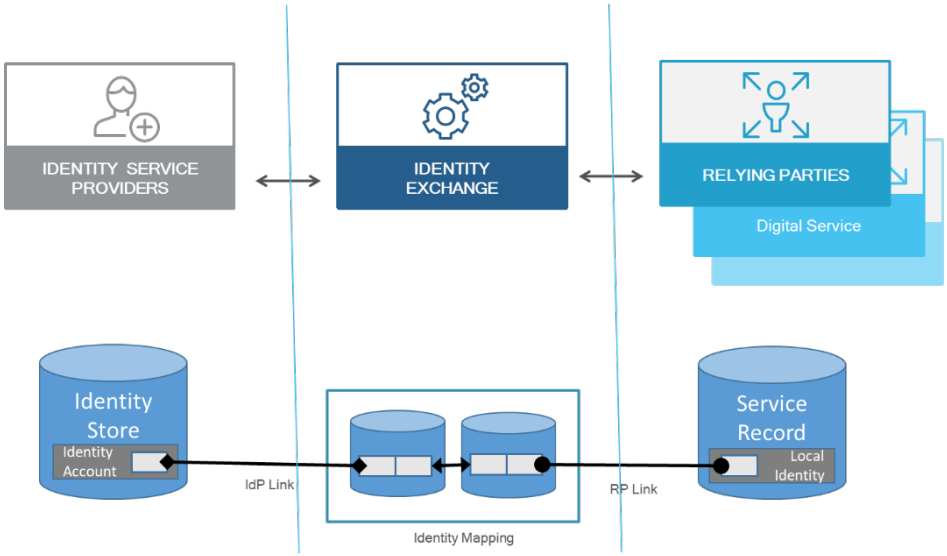
*Relates to TDIF requirements **FED-02-03-01** to **FED-02-03-09** of section 2.3.1.1 in the TDIF 06 – Federation Onboarding Requirements.*

Pairwise Identifiers are used in the *Australian Government Digital Identity System* to support the *Authentication* processes that enable an *Individual* to have ongoing access to digital services at a *Relying Party* by creating identity linkages. These are *identifiers* generated by either an *Identity Service provider* or *Identity Exchange* which are unique for each client of the provider of the identifier, as per the specification in section 8.1 of the OpenID Connect core 1.0 specification. This prevents the creation of a single *identifier* for a *User* across the *Australian Government Digital Identity System*.

To enable *Users* to *Authenticate* and then be able to reuse their *Identity* at a *Relying Party*, the following identity linkages exist as persistent pseudonymous *identifiers* in the *Australian Government Digital Identity System*:

- *IdP Link*. This *identifier* links the *identity* for an authenticated *user* at an *IdP* with the *Digital Identity* brokered by an *Identity Exchange*. This *pairwise identifier* is generated by the *Identity Service Provider*.
- *RP Link*. This *identifier* links the *Digital Identity* brokered by an *Identity Exchange* to the service record (client record, customer record) at a *Relying Party*. The *Identity Exchange* generates this *pairwise identifier*. This *RP Link* is unique for each *User* at each *Relying Party*.

Figure 5: Identity Linkages in the *Australian Government Digital Identity System*

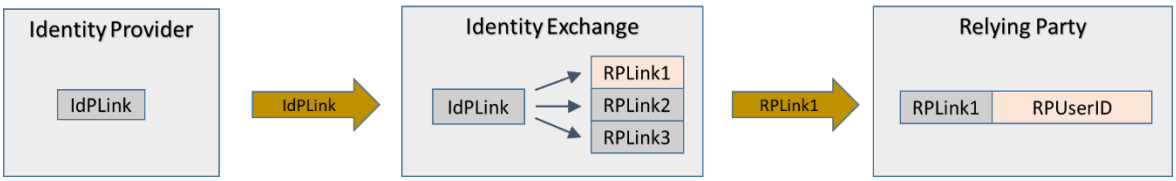


As per **Figure *5***, an *Identity Exchange* maintains a mapping between the *IdP Link* (the identity at an *Identity Service Provider*) and the *RP Link* (the service record at the *Relying Party*).

