Australian Government
Digital Transformation Agency

Architecture Overview

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	Apr 2018	TM	Initial version
0.2	Jun 2018	TM	Minor updates
0.3	Sep 2018	TM	Minor updates
0.4	Feb 2019	TM	Incorporated feedback from stakeholders and 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 Trusted Digital Identity Framework (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 provides an architecture overview that describe the functions of the TDIF participants and how they interact.

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 Architecture Overview

2.1 Architecture Overview

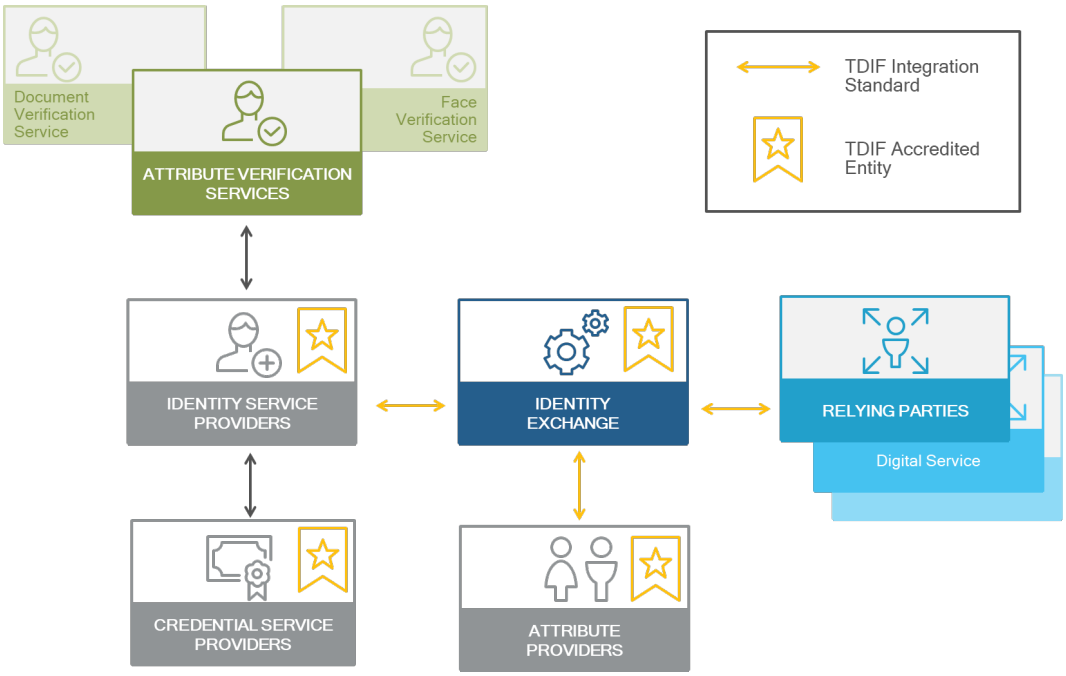
The TDIF Architecture implements a federated model of identity.

Key aspects of the TDIF Architecture include:

- The TDIF sets the standards, policies and compliance requirements for all participants in the identity federation.
- The TDIF Architecture enables the reuse of credentials and verified identity attributes provided by an Identity Service Provider across Relying Parties. The verified identity attributes support the registration of an individual at a Relying Party and the credentials enable ongoing access to the digital services provided by the Relying Party.
- The TDIF Architecture implements a federated model of identity. An implementation of an identity federation that complies with the TDIF, and hence the conceptual architecture described here, is referred to as the TDIF identity federation.
- A broker called the Identity Exchange mediates all interactions between Identity Service Providers, Attribute Providers and Relying Parties.
- An Identity Exchange provides a privacy barrier between Identity Service Providers and Relying Parties. Neither party can identify the other during an interaction.
- 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. 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 IdP binds the verified digital identity attributes to a credential to create a digital identity.

- An Exchange may mediate interactions with additional Attribute Providers to support the sharing of attributes that are in addition to the core identity attributes available for individuals from Identity Service Providers.
- Identity Service Providers, Attribute Providers, and an Identity Exchange must all be highly available and reliable to support the effective functioning of the digital identity eco-system.
- The TDIF Architecture supports the needs of Individuals accessing digital services as a natural person. This architecture can be extended to support other identity contexts, e.g. where an Individual as acts on behalf of an organisational entity such as a registered business entity (ABN).
- TDIF provides the technical integration standards for the interactions between the key components in the identity federation. These technical integration standards are based on standard technical federation protocols to minimise the barriers for Identity Service Providers and Relying Parties onboarding to an Identity Exchange.
- Central to the TDIF Architecture is a user-centred design process (Service Design) that considers the end-to-end user journey to ensure digital identity solution effectively meets the needs of the individuals that need to use it.

Figure 1: *TDIF Conceptual Architecture.*



2.2 The importance of Service Design

Service Design is an important aspect of the implementation of a digital identity eco-system. Some the key challenges that service design needs to address in the context of a federated digital identity eco-system are:

- Ensuring that the end-to-end process is accessible and integrated in a way that ensures digital identity becomes an enabler rather than a barrier to inclusive access.
- Ensuring that the user is not over-burdened with additional concepts and a need to understand the technical underpinnings of the conceptual architecture in order to use their digital identity to access services.
- In a brokered model, such as the TDIF identity federation, understanding the extent to which the broker, the Identity Exchange, needs to be a visible actor in interactions that involve a digital identity.
- Ensuring the eco-system can support the individual to make the choices that best meets their needs.
- Ensuring the eco-system provides services that supports the needs of all users, includes those that are “identity poor” and those that have been victim of identity theft. This includes ensuring that non-digital processes are available to support people who are unavailable to complete the identity verification in a wholly digital process.

2.3 Key concepts.

The *TDIF: Overview and Glossary* provides a high-level overview of the TDIF including its scope and objectives and the definition of key terms.

2.3.1 Key Entities

The key entities in the TDIF identity federation are:

- *Relying Party (RP)*. A Relying Party is an organisational entity that provides Digital Services.
- *Identity Exchange*. An Identity Exchange is the authentication and attribute broker in a TDIF identity federation.

The following entities that are used to provide identity related services to Relying Parties via an Identity Exchange:

- *Credential Service Provider (CSP)*. A Credential Service Provider issues and manages credentials.
- *Attribute Provider (AP)*. An Attribute Provide provides additional verified attributes to support the needs of Relying Parties in the TDIF identity federation. An Attribute Provider needs to be an authoritative source of attributes for the identity federation. Typically, an Attribute Provider will be integrated with a registry that holds the attributes.
- *Identity Service Provider (IdP)*. An IdP manages verified identity attributes and the binding of these attribute to credentials. Conceptually, an Identity Service Provider is a specialised Attribute Provider that is authoritative for the identity attributes of an Individual. An IdP integrates with a CSP to enable authenticated access to the attributes it manages.

- There are additional services in the digital identity eco-system that support the function of the Identity Service Provider.
  - *Attribute Verification Services*. Attribute Verification Services enable the verification of attributes against the authoritative source. Examples are the identity document verification services: DVS and FVS.

2.3.1.1 Relying Parties and Digital Services

Relying Parties are the organisational entities that provide digital services. A Relying Party represents a local domain, or silo, of identity. Within a local domain identity attributes may be shared, and typically there is a common underlying identity record that is a referred to as the customer record, client record, or service record.

To enable access to digital services, Relying Parties need the following:

- Authentication. Individuals need to be able to authenticate to a service using a digital credential such as Username and Password.
- Verified Identity Attributes. The Digital Service may need to know who the Individual accessing the service is by using verified identity attributes such as name and date of birth.
- Additional attributes may also be needed to enable access to the digital service such as:
  - Attributes that describe a qualification that the individual possesses.
  - Attributes that describe an authority or relationship that an Individual possesses, e.g. attributes that describes the ability to act on behalf of another entity to access a digital service.

A Relying Party needs to be able to trust the authentication and attributes. The level of assurance required is determined by the needs of the Digital Service being accessed. Relying Parties may provide many different Digital Services. Each Digital Service may have different identity and attribute assurance requirements. Digital Services can be provided by a Relying Party as:

- Full Digital Services. A digital application that that is directly accessible using a user agent, i.e. a web browser.
- Digital Service access by a Mobile Client. A digital application that is accessed via an installed software client, such as a mobile app.

A single organisation may be composed of a number of Relying Parties. For example, in the Federal Government context the Department of Human Services (DHS) provides services for the Centrelink, Child Support, and Medicare service delivery programs. Each of these service delivery programs is a separate Relying Party.

Conversely a Relying Party may span a number of organisations. For example, some State Government jurisdictions have created a common identity record than spans digital services delivered by a number of agencies.

Because a Relying Party can be composed of many digital services, with potentially these services being provided by different organisational entities, it is important to be able to correct identify what a Relying Party is from the perspective of the TDIF. This relationships between Relying Parties and digital services has the following impact:

- Identity linkages managed by an Identity Exchange occur at the Relying Party level, i.e. all digital services that compose a Relying Party receive the same identity linkage. These linkages are described in section 2.3.2.1.

- Sharing of attributes may be specific to a particular digital service at a Relying Party, so in order for user consent to be also specific, the digital service may also need to be known by the Identity Exchange.

2.3.1.2 Identity Exchanges and Identity Sectors

The TDIF does not require a single Identity Exchange to support the needs of all Relying Parties. The concept of an Identity Exchange that supports an *Identity Sector* can potentially cater for the different needs of Relying Parties in the broader economy. The Commonwealth government will deliver an Identity Exchange that can

be used by government agencies. A public sector jurisdiction such as a State Government or a private sector industry vertical such as the financial sector may need to operate as a distinct identity sector that is serviced by its' own Exchange. Reasons may include:

- Commercial, contractual, and liability considerations.
- Additional regulatory requirements.
- Privacy considerations.
- Implementation complexity, e.g. managing the relationships with Relying Parties, or specific technical integration needs.
- Branding and service design considerations.
- Additional attributes and services that may be required to be supported in that sector.

No specific integration requirements to support interactions between Identity Exchanges are currently elaborated. In an eco-system that can potentially consist of multiple Identity Exchanges, it is envisioned that the following would hold true:

- An Identity Service Provider may integrate with more than one Exchange. Ideally all Identity Service Providers may integrate with all Identity Exchanges.
- A Relying Party will generally integrate with only one Identity Exchange.
- An Identity Exchange may act as an Attribute Provider to another Exchange.
- Integration between Identity Exchanges will leverage the technical integration standards outlined in this document.
- Service design will inform the need for any additional integration standards between Identity Exchanges to ensure the user experience is kept as simple as possible.

2.3.1.3 Identity Service Providers and Credential Service Providers

An identity is fundamentally a collection of attributes that describes an entity. The TDIF defines the attributes that represent an individual. A digital identity associates these attributes with a credential to make these attributes available in a digital eco-system.

An Identity Service Provider is responsible for implementing the business processes that verify identity attributes in accordance with the TDIF.

A Credential Service Provider is responsible for managing the credentials that are used to implement a digital identity.

An Identity Service Provider integrates with a Credential Service Provider to create and manage a digital identity. The roles of Identity Service Provider and Credential Service Provider will typically be performed by the same entity.

2.3.1.4 Attribute Providers

The conceptual architecture can be extended to support the sharing of additional attributes to support the needs of the Relying Parties. Additional attributes are supplied by an Attribute Provider. Specific integration requirements have not been currently elaborated for Attributes Providers. It is envisioned that the following will hold true for Attributes Providers:

- TDIF will define the additional attributes that are applicable across the entire digital eco-system and elaborate any policy constraints on the use of these attributes.
- An accredited Attribute Provider will be required to be authoritative for the attributes that it supplies.
- The participation of an Attribute Provider in the identity and the attributes it provides will be governed by the TDIF Oversight Authority.
- An accredited Attribute Provider will participate in the identity federation in much the same way as an Identity Service Provider.
- Service design will inform any specific integrations standard for an Identity Exchange to support an Identity context.

2.3.2 Identity Federation

The TDIF identity federation implements a brokered model of identity federation. Typically, federations are “one-legged” in that a Relying Party directly integrate with one or more providers of identity services. A brokered model of federation is “two-legged”. On one leg of the federation we have the Relying Parties. Relying Parties are the entities that consume identity services to provide digital services. The other leg are the providers that provide the authentication and attributes that are needed to enable Individuals to access digital services.

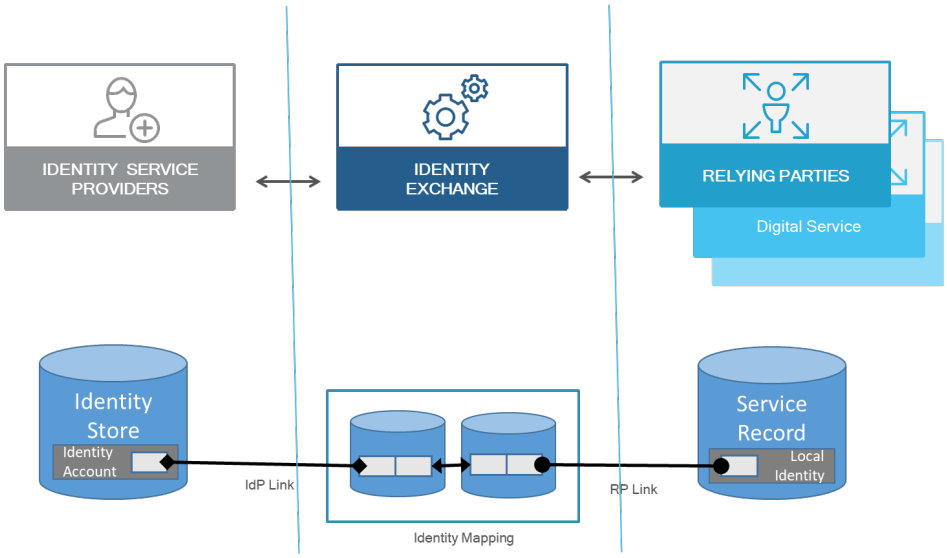
In a TDIF identity federation the authentication and attribute broker is called an Identity Exchange. A TDIF identity federation has the following characteristics:

- Relying Parties onboard to the Identity Exchange.
- Providers of identity services onboard to the Identity Exchange.

- 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 Identity Exchange provides the enforcement point for user consent and visibility to the user of the use of their identity attributes.
- The presence of the Identity Exchange as an intermediary broker results in what is termed a “double blind” federation. 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.

The federated model provides a persistent identifier that a Relying Party can use to identify an individual that can been authenticated via an Identity Exchange. This identifier remains the same for the individual at a Relying Party across interactions with the same Identity Service Provider via an Identity Exchange. These identifiers are pairwise unique identifiers and function as a unique, anonymous link between the identity at the Relying Party and the identity provided by the broker. In the two-legged federations, there is also a pairwise unique identity link between the broker and the Identity Service Provider that identifies the linkage between the Identity Exchange and the identity record held at the Identity Service Provider.

Figure 2: *Identity Linkages in the TDIF identity federation.*



The identity links in a TDIF identity federation are used to support the authentication processes that enable an individual to have ongoing access to digital services at a Relying Party. The authentication process for an individual at a Relying Party typically includes two key steps are follows:

1. Establishing a local identity at the Relying Party. An individual has verified identity attributes at an Identity Service Provider. The individual authenticates at an Identity Service Provider and consents to the release of these verified identity attributes (and possibly additional attributes) to the Relying Party at an Identity Exchange. The Relying Party:

    a. Uses the identity attributes to identity any existing service record that may hold for the individual by performing *Identity Matching*. The Relying Party may need to request additional information from the individual to ensure they have the correct service record. These additional questions together with Identity Matching constitute a process generally called *Proof of Record Ownership (PORO)*. 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.

    b. Creates a service record for the user at the Relying party using the identity attributes if no existing identity record is found.

    c. Stores the RP Link provided by the Identity Exchange if continued access to digital services is required.