When a user authenticates to a *Relying Party* using the services of an *Identity Service Provider* the same *RP Link* will be presented to the *Relying Party* across all authentication events.

A generalised depiction of the flow and storage of identity links is shown in Figure 6.

Figure 6: Identity Mapping across any *Identity Exchange*.

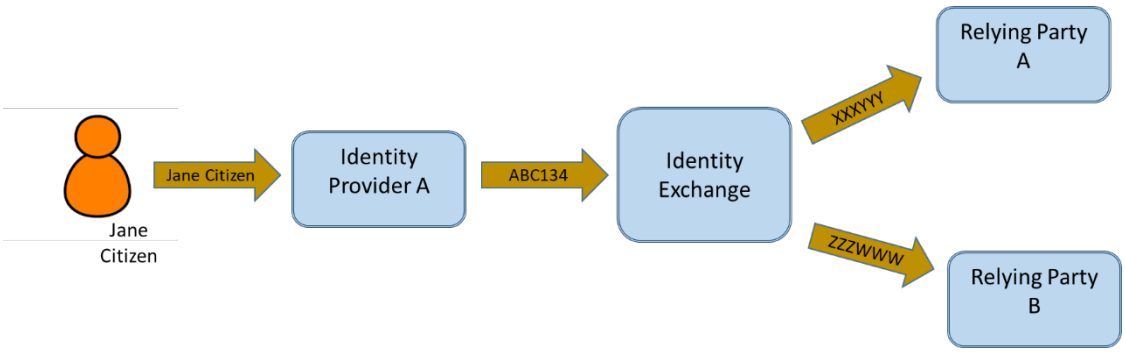


1. The *Identity Service Provider* persists a single *identifier* for each unique *identity* it recognises (*IdP Link*).
2. At the time of *Authentication*, the *IdP Link* is passed to the *Identity Exchange*.
3. The *Identity Exchange* persists the *IdP Link* against a table of internally generated *Relying Party* specific *Identifiers* (*RP Link*).
4. The *Identity Exchange* selects or generates the *RP Link* that matches the *Relying Party* that has requested *Authentication*.

5. The *Identity Exchange* passes the *RP Link* to the *Relying Party*.
6. The *Relying Party* maps the *RP Link* to its internal customer record.

An example of identity mapping that occurs in the *Authentication* of a *User* is shown below:

***Figure 7**: Mapping of a User's identity in an Authentication Event.*



The use of *Pairwise Identifiers* is a key privacy mechanism. When a *Relying Party* utilises them they should consider specific privacy and administrative arrangements that operate in their jurisdiction, including any legislative requirements concerning how personal information should be collected, accessed and stored correctly.

OIDC Relying Party Sector Identifiers

The *OIDC* specification closely couples the concept of a *Relying Party* to a client, or a software application instance. A *TDIF Relying Party* may need to register multiple *OIDC* clients for the different digital services that it provides but still require the same underlying *Pairwise Identifier* for an authenticated *User* to be passed to all of its registered *OIDC* clients. The *OIDC* standard provides a mechanism to enable multiple clients to receive the same *Pairwise Identifier*. This mechanism is termed a Sector Identifier and is defined in the **[OpenID.Core]** https://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg and is further expanded on the specification for Dynamic Client Registration https://openid.net/specs/openid-connect-registration-1_0.html#SectorIdentifierValidation. The use of sector identifiers is supported in the *Australian Government Digital Identity System,* as required by **FED-02-03-06.**

Deduplication

*Relates to TDIF requirements **FED-02-03-10** to **FED-02-03-20** of section 2.3.1.2 in the TDIF 06 – Federation Onboarding Requirements.*

The aim of *Deduplication* is for *Individuals* with multiple *Digital Identities* at one or more *IdPs* to appear as having a single *Digital Identity* to a *Relying Party*. In the *Australian Government Digital Identity System*, this is conducted by the *Identity Exchange* with assistance from *Identity Service Providers*, who provide an *EDI* which an *Identity Exchange* may use for the purposes of *Deduplication*.

Deduplication in the system relies on *Identity Service Providers* passing a unique *Attribute* called an Evanescent Deterministic Identifier (*EDI*) in response to an *Authentication Request* for a User. When generating an *EDI*, the *IdP* is required to combine several *Attributes* taken from verified documents, concatenate these, convert the resulting string to utf-8 and then hash the text using SHA-256. The document type code which is required to be used in this transaction is the same document type code as is used to request the document. This can be found in section 6.1 of the *TDIF: 06D – Attribute Profile*.

The document used to generate an EDI is specified in section 2.2.1.2 of the *TDIF: 06 – Federation Onboarding Requirements*. These documents and the precedence of documents to be used will be updated by *Finance* as more documents become accessible in the federation. Furthermore, for new documents, *Finance* will advise what *Attributes* need to be used and in what order these will be used.

An *Identity Exchange* utilises the *EDI* to deduplicate identities. They are not allowed to store the *EDI* or send it to other *Participants* in the *Australian Government Digital Identity System*.

One implementation of *Deduplication* is to transform the *EDI* into a unique identifier specific for a *User* at each *Relying Party*. This is then used as a lookup to check whether a different *Digital Identity* with the same unique identifier has previously accessed that *Relying Party*.

If there is, the *RP link* of that *Digital Identity* is mapped to the *IdP link* of the *User*. This ensures that *Deduplication* isn't done across entire identities, but instead is done at

each *Relying Party* and that an *Individual* can appear the same to a *Relying Party*, regardless of which *IdP* was used. This unique *Relying Party* specific *Identifier* can also be configured in accordance with *Relying Party* sector identifiers.

Single Sign on/Single Log out

*Relates to TDIF requirements **FED-02-03-21** to **FED-02-03-30** of section 2.3.2 in the TDIF 06 - Federation Onboarding Requirements.*

These requirements operate in addition to the requirements in section 6.3 of the *TDIF 05 – Role Requirements*, adding additional obligations for an *Identity Exchange* performing *single sign on* and *single log out* in the *Australian Government Digital Identity System*. Where a requirement has been archived, if the content has been moved to the *TDIF 05 – Role Requirements*, this is called out in the requirement with a reference to the specific requirement which has replaced it.

This section provides additional guidance for implementing *single sign on* and *single log out* in the *Australian Government Digital Identity System.*

Known Subject Authentication

FED-02-03-21 is intended to support *Authentication* scenarios where the *Identity* (service record) of the *User* at a *Relying Party* is already known, sometimes known as Known subject *Authentication*. These *Authentication* scenarios include:

- *Relying Party* clients where the identity of the user can be remembered, such as a mobile client.
- Scenarios where a previous authentication event has established the identity of the user at the *Relying Party*. These scenarios include:
  - Re-authentication. The *User's Authentication* session has expired at the *Relying Party* and the user needs to be re-authenticated.
  - Step-up *Authentication*. The user has previously authenticated at the *Relying Party*, but the *Relying Party* has determined that a higher level of assurance is required, so triggers an additional *Authentication* for the *User*.

Relying Parties are able to make requests indicating that they know the subject of the *Authentication* using the `sub` claim if they are using the *OIDC* profile for

Authentication Requests. A *Relying party* utilising *OIDC* as its *Federation Protocol* may also use an id_token_hint. Further detail on how an *Identity Exchange* can support this is present in the requirements set out in section 4.2.1.2 of the *TDIF: 06 - Federation Onboarding Requirements*.

If the *Relying Party* is utilising the *SAML Federation Protocol* by using the `<saml:Subject>` element in the *SAML* `<AuthnRequest>` message. Further detail on how an *Identity Exchange* can support this can be found in the requirements in section 4.2.4.2 and section 4.2.5.3.3 of the *TDIF: 06 – Federation Onboarding Requirements.*

Single Log Out

In the *Australian Government Digital Identity System* the implementation of single logout is more complex as an *Identity Exchange* needs to propagate any logout requests between the parties which have utilised a single *session*. There are two generic Single Logout use-cases.