2. Ongoing Access Digital Services at the Relying Party. Once the service record at a Relying Party has been established the user can access Digital Services by authenticating at the Identity Service Provider via the Identity Exchange. The Relying Party does not need to repeat any PORO process as it can simply use the RP Link to identify the individual accessing the service.

2.3.2.1 Identity Linkages

The following identity linkages exist as persistent pseudonymous identifiers in the TDIF identity federation:

- IdP Link. This identifier links the identity for an authenticated user at an IDP with the digital identity brokered by an Identity Exchange. This 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 identifier.

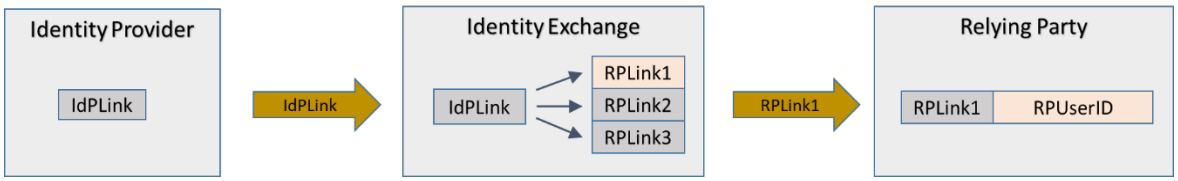
Both the IdP Link and RP Link are implemented using pairwise unique identifiers. An Identity Exchange maintains a mapping between the IDP Link (the identity at an Identity Service Provider) and the RP Link (the service record at the Relying Party).

When a user authenticates to a Relying Party using the services of an Identity Service Provider the same identifier (IdP Link) will be presented to the Relying Party across all authentication events. If a user authenticates to that Relying Party using a second Identity Service Provider, then a different identifier (RP Link) will be presented.

An Exchange employs persistent identifiers as the identity links. When a user returns to an Identity Service Provider they will be associated with the same identifier on every occasion. Similarly, the user will be associated with a constant identifier every time they authenticate to a relying party however the identifier will vary between relying parties.

A generalised depiction of the flow and storage of identity links is shown in Figure 3.

***Figure 3**: Identity Mapping across any Identity Exchange.*

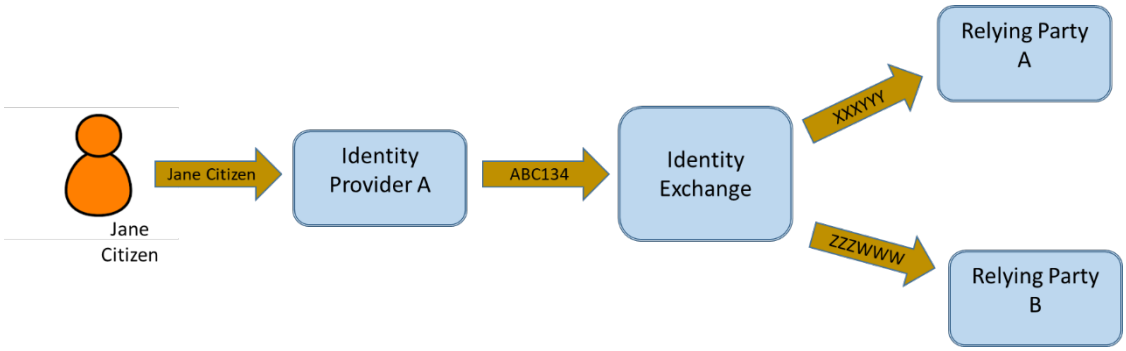


1. The Identity Service Provider persists a single identifier for each unique identity it recognises (IdP Link).
2. At the time of authentication, the IdP Link is passed to the Identity Exchange.
3. The exchange persists the IdP Link against a table of internally generated Relying Party specific identifiers (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 user ID for the service record.

The RP Links generated by an Identity Exchange are generated randomly and stored in an identity mapping database. They are not cryptographically or otherwise mathematically derived from the IdP Links.

An example of identity mapping that occurs in the authentication of a user is shown below:

***Figure 4**: Mapping of a User's identity in an Authentication Event.*



2.3.3 Levels of Assurance and the Concept of Binding

The TDIF defines two Levels of Assurance, the Credential Level (CL) and Identity Proofing Level (IP).

2.3.3.1 Credential Level (CL)

Credential Level (CL) has 3 levels of ascending assurance that indicate the strength of the credential used to authenticate. CL 1 is a single-factor authentication mechanism such as username and password. Multi-factor authentication is required to achieve CL 2. CL 3 imposes further constraints on what credentials may be used, and additional security controls that must be present as part of the credential management process.

2.3.3.2 Identity Proofing Level (IP)

The Identity Proofing Level (IP) indicates the level of assurance associated with the core identity attributes.

In the broadest terms:

- IP 1. Identity attributes are essentially self-asserted by the user.
- IP 2. The identity attributes have been validated as being authentic, but there is only a weak binding to the user presenting them for validation.
- IP 3. As per IP 2, but now there is a strong binding that the user presenting them is the owner of the attributes. Typically, this is accomplished via verifying the user's face against a photo ID document.

- IP 4. As per IP 3, but requires further assurance by being checked against additional identity sources and requiring an in-person interview.

2.3.3.3 Binding of Identity Attributes

Whereas the National Identity Proofing Guidelines (NIPG)[2] focusses on proving the identity of a natural person, the TDIF caters for the digital world when the natural person may not be physically present. To support digital identity, the binding of identity attributes to a natural person needs to be accompanied by an additional binding: the binding to the digital credential. Either the digital credential needs to be used as part of the identity proofing process, or a process that associates verified attributes to a pre-existing digital credential needs to ensure it cannot be intercepted by an imposter.

2.3.3.4 Permissible Combinations of Credential Level and Identity Proofing Level

In general, a higher identity assurance level requires a higher level of credential assurance to ensure that trust is maintained. The TDIF defines the permissible combinations of Credential Level and Identity Proofing Level.

The permitted combinations of Credential Level and Identity Proofing Level are specified by the TDIF in the *TDIF: Identity Proofing Requirements.*

Table 1: *Permissible Combinations of Credential Level and Identity Proofing Level.*

		Authentication Credential Level		
		CL1	**CL2**	**CL3**
Required Identity Proofing Level	**IP1**	Allowed	Allowed	Allowed
	IP2	NO	Allowed	Allowed
	IP3	NO	Allowed	Allowed
	IP4	NO	NO	Allowed

[2] Insert link to NIPG

The most common scenarios for access to digital services that require verified identity will be to require IP 2 or IP 3. The minimum CL for both IP2 and IP3 is CL2.

2.3.4 Identity Attributes

The core identity attributes for an individual are Name and Date of Birth. An IdP will generally also use a verified email address and/or mobile to manage user credential, and these may also be shared with RPs. These attributes that are defined as part of the TDIF are the current minimal set of attributes identified to support the needs of individuals accessing digital services.

Additional attributes will be added in future iterations of TDIF to support the needs of individual and Relying Parties in the digital identity eco-system. These additional attributes will be governed by the TDIF and will specify the consent requirements for these attributes, including any constraints regarding which Relying Parties are able to request and receive these attributes. The TDIF will also detail any trust characteristics that are associated with these attributes, for example whether they are verified or not.

Additional attributes may be supplied to the digital identity eco-system by Identity Service Providers where these attributes are a natural part of managing a person's identity. An example is address attributes. Additional attributes may be sourced from accredited Attribute Providers.

Additional identity attributes beyond the core identity attributes may need to be made available to some Relying Parties as part of an authentication request. An example are attributes relating to the identity documents used as part of the identity verification process. The availability of the attributes will be tightly governed by the TDIF and enforced by an Identity Exchange.