RP-initiated Single Logout. In this use-case the following steps occur:

- The *User* initiates the SLO at a *RP*.
- The *RP* then sends the logout request to the session broker.
- The session broker determines every other participant that has been signed in during the current logon session at the session broker.
- The session broker sends that logout request to every other session participant (RP). Each *RP* terminates its logon session.
- The session broker terminates its own logon session and sends a logout response to the initiating *RP*.
- The initiating *RP* terminates their logon session.

IdP-initiated Single Logout.

- The user initiates the SLO at the session broker.
- The session broker determines every other participant that has been signed in during the current logon session at the session broker.
- The session broker sends that logout request to every other session participant (RP). Each RP terminates its logon session.
- The session broker terminates its logon session.

Within the *Australian Government Digital Identity System*, this means that:

- In RP-initiated Single Logout use-case, an *Identity Exchange* performs the role of a session broker. In addition, a logout request is sent to the *IdP* that the *User* authenticated with.
- In the IdP-initiated Single Logout use-case, the *Identity Exchange* accepts a logout request from the *IdP* that the user *Authenticated* with. The *Identity Exchange* acts as session broker in the SLO interaction and send a logout request to all RPs that have been authenticated as part of the same logon session at the IdP. In addition, a logout response is sent to the initiating IdP.

Attribute Service Provider Requirements

This section describes the unique technical requirements specific to *Attribute Service Providers* seeking to onboard onto the *Australian Government Digital Identity System*.

The technical requirements detailed in section 3 of the *TDIF: 06 - Federation Onboarding Requirements* assume the following:

- An *Attribute Service Provider* is integrated with an *Identity Exchange* as a Relying Party in order to make the *Attributes* available to *Relying Parties*.
- The *User* authenticates to the *Attribute Service Provider* using their chosen *Identity Service Provider*.
- The *Identity Exchange* makes the Attributes available to Relying Party in accordance with the technical requirements detailed in TDIF: 06 - Federation Onboarding Requirements.
- Attributes provided by Attribute Service Providers are specified in section 6 of the TDIF: 06 - Federation Onboarding Requirements.
- Attribute Sets provided by different Attribute Service Providers are disjoint, i.e. there is a 1:1 correspondence between Attribute Sets and an Attribute Service Provider.

Technical Requirements

*Relates to TDIF requirements **FED-03-01-01** to **FED-03-01-07** of section 3.1 in the TDIF 06 – Federation Onboarding Requirements.*

An *Identity Exchange* may request *Attributes* from an *Attribute Service Provider* through an *API*. It is recommended that the *API* provided by an *Attribute Service Provider* be implemented as a REST *API*.

FED-03-01-07 states that *Attribute Service Providers* may also make *Attributes* available to a *Relying party* by authorising the *Relying Party* to directly retrieve the attributes from the *Attribute Service Provider*. This mechanism requires the *Identity Exchange* to return a security token to the *Relying Party*. The *Relying Party* can then use this security token to retrieve *Attributes* from the *Attribute Service Provider*.

Where the retrieval of *Attributes* directly from an *Attribute Service Provider* by a *Relying Party* is permitted it is recommended that this be implemented using distributed claims as detailed in section 5.6.2 of the **[OpenID.Core]** https://openid.net/specs/openid-connect-core-1_0.html#AggregatedDistributedClaims.

Audit Logging

*Relates to TDIF requirements **FED-03-02-01** to **FED-03-02-03** of section 3.2 in the TDIF 06 – Federation Onboarding Requirements.*

These requirements operate in addition to the requirements outlined in section 4.2.6 of the *TDIF 04 – Functional Requirements*. See these requirements for what the *Attribute Service Provider* is required to store in its *audit* log.

The RP Audit ID *Attribute* is intended to be used to support the auditing of transactions across the system and enable a transaction to be traced through a system. Under **PROT-04-02-24b,** an *Attribute Service Provider* is required to have a unique identifier for each activity. For the activities specified in **FED-03-02-02,** an *Attribute Service Provider* may use the RP Audit ID as this unique identifier.

Exchange Requirements

Integration Requirements

Audit Ids

*Relates to TDIF requirements **FED-04-01-01** to **FED-04-01-05** of section 4.1.1 in the TDIF 06 – Federation Onboarding Requirements.*

These requirements operate in addition to the requirements outlined in section 6.1 of the *TDIF 05 –Role Requirements*. They create obligations on an *Identity Exchange* to use a particular *Attribute* (RP_Audit_ID) as the unique audit id described in IDX-06-01-01 to ensure that all transactions with *Relying Parties* and *Attribute Service Providers* can be audited.

The *Identity Exchange's* unique position in the *Australian Government Digital Identity System* endows it with an important role in relation to auditing and logging. The ability of both the *Identity Service Provider* and *Relying Party* to perform these functions is limited due to the privacy preserving nature of the *Australian Government Digital Identity System*. An *Identity Exchange* is the only party that has visibility of what *Attributes* are being shared with a *Relying Party*, and what *Participant* was the source of those attributes. Furthermore, these requirements place limits on an *Identity Exchange's* ability to provide information that could be used to trace a transaction at a *Relying Party* with an *Identity Service Provider* to help protect the privacy of *individuals* using the *Australian Government Digital Identity System*.

Audit History, Consumer History and User Dashboard

*Relates to TDIF requirements **FED-04-01-06** to **FED-04-01-08** of section 4.1.2 in the TDIF 06 – Federation Onboarding Requirements.*

The *User Dashboard* is required for an *Applicant* participating in the *Australian Government Digital Identity System*. To implement a *User Dashboard* an *Applicant* is required to meet the requirements found in section 6.4 of the *TDIF 05 – Role*

Requirements. For further guidance on how to implement a *User Dashboard* refer to the Guidance for User Dashboards found in the *TDIF 05A – Role Guidance*.

Attribute Service Provider Integration

*Relates to TDIF requirements **FED-04-01-09** to **FED-04-01-12** of section 4.1.3 in the TDIF 06 – Federation Onboarding Requirements.*

These requirements are intended to support the integration of an *Identity Exchange* with an *Attribute Service Provider* and grant an *ASP* flexibility in how it shares *Attributes* with a *Relying Party.*

IdP Selection

*Relates to TDIF requirements **FED-04-01-13** to **FED-04-01-16** of section 4.1.4 in the TDIF 06 – Federation Onboarding Requirements.*

An *Identity Exchange* operating in the *Australian Government Digital Identity System* is required to implement *IdP Selection.* The requirements describing how an *Identity Exchange* is required to implement *IdP Selection* have been moved to section 6.5 of the *TDIF 05 – Role Requirements.*

In the context of the *Australian Government Digital Identity System IdP selection* takes place as part of the *Authentication* interaction, as described in section 2.1.1.1 of this document. For further guidance refer to the Guidance for *IdP Selection* in the *TDIF 05A - Role Guidance.*

Federation Protocol Mapping Requirements

An *Identity Exchange* operates as a broker of *Authentication Requests* from a *Relying Party* to an *Identity Service Provider*. This means that it is required to conduct certain processes as part of its role, specifically regarding mapping between different federation protocols.

It performs this mapping at the following instances:

1. When an *Identity Exchange* receives an *Authentication Request* from a *Relying Party*, it maps the information in the request to the *Federation Protocol* used to make an *Authentication Request* to the *User's* chosen *Identity Service Provider*.
2. When an *Identity Exchange* receives an *Authentication* response from an *Identity Service Provider*, it must map this to the *Federation Protocol* used by the *Relying Party* in the original *Authentication Request*.

This requires the following mappings to be done:

- Mapping of claims to scopes
- Handling of the `sub` claim
- Mapping of assurance levels
- Mapping of specific request parameters (e.g. max_age, prompt)

The guidance for the above mappings can be found below. Other mappings specific to each protocol are discussed in greater detail in their relevant section.

When an *Identity Exchange* is conducting it's mapping it filters out which claims and scopes it will request of an *Identity Service Provider*, and which claims and scopes need to be requested from other participants, like an *Attribute Service Provider*.

Levels of Assurance

Levels of Assurance are a commonly used mechanism to describe the degree of confidence in an *Authentication* process. The *Australian Government Digital Identity System* uses two values to represent the degree of confidence in an *Authentication* process; *Identity Proofing Level* and *Credential Level*. For more detail on these different levels of assurance and how they are obtained, see the *TDIF: 05 - Role Requirements*.