The attributes supported by the TDIF, the source of the attributes, and the applicable attribute sharing policies are defined in the *TDIF: Attribute Profile*. The governance of these attributes is the responsibility of the TDIF Oversight Authority.

2.4 Key digital identity interactions

2.4.1 Overview

The key digital identity interactions that the digital identity eco-system supports are:

- Authentication. Authentication is the end-to-end interaction that occurs when a user (individual) accesses a digital service at a Relying Party that requires authentication and may also require verified identity attributes.
- Identity Proofing. Identity Proofing is the process via which an Identity Service Provider verifies an individual's identity attributes. Identity Proofing may occur as part of an Authentication interaction with a Relying Party
- Credential Management. Credential Management are the processes for managing the credentials that are implemented by a Credential Service Provider.
- Identity Management. Identity Management are the processes for managing the lifecycle of identity attributes that are implemented by an Identity Service Provider.

The authentication interaction is the primary interaction that touches all the components in the digital identity eco-system.

2.4.2 Authentication User Interaction

Figure 5 illustrates the authentication user interaction for an individual accessing a digital service at a Relying Party. From the user's perspective, the key steps in this interaction are:

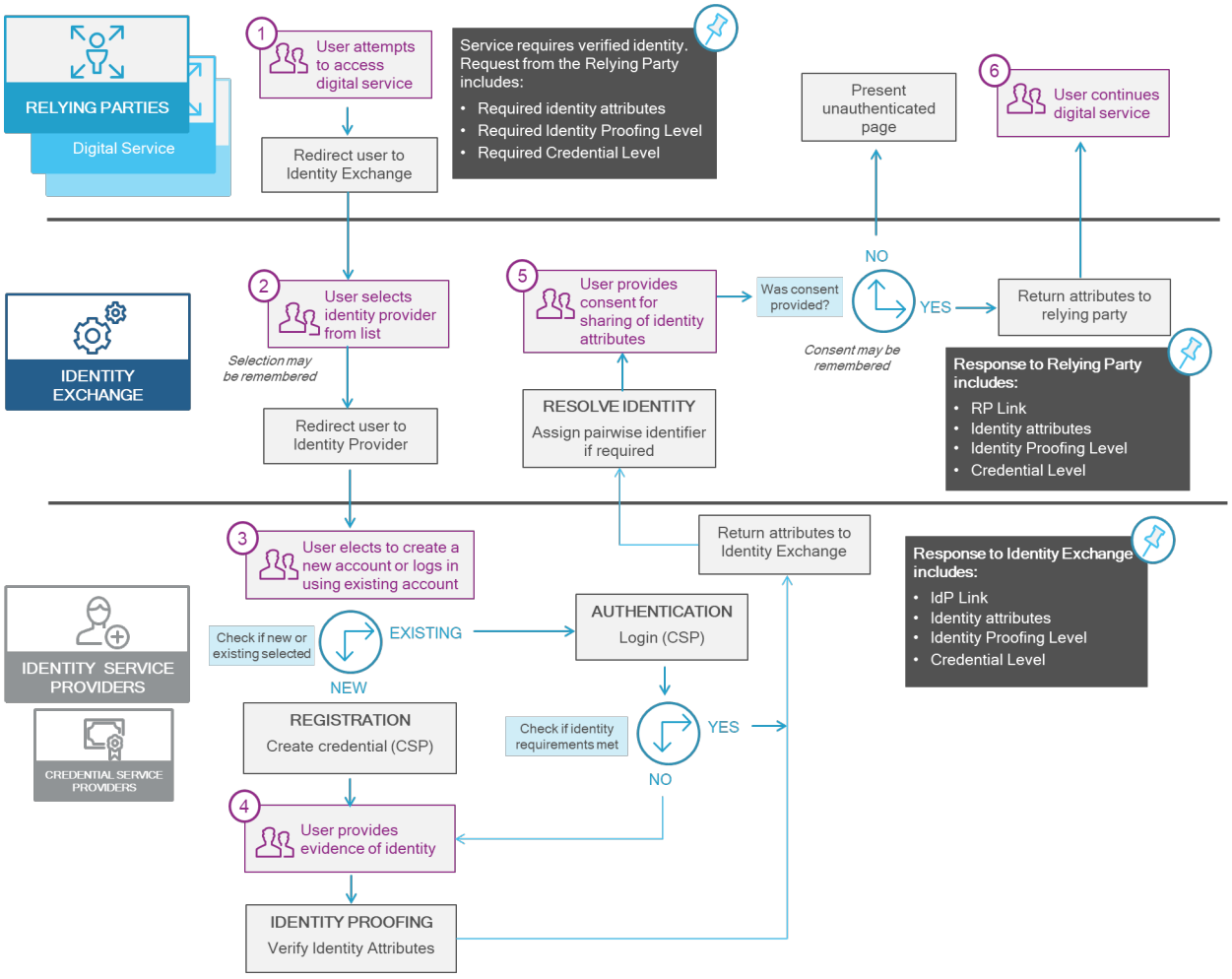
1. The user discovers the digital service at a Relying Party and attempts to access the service.
2. The user chooses the IdP they wish to use to access the service.
3. The user either logs in with their existing account at their selected IdP, or creates an account at the selected IdP.
4. The user proves their identity if they have not previously done this.

5. The user provides consent to share their digital identity attributes with the Relying Party.
6. User is returned to the digital service and they continue with their intended transaction.

Key variants of this interaction include:

- Updating their digital identity, e.g. where a user already has an account at an Identity Service Provider but needs to prove their identity to a higher level.
- Reusing their digital identity at the same Relying Party. In this flow the user has already proved their identity and previously used it to access the Relying Party. The user's selected Identity Service Provider and consent to share attributes may be remembered, so in effect it is a simple authentication-only flow in which the user goes to the service, logs in, and then continues.
- Reusing their digital identity at a different Relying Party. In this flow the user has already proven their identity to the required assurance level, but has not used it to access the Relying Party. The user's selected Identity Service Provider may be remembered, but the user will need to provide the consent to share the attributes with the Relying Party. The user does not have to prove their identity again.
- Completing or commencing identity proofing directly at the IdP. The identity proofing process will generally be triggered by a need to access a digital service, but the user may complete the process of identity proofing independently of accessing a specific digital service. For example, a user may be completing an identity proofing over multiple online sessions, or as a result of a hand-off from a non-digital channel.