In an authentication interaction, these two values are represented by an Authentication Context Class Reference (*ACR*). *ACR's* are a concept supported by both the OpenID Connect 1.0 and SAML 2.0 *Federation Protocols* and specify the set of authentication methods or procedures that have been used in a given *Authentication*.

Required *ACR* values are represented in an *OIDC Authentication Request* using either the `acr_values` parameter or the `acr` claim. Required ACR values are represented in a *SAML* request using the `<saml:AuthnContextClassRef>` element.

In the *TDIF URNs* are used to define each of the assurance levels. The *URNs* are the permissible combinations of the *Identity Proofing Level* LoA and *Credential Level* LoA defined by the *TDIF*. The possible values are set out in Table 4 of the *TDIF: 06-Federation Onboarding Requirements.* As described in **[TDIF.OIDC]** and **[TDIF.SAML]** a *Relying Party* may specify a minimum value for an *ACR* which satisfies its requests. If it does so then the below table demonstrates what values the exchange should send as satisfying a request for a minimum *ACR*.

Figure 8: ACR Levels which satisfy a request for a minimum ACR

IP Level		IP1			IP1 PLUS			IP2		IP2 PLUS		IP3		IP4
	Credential Level	CL1	CL2	CL3	CL1	CL2	CL3	CL2	CL3	CL2	CL3	CL2	CL3	CL3
IP1,	CL1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CL2	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CL3	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP1 PLUS	CL1	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CL2	×	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
	CL3	×	×	×	×	×	✓	✓	✓	✓	✓	✓	✓	✓
IP2	CL2	×	×	×	×	×	×	✓	✓	✓	✓	✓	✓	✓
	CL3	×	×	×	×	×	×	×	✓	✓	✓	✓	✓	✓
IP2 PLUS	CL2	×	×	×	×	×	×	×	×	✓	✓	✓	✓	✓
	CL3	×	×	×	×	×	×	×	×	×	✓	✓	✓	✓
IP3	CL2	×	×	×	×	×	×	×	×	×	×	✓	✓	✓
	CL3	×	×	×	×	×	×	×	×	×	×	×	✓	✓
IP4	CL3	×	×	×	×	×	×	×	×	×	×	×	×	✓

OIDC to OIDC Mapping

Mapping Assurance Levels

*Relates to TDIF requirements **FED-04-02-08** to **FED-04-02-10** of section 4.2.2.3 in the TDIF 06 – Federation Onboarding Requirements.*

While *OIDC* does not provide a mechanism for specifying an acr value as a minimum required *ACR,* the **[TDIF.OIDC]** describes a mechanism whereby a *Relying Party* can specify a single *ACR* value.

An example is shown below:

`acr_values` received from the *Relying Party*:

```
acr_values=urn:id.gov.au:tdif:acr:ip3:cl2
```

`acr_values` mapped by an *Identity Exchange* in an *Authentication Request* to the *Identity Service Provider*.

```
acr_values=urn:id.gov.au:tdif:acr:ip3:cl2
urn:id.gov.au:tdif:acr:ip3:cl3 urn:id.gov.au:tdif:acr:ip4:cl3
```

The value of the `acr` claim returned from the *Identity Service Provider* to the *Identity Exchange* as part of the ID Token:

```
"acr":"urn:id.gov.au:tdif:acr:ip3:cl3"
```

Value of `acr` claim returned to the *Relying Party* as part of the ID token

```
"acr":"urn:id.gov.au:tdif:acr:ip3:cl2"
```

The value of the acr returned is the minimum value which the *Relying Party* deemed acceptable for an *Authentication.*

Other OIDC Request Parameters

id_token_hint Parameter

*Relates to TDIF requirements **FED-04-02-12** to **FED-04-02-14** of section 4.2.2.4.2 in the TDIF 06 – Federation Onboarding Requirements.*

Where an *Identity Exchange* receives an `id_token_hint` within an *Authentication Request* from a *Relying Party* the *Identity Exchange* is required to validate the token and extract the subject. This subject is then matched to a subject identifier at the *Identity Service Provider* as per the resolution of a `sub` claim.

OIDC to SAML Mapping

Mapping Claims to Scopes

*Relates to TDIF requirements **FED-04-02-16** of section 4.2.3.1 in the TDIF 06 – Federation Onboarding Requirements.*

Section 4.3.1 of the *TDIF 06D – Attribute Profile* specifies the mapping between *OIDC* claims and their corresponding *SAML Attributes.*

Mapping Assurance Levels

*Relates to TDIF requirements **FED-04-02-17** to **FED-04-02-19** of section 4.2.3.2 in the TDIF 06 – Federation Onboarding Requirements.*

The *ACR* values required by a *Relying Party* are represented in an *OIDC Authentication Request* using either the `acr_values` parameter or the `acr` claim. Required acr values are represented in a *SAML* request using the `<saml:AuthnContextClassRef>` element.

When mapping *OIDC* `acr` requests to *SAML* the same rules apply for *Relying Parties* requesting minimum values when they are translated to *SAML* as they do in *OIDC*, as described above in section 4.1.2.3.

An *Identity Exchange* passes the set of `<saml;AuthnContextClassRef>` values that meet or exceed the value of the requested acr to the *Identity service Provider* in the generated *Authentication Request*. Whether a value meets or exceeds the requested acr value is highlighted in the diagram in section 4.2.1 of this document.

An example is show below:

`acr_values` received from the *Relying Party*:

```
acr_values=urn:id.gov.au:tdif:acr:ip3:cl2
```

`acr_values` mapped to *SAML 2.0* by an *Identity Exchange* in a request to the *Identity Service Provider*:

```
<samlp:RequestedAuthnContext Comparison="minimum">
    <saml:AuthnContextClassRef>
      urn:id.gov.au:tdif:acr:ip3:cl2
    </saml:AuthnContextClassRef>
    <saml:AuthnContextClassRef>
      urn:id.gov.au:tdif:acr:ip3:cl3
    </saml:AuthnContextClassRef>
    <saml:AuthnContextClassRef>
      urn:id.gov.au:tdif:acr:ip4:cl3
    </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

ACR values returned from the *Identity Service Provider* to the *Identity Exchange* as part of the *SAML 2.0* response:

```
<saml:AuthnContext>
    <saml:AuthnContextClassRef>
      urn:id.gov.au:tdif:acr:ip3:cl3
    </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

Value of `acr` claim returned to the *Relying Party* as part of the ID Token

```
"acr":"urn:id.gov.au:tdif:acr:ip2:cl3"
```

max_age Parameter

*Relates to TDIF requirements **FED-04-02-23** of section 4.2.3.3.3 in the TDIF 06 – Federation Onboarding Requirements*

A *Relying Party* may include a value for the max_age parameter in the *OIDC Authentication Request*, as per Section 3.1.2.1 of the **[OpenID.Core]**. This parameter specifies the allowable elapsed time in seconds since the last time the End-User was actively *Authenticated* by the OP. If the elapsed time is greater than this value, the OP must attempt to actively re-authenticate the End-User. There is no equivalent functionality in SAML 2.0 protocol.

The processing rules for how an exchange deals with the receipt of this in an authentication request can be found in section 4.2.2.3.3 of the *TDIF 06Federation Onboarding Requirements*.

SAML to OIDC Mapping

Mapping Attributes to Claims and Scopes

*Relates to TDIF requirements **FED-04-02-34** of section 4.2.5.1 in the TDIF 06 – Federation Onboarding Requirements.*

As in translating the attributes from OIDC to SAML, the mapping of *TDIF Attributes* in *SAML* to *OIDC* is expected to be done using the attribute to protocol mappings found in section 4.3.1. of the *TDIF*: *06D – Attribute Profile*.

Attribute Profile

The *TDIF: 06D – Attribute Profile* is intended to be a live document, and it is anticipated that it will change between periods of maintenance of accreditation. 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*. These *Attributes* will be added to the *TDIF: 06D - Attribute Profile*, a live document which is anticipated to change. During Accreditation, the version of the attribute profile to be used will be agreed on prior to the accreditation process being undertaken.