***Figure 5**: Authentication User Interactions.*

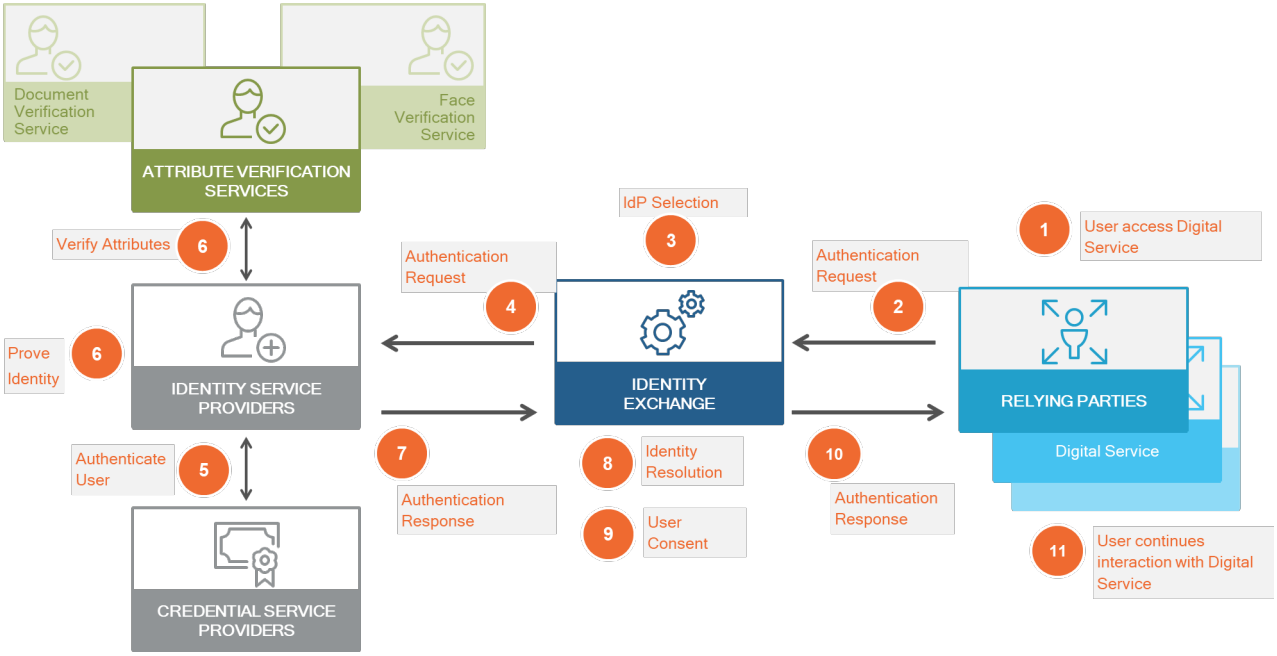


2.4.3 Authentication Entity Interactions

Figure 6 provides an overview of the interactions between the key entities in the digital identity eco-system that occur as part of the authentication user interaction. Technical interactions occur between the following entities as part of this interaction:

1. Between Relying Parties and the Identity Exchanges. This technical integration is implemented in accordance with the technical integration standards specified in the TDIF. These standards use standard federation protocols.
2. Between the Identity Exchange and Identity Service Providers. This technical integration is implemented in accordance with the technical integration standards specified in the TDIF. These standards use standard federation protocols.
3. Between the Identity Service Provider and Attribute Verification Services. The provider of these verification services defines the technical integration requirements.
4. Between the Identity Service Provider and Credential Service Providers. This technical integration is specific to the Identity Service Provider and beyond the scope of the TDIF technical integration standards.

***Figure 6**: Authentication Entity Interactions.*



1. The user discovers the digital service at a Relying Party and attempts to access the service.
2. The user is redirected to the Identity Exchange by the Relying Party. This redirection is an authentication request implemented using a federation protocol. The request to the Identity Exchange includes the attributes, Credential Level, and Identity Proofing Level that the Relying Party requires for the user to access the digital service.
3. The Identity Exchange presents the user with a choice of Identity Service Providers. The user chooses the Identity Service Provider they wish to use to access the service.
4. The Identity Exchange redirects the user to the selected Identity Service Provider. The request to the Identity Service Provider includes the attributes, Credential Level, and Identity Proofing Level that the Relying Party requested in step 1. If the user has previously selected an Identity Service Provider, the selection may be remembered by the Identity Exchange and this step may proceed without any user actions being required.
5. The user logs at the Identity Service Provider using their credential at the Credential Service Provider used by the Identity Service Provider if they already have an account. If they do not have an account then the user will create an

account and be issued with the credentials that meet the required Credential Level.

6. If the user does not already have attributes associated with their account that meets the required Identity Proofing Level then the Identity Service Provider proves the identity by verifying the identity attributes of the user and binding them to the credential. This Identity Proofing may involve numerous interactions with the user and attribute verification services to verify the attributes.
    a. Some users will not be able to satisfy the requirements of the online process in which case, they will exit the process after credential creation and be assisted through a non-digital channel (for example a shopfront).
    b. Some users may not be able to complete the identity proving process in a single online session. They will need to be able to log in to the Identity Service Provider and complete the identity proofing process.
7. The Identity Service Provider redirects the user to the Identity Exchange. This interaction is the authentication response to the authentication request in step 4. The authentication response includes the required identity attributes of the user and the achieved Credential Level and Identity Proofing Level, and the IdP Link for user at the Identity Service Provider.
8. The Identity Exchange resolves the identity for the user at the Identity Service Provider to the identity at the Relying Party by mapping the IdP link from the Identity Service Provider to the RP link for Relying Party. If an RP Link does not exist for the user at the Relying Party then it generates one.
9. The Identity Exchange displays the identity attribute values received from the Identity Service Provider and requests the user's consent to disclose these to the Relying Party. The user provides consent to disclose their identity attributes to the Relying Party. If the user has previously provided consent to the share these attributes with this Relying Party and has permitted the Identity Exchange to remember this consent than this step may process without any user action being required.
10. The Identity Exchange redirects the user to the Relying Party. This interaction is the authentication response to the authentication request in step 7. The authentication response includes the required identity attributes of the user and

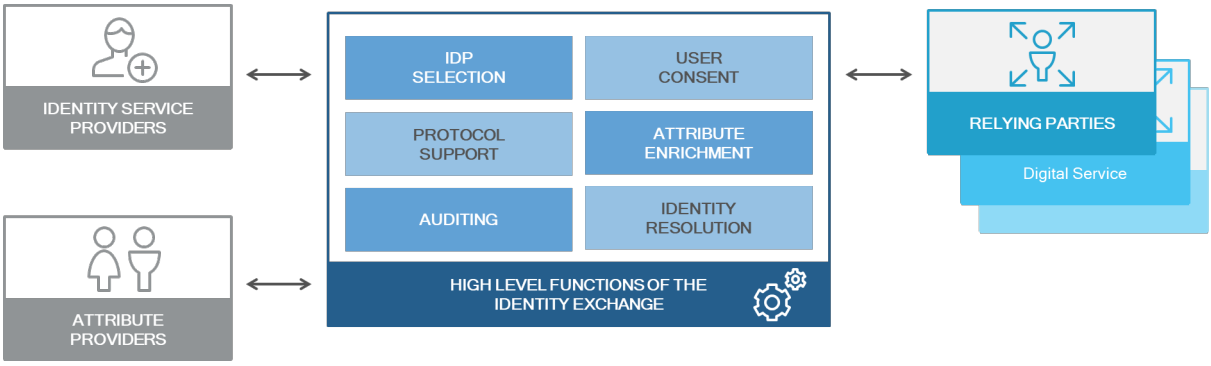
the achieved Credential Level and Identity Proofing Level, and the RP Link for user.

11. The user continues with their interaction with the digital service at the Relying Party.

2.5 Identity Exchange Functional Overview

2.5.1 Overview

Figure 7: *Key Functional Capabilities of an Identity Exchange.*



The key functional capabilities of an Identity Exchange as shown in Figure 7 are:

- IdP Selection.
- User Consent.
- Identity Resolution.
- Protocol Support.
- Attribute Enrichment.
- Auditing.

In addition, an Identity Exchange must implement a User Dashboard to provide a user with an integrated way to manage the use of their digital identity.

2.5.2 IdP Selection

IdP Selection is the function via which an Identity Exchange manages the user's selection of the IdP as part of an authentication interaction.

The IdP Selection function does the following:

- Determines the available Identity Service Providers that can service the authentication request from a RP. The available Identity Service Providers are the subset of Identity Service Providers integrated with an Exchange that are accredited to meet to the required assurance levels required by the Relying Party. The function is termed *IdP Filtering*.
- Interacts with the user so they can choose their preferred Identity Service Provider.
- Provides the user with the option to remember their Identity Service Provider selection. Remembering the Identity Service Provider selection can be done using the user agent (browser). For a web browser this is through the use of a cookie or via HTML 5 storage. The end-to-end service design must provide a mechanism for the user to change this preference and will inform whether there is a need for an Identity Exchange to persist this preference server-side.

2.5.3 User Consent

In the context of Digital Identity, consent refers to a user authorising the disclosure of their identity attributes to a Relying Party. Key privacy requirements relating to consent are detailed in the *TDIF: Privacy Requirements* and includes the need for consent to informed, voluntary, current and specific. An additional privacy requirement relating to the sharing of attributes is the principle of minimum disclosure. Only the minimum information needed to support a Relying Party's transaction should be disclosure. This includes the need to support computed attributes (also termed attribute references) that are derived from raw attribute data but do not include raw attribute data. An example is providing a proof of age attribute rather that the raw date of birth.