Attribute Requirements Guidance

*Relates to TDIF requirements **FED-05-01-01** to **FED-05-01-07** of section 5.1 in the TDIF 06 – Federation Onboarding Requirements.*

These requirements specify the *attributes* that must be supported by an *Accredited Participant.* The *TDIF 06D – Attribute Profile* specifies the *attributes* supported in the *Australian Government Digital Identity System*, and specifies what *Attributes* are mandatory and must be provided and which *Attributes* are optional. *Attributes* are divided into *Attribute Sets* (as outlined in section 2.1 of the *TDIF 06D – Attribute Profile)* which 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 use of an *Attribute Set* does not preclude *Attributes* being requested individually by an *RP* to support the principle of only releasing the minimum *Attributes* required.

Section 4 of the *TDIF 06D – Attribute Profile* describes the mapping between the *Attributes* which an *Accredited Participant* is required to support and the *Federation Protocols* supported (*SAML* and *OIDC*).

Furthermore, Appendix C of the *Australian Government Digital Identity System* provides the mapping of the *Attributes* specified in the *TDIF 06D – Attribute Profile* and those which *IdPs* may collect, disclose and verify.

Computed Attributes

*Relates to TDIF requirements **FED-05-02-01** to **FED-05-02-03** of section 5.1 in the TDIF 06 – Federation Onboarding Requirements.*

A *Computed Attribute* is an *Attribute* that is dynamically derived from one or more other *Attributes*. 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 Service Provider*, or by an *Identity Exchange*. In an *Australian Government Digital Identity System* where there are multiple *IdPs*, an *Identity Exchange* can more readily adapt to support the needs of the *RPs* that it supports.

Computed Attributes are synonymous with attribute references defined in the NIST digital identity standards[3]. 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."*

Attribute Service Provider Attributes

*Relates to TDIF requirements **FED-05-03-01** to **FED-05-03-02** of section 5.3 in the TDIF 06 – Federation Onboarding Requirements.*

These *Attributes* are those *Attributes* in the *Australian Government Digital Identity System* provided by *Attribute Service Providers*. When an *Attribute Service Provider* onboards onto the *Australian Government Digital Identity System* it is required under section 3.1 of the *TDIF: 06 – Federation Onboarding Requirements* to publish a

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

schema for any *Attributes* it provides. This schema is utilised to develop the attribute profile to be included in section 5 of the *TDIF: 06D – Attribute Profile.*

Attribute Sharing Policies

*Relates to TDIF requirements **FED-05-04-01** of section 5.4 in the TDIF 06 – Federation Onboarding Requirements.*

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 relation to the operation of *Consent*. Section 2.2 of the *TDIF: 06D- Attribute Profile* states what *Attribute Sharing Policies* are to be applied to each *Attribute Set*. The different *Consent* types are defined below:

Consent Type	Description
Not required	*Consent* is not required for the *Attributes*. In general, this applies to technical attributes that support the operation of the *Australian Government Digital Identity System* rather than *Attributes* that describe an *Individual*.
Single-use	*Consent* is required for the *Attributes* every time a *User Authenticates* to a *Relying Party*.
Ongoing	*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 *Consent* for the *Attributes* every time an *Attribute* has changed. To meet this requirement the *Attributes* have a date time attribute associated with it that that enable an *Identity Exchange* to determine if the *Attribute* has changed since the last time that *Consent* was provided.

The *Attribute Sharing Policies* apply to all the *Attributes* in the *Attribute Set* regardless of whether the *RP* has requested the whole *Attribute Set* or any of the specific attributes comprising the *Attribute Set*.

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

Attribute Data Representation

*Relates to TDIF requirements **FED-05-05-01** of section 5.5 in the TDIF 06 – Federation Onboarding Requirements.*

The requirements around *Attribute* data representation are aimed at ensuring consistency in the *Australian Government Digital Identity System* regarding the format of *Attributes* being shared by participants in the *Australian Government Digital Identity System*. The *Attribute* data representation can be found in section 6 of the *TDIF: 06D – Attribute Profile.*