An Identity Exchange, unlike an Identity Service Provider or Attribute Provider, has visibility of both the Relying Party a user is wishing to access and the identity attributes being passed from the Identity Service Provider or Attribute Provider. As such, it can enforce a consistent consent mechanism irrespective of the sources of the attributes. Visibility of attributes to the exchange provides the capacity for users to view the actual values they are conveying to the Relying Party and to provide specific

consent on this basis. The user can abandon the authentication interaction if they do not wish to disclose the displayed information to the service.

The user may also be given the option to have their consent remembered and reused for future authentication interactions. This can be viewed or revoked at the User Dashboard. Consent that is persistent across authentication interactions is termed *Ongoing Consent*.

2.5.4 Identity Resolution

Identity Resolution is the process whereby the Identity Exchange maps the identities managed by Identity Service Providers to the records held by the Relying Parties that consume these identities. This is function is central to TDIF federated identity architecture. The mapping of identities performed by an Identity Exchange is detailed in Section 2.3.2.

2.5.5 Protocol Support

An Identity Exchange implements the federated authentication protocols that are specified by the TDIF integration standards. A number of federation protocols exist that can be used to implement the TDIF identity federation including OpenID Connect 1.0 and SAML 2.0. While these protocols can differ markedly in their technical implementation, these protocols provide very similar high level capabilities. The Protocol Support function implements these protocols and manages the onboarding of Identity Service Providers and Relying Parties to the Identity Exchange.

The preferred federation standard for the TDIF identity federation is OpenID Connect 1.0 (OIDC). OIDC is based on a modern collection of standards that simplify the technical integration for Relying Parties and Identity Service Providers.

The technical integration standards for federated authentication will be specified using standard federation protocols. Any additional direct interactions required between components in the digital identity eco-system will be based on web APIs with access authorised using the OAuth 2.0 standard that underpins OIDC.

An Identity Exchange may also need to support additional federation protocols to support the needs of Relying Parties and Identity Service Providers that wish to integrate with it due to technology or other organisational constraints. To support additional protocols an Identity Exchange must support *Protocol Translation*. An Identity Exchange mediates every interaction between an Identity Service Provider and a Relying Party. As the federation protocols are effectively functionally equivalent, the Identity Exchange can translate between the protocol used by a Relying Party and that of the user's Identity Service Provider. By providing translation between these protocols, the Identity Exchange can allow a Relying Party or Identity Service Provider to use the protocol that best meets its requirements.

At the time of writing, SAML 2.0 is still widely used in federated identity solutions, so a SAML 2.0 profile will be provided that is functionally equivalent to the preferred OIDC-based technical integration standards.

The Protocol Support function includes:

- Implementation of the TDIF integration standards.
- Support for Protocol Translation, as required.
- Management of the federation metadata that support the technical onboarding of Identity Service Providers and Relying Parties.
- Automated provisioning of Identity Service Providers onboarding to the Exchange.
- Automated provisioning of Relying Parties onboarding to the Exchange.
- Providing technology integration environments to support the onboarding process.

2.5.6 Attribute Enrichment

Attribute Enrichment is the function whereby an Identity Exchange may integrate with additional Attribute Providers to provide additional verified attributes to Relying Parties in a TDIF identity federation.

Following the authentication by the Identity Service Provider, if there are gaps in the list of attributes that the Relying Party requested that were not satisfied by the Identity Service Provider, the Identity Exchange will retrieve those attributes from the relevant Attribute Provider.

Some attributes may be scoped to some Relying Parties. That is, they can only be requested by some Relying Parties and not others.

Attributes will also be scoped as to who can assert them. Only attributes for which they are authoritative may be expressed as verified attributes by any of the Identity Service Providers or Attribute Providers.

2.5.7 Auditing

The Identity Exchange's unique position in the identity federation 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 TDIF identity federation. An Identity Exchange is the only party that has visibility of what identity attributes are being shared with a Relying Party, and what Identity Service Provider was the source of those attributes.

Information logged by the exchange will be limited to that required in order to meet forensic and non-repudiation requirements defined by the TDIF. The name of identity attributes that were shared via the Identity Exchange will be retained as part of the audit history, but the values of these attributes will not be retained. The TDIF technical integration standards provide for traceability in the authentication interactions between a Relying Party and Identity Service Providers via an Identity Exchange.

2.5.8 Consumer History

All information recorded about users' digital identity interactions will be able to be viewed at the *User Dashboard*, including for each interaction:

- Attributes requested by a Relying Party.
- Consent provided.
- Attributes returned to a Relying Party (but not the actual values returned).

2.5.9 User Dashboard

The User Dashboard is a user interface where the user can view their consumer history and manage their consent preferences. The User Dashboard may be

presented as an integrated part of a broader set of common services for an individual. An Identity Exchange may exist alongside other common platforms or a common access point such as a Whole-of-Government portal that supports digital access to Relying Parties.

The user will need to be authenticated by an Identity Service Provider to access the User Dashboard and will be provided with a view of the digital identity interactions they have undertaken using that Identity Service Provider.

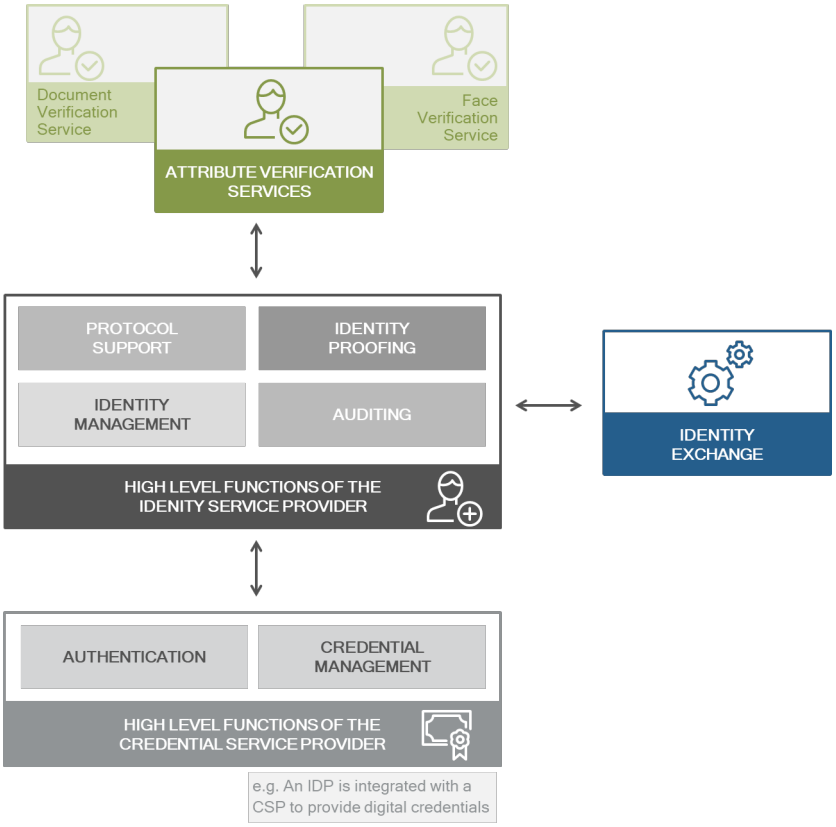
Subject to service design, this view may include:

- Consumer History. A listing of the Relying Parties that a user has interacted with via the Exchange, and which attributes (but not values) were shared.
- Consent Management. Where a user has chosen to have their consent remembered, they will be able to see all such ongoing consent, as well as having the option to revoke it.

2.6 Identity Service Provider Functional Overview

2.6.1 Functional Overview

Figure 8 *Key Functional Capabilities of an Identity Service Provider.*



An Identity Service Provider (IdP) is the entity that provides Relying Parties with verified identity attributes. The responsibilities of an Identity Service Provider are broad and include:

- Verification of identity attributes.
- Binding of a credential to identity attributes.
- Storage of identity attributes.
- Management of identity attributes (e.g. change of name).

An Identity Service Provider integrates with a Credential Service Provider (CSP) that provides:

- Authentication.

- Management of credentials.

2.6.2 Protocol Support

An Identity Service Provider integrates with an Identity Exchange by implementing the federated protocols specified by the TDIF integration standards.

2.6.3 Identity Proofing

Identity Proofing is the function via which identity attributes are verified in conformance with the TDIF Identity Proofing standards.

A key element of the identity proofing process is the verification of identity attributes using identity documents such as a birth certificate. By verifying the attributes on a set of documents that should only be in the possession of the subject of those documents, we can connect the attributes in those documents to that person. In a digital process, as we do not have access to the physical documents, we ask the user to provide the information from the documents and then verify that information at the issuer of the particular document.

An Identity Service Provider uses Attribute Verification Services to verify identity attributes at their source. For attributes that are based on identity documents these attributes can be verified using the Document Verification Service (DVS). For photo ID documents that include a biometric facial image, The Face Verification Service (FVS) can be used as part of digital process to verify that the person that presented the photo ID document is the owner of the photo Id document. Use of a photo ID enables a higher level of assurance to be achieved in the identity verification process.

Digital verification of a photo ID has the following key aspects:

- Capture of a facial image of sufficient quality to enable biometric verification.
- Liveness testing to ensure that image is that of real, present person and is not being substituted (e.g. holding up a photo to the camera).
- The image and photo data is sent to the FVS for verification, the FVS brokers the interaction with the issuer of the photo ID to perform the biometric verification.

- The image captured by the Identity Service Provider for the purposes of verifying ownership of a photo Id is not retained by the Identity Service Provider.

In addition to the digital processes that support identity proofing an Identity Service Provider may need to provide in-person services to support the identity proofing process via a non-digital channel. These in-person identity verification processes will typically be provided via a shopfront and support:

- Fully non-digital identity proofing processes with a subsequent handoff to a digital channel to enable the creation of a digital identity.
- Digitally assisted processes whereby identity verification can be partially complemented digitally with a handoff to a non-digital channel to complete the verification.

A critical element in any cross channel handoff or post-verification creation of a digital identity is ensuring that integrity of the binding between the verified attributes and the credential is not compromised. This ensures that a digital imposter cannot claim the verified attributes.

2.6.4 Identity Management

Identity Management is the function that manages the lifecycle of identity attributes at an Identity Service Provider.

The Identity Service Provider must securely store the following identity data for a user:

- Identity attributes defined by the TDIF.
- IP Level for any verified identity attributes.
- A record of any change in the identity attributes that includes details of any identity documents that were provided as part of the change.

An Identity Service Provider must support the following key lifecycle events:

- Creation of an identity record, i.e. registration.
- Verification of identity attributes as part of identity proofing processes. In many instances this process will be re-entrant, i.e. will be required to be completed over

a number of interactions, with these interactions potentially spanning digital and non-digital channels.

- Change in the identity attributes, these changes will also require verification.
- Upgrade of IP Level, if the Identity Service Provider supports multiple IP Levels.
- Maintenance of identity data in accordance with the TDIF, e.g. implementing any requirement for re-attestation of identity attributes or expiration of unused identity records.

2.6.5 Auditing

Information logged by an Identity Service Provider will be limited to that required in order to meet forensic and non-repudiation requirements defined by the TDIF.

At a minimum, an Identity Service Provider (and any integrated CSP) will need to able to provide an audit trail for all:

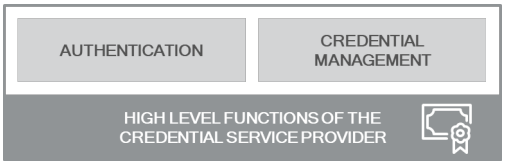
- Authentication events.
- Credential management events.
- All identity proofing events.

The Identity Service Provider must provide an authenticated user will a viewable history of these events.

2.7 Credential Service Provider Functional Overview

2.7.1 Overview

***Figure 9**: Key functional capabilities of a Credential Service Provider.*



A Credential Service Provider (CSP) is integrated with an Identity Service Provider to provide authentication (login) and credential management. A Credential Service Provider does not connect directly to an Identity Exchange. A CSP may be

implemented by the same organisational entity that implements the Identity Service Provider, or it may be delivered by an entity that is external to the Identity Service Provider. A CSP could support more than one Identity Service Provider, and an Identity Service Provider could use more than one CSP to provide a wider range of credentials.

2.7.2 Authentication

Authentication is the use of digital credentials to provide authentication mechanisms that can be used by a person to login.

A Credential Service Provider can support a variety of credential types. The different types of credentials and the Credential Level that they support is detailed in the *TDIF: Authentication Credential Requirements*. Both CL 2 and CL 3 require the use of at least two authentication factors. These credential requirements are summarised in Table 2 that has been reproduced from the *TDIF: Authentication Credential Requirements.*

Examples of credentials include:

- Memorised Secret.
- Look-Up Secret.
- Out-of-Band Devices.
- Single-Factor One-Time-Password (OTP) Device.
- Multi-Factor OTP Device.
- Single-Factor Cryptographic Software.
- Single-Factor Cryptographic Device.
- Multi-Factor Cryptographic Software.
- Multi-Factor Cryptographic Device.

The TDIF authentication credentials are based on the authenticators and assurance levels defined in the NISI publication NIST SP 800-63B. The NIST Authenticator Assurance Levels (AAL) equate to TDIF CLs. NIST 'authenticator' requirements equates to TDIF credential requirements.

***Table 2**: Summary of Authentication Credential Requirements.*

Credential Objectives	**CL1**	**CL2**	**CL3**
Confidence	Provides some confidence that the person controls a credential bound to their IdP account	Provides moderate confidence that the person controls credential(s) bound to their IdP account	Provides high confidence that the person controls credential(s) bound to their IdP account
Individual confirms possession via	A single factor authentication	Multi-factor authentication (MFA)	MFA, inclusive of a hardware based credential
Credential Strength	Refer to NIST SP 800-63B in relation to credential types and the requirements applicable to the respective CLs		
Example Credential Types	Refer to NIST SP 800-63B 4.1.1	Refer to NIST SP 800-63B 4.2.1	Refer to NIST SP 800-63B 4.3.1
Intended use	For low risk, low value services where fraud will have only minor consequences (eg. provision of utility services)	For moderate risk, or moderate value with serious consequences from fraud (eg. provision of common government services such as issuing licences, access cards, or undertaking financial exchanges).	For high risk, or services where very serious consequences arise from fraudulent verifications. (eg. provision of trusted government credentials, such as passports, secure access, etc, or to proof 'trusted' roles such as privileged positions)

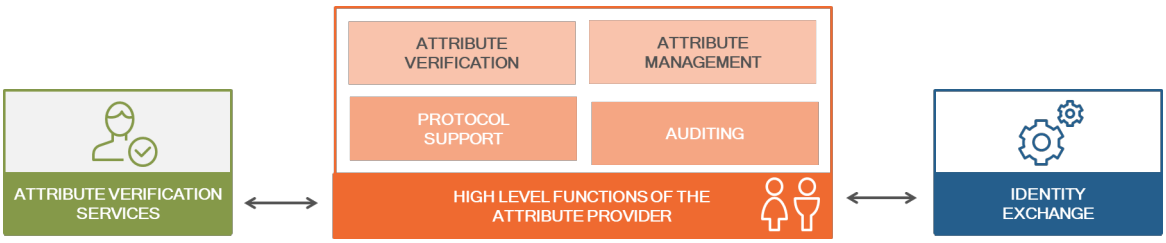
2.7.3 Credential Management

The credential management function manages the lifecycle of a digital credentials from issuance through to revocation. Credential management processes that are required to support the different credential types are specified in the *TDIF: Authentication Credential Requirements.*

2.8 Attribute Provider Functional Overview

2.8.1 Overview

Figure 10: *Key functional capabilities of an Attribute Provider.*



An Attribute Provider is an entity that is integrated with an Identity Exchange to support the provision of additional attributes to Relying Parties. An Identity Service Provider is a specialised Attribute Provider that provides verified identity attributes. An Identity Exchange may integrate with additional Attribute Providers to provide additional attributes that are required by the Relying Parties in a TDIF identity federation. These additional attributes may include:

- Additional attributes relating to the Individual that relate to a common need across digital services provided by Relying Parties.
- Additional attributes that describe a qualification or authority held by an Individual.
- Additional attributes that describe an entitlement held by the individual.
- Additional attributes that describe relationships to other entities, e.g. organisational entities and the scope of that relationship, i.e. any authorisations that may be attached to the relationship.

Some of the key features of an Attribute Provider worth noting are:

- An Attribute Provider must be authoritative for the attributes that they provide.

- An Attribute Provider will typically be integrated with a Registry that manages the attributes. This integration may be by the Attribute Provider entity:
    - Being implemented by the same entity that operates the Registry.
    - Integrating with the Registry operated by a different entity via technology interfaces provided by the Registry. In this instance, the Registry acts as an Attribute Verification Service.
- An Attribute Provider operates within the policy framework of the TDIF, and complies with the overarching privacy principles of the TDIF identity federation.

The functions of an Attribute Provider are not detailed here as they are special-purpose entities designed to meet a specific need. This need may be globally relevant to the eco-system, or specific to a community of Relying Parties. The conceptual architecture can be extended to support additional attributes in concert with a consideration of the following aspects:

- TDIF policy aspects such as legal, regulatory, privacy and security impact.
- Service design impacts on the end-to-end user journey for digital identity.
- Accreditation requirements for Attribute Providers. In order to be the trusted provider for attributes in the digital eco-system an Attribute Provider will need to be accredited in the same way as an Identity Service Provider, but without meeting the specific functional requirements that relate to identity proofing and credentials.

Existing entities in digital identity eco-system could potentially also the perform the role of an Attributes Provider, e.g. a Relying Party that provides digital services may also be authoritative for some additional attributes required by other participants in the identity federation.

Key interactions that an Attribute Provider will have with an Identity Exchange are as follows:

- Attribute Binding. The attributes managed by an Attribute Provider need to be bound to the digital identity brokered by an Identity Exchange. The user will need to be authenticated to the Attribute via the Identity Exchange using an Identity Service Provider. The user will then need to verify that they own the attributes, i.e. bind them to their digital identity. The process of binding these attributes may require the use of verified identity attributes provided by an Identity Service

Provider via the Identity Exchange. To enable this an Attribute Provider is integrated with the Identity Exchange in the same way as a Relying Party. This attribute binding process can be implemented using the same federation model and protocols that underpin the TDIF Architecture. If the attribute binding process can be achieved to different levels of assurance then a trust model will need to be developed to describe and govern these additional attributes.

- Attribute Retrieval. Having established a linkage to the attributes provided by an Attribute Provider, these attributes need to be made available to the Relying Parties via the Identity Exchange by:
  - Enabling user consent for these attributes, and catering for any additional policy constraints that may further constrain the Relying Parties that may receive these attributes.
  - Integrating an API provided by the Attribute Provider with the Identity Exchange to enable the retrieval of the attributes.

2.9 Attribute Verification Service Functional Overview

An Attribute Verification Service is used by an IdP to verify identity attributes against the authoritative source. An example of Attribute Verification Services are the National Attribute Verification Services operated by the Commonwealth of Australia that can be used to support identity proofing processes.

2.9.1 National Attribute Verification Services

The Commonwealth of Australia operates the following attribute verification services:

- Document Verification Service (DVS).
- Face Verification Service (FVS).

Most government issued documents can be verified via the Document Verification Service (DVS). The DVS provides a hub that brokers verification requests to the issuers of government documents.

The FVS provides a similar service to DVS, except that it caters for the verification of photo ID documents such as passports, immigration cards, and driver's licence. The verification request to the FVS includes a biometric quality image of the person that is

claiming to own the photo ID as well as the document details. The request for biometric image matching is brokered to the services that provide the biometric matching services for the relevant document issuer. A positive biometric match enables the requestor to bind the attributes on the identity document to the person presenting the document.

Attributes that are based on identity documents can be verified using the Document Verification Service (DVS). For documents that include a biometric image of a person, i.e. a photo ID, the Face Verification Service (FVS) can be used to achieve a higher level of assurance in the identity verification process. To ensure information is not leaked by the services, both the DVS and the FVS operate in the same way. Details requiring verification are sent to the document issuers and a yes/no answer is returned indicating whether the information is has been matched. Information about source documents cannot be retrieved.

All biometrics are probabilistic in nature, so the use of facial biometric matching to support the identity verification processes contains a number of inherent risks. These risks relate to the quality of the biometric matching process as well as vulnerabilities in the biometric matching process. In the context of digital identity these risks arise due to the:

1. Capture of facial images from uncontrolled consumer devices.
2. Vulnerabilities that may arise in the facial capture process, such as an impostor attempting to impersonate individuals by presenting fake or stolen facial images.
3. Biometric using a diverse set of algorithms from different biometric matching providers across source documents such Passports, Immigration documents, and Driver's Licences. This risk is compound by the use of diverse biometric datasets for photo IDs, e.g. driver's licence images from different jurisdictions.
4. The need to separately tune and refine the performance of each of the biometric matching processes above.

It is the responsibility of an Identity Service Provider to implement measures to address risks 1 and 2 as these arise during the interaction with the user. It is the responsibility of the FVS operator is conjunction with the source agencies to monitor and improve the quality of the biometric matching processes to address risks 3 & 4.

2.10 Conceptual Data Model

This section provides a high level conceptual overview of the functional data held by a Credential Service Provider, Identity Service Provider and Identity Exchange. Any specific technical requirements that relate to this data, such as retention periods for audit trails, are detailed in the *TDIF: Technical Requirements*.

2.10.1 Functional Data held by the Credential Service Provider

2.10.1.1 Credentials

A Credential Service Provider implements authentication mechanisms that use digital credentials. To manage their credentials a Credential Service Provider must use a secure credential store that contains user identifiers and credentials. Credentials may include shared secrets and cryptographic keys that support the authentication mechanisms.

2.10.1.2 Authentication Events

The audit history of a Credential Service Provider provides a record of all authentication events for a user.

The Audit History for an authentication event includes:

- Timestamp.
- Unique authentication Id. Each authentication event must have a unique identifier.
- User Identifier. The unique identifier that identifies the user at the IdP.
- Credential Types Used. A multi-factor authentication mechanism uses more than one digital credential.
- CL Level. Achieved authentication assurance for the authentication event.

Each authentication event log must have a unique identifier that can be used to by an Identity Service Provider to correlate the authentication events with identity proofing events.

2.10.1.3 Credential Management Events

In addition, a Credential Service Provider must record an audit record for all credential management events such as:

- Issuance & Revocation.
- Credential Change - e.g. change or reset a password.
- Credential Status Change. Any change in the status of credential e.g. activation/deactivation.

2.10.2 Functional Data held by an Identity Service Provider

2.10.2.1 Identity Attributes

An Identity Service Provider stores an identity record that contains attributes for an individual. The identity attributes that an Identity Service Provider stores for an individual are specified in the *TDIF: Identity Proofing Requirements.*

In addition to the identity attributes, the Identity Service Provider must also record the IP Level for those attributes and the status of that identity record, e.g. current, historical, revoked. An individual may upgrade or change their identity attributes and this will the creation of a new local identity record.

2.10.2.2 Identity Proofing Events

For each identity record stored by an Identity Service Provider, the Identity Service Provider must store the details of how the identity attributes were verified to achieve the IP Level. This identity proofing event data includes:

- Timestamp.
- Unique authentication event id. To tie the identity proofing event to the authentication event at the Credential Service Provider.
- Identity Record Identifier. Unique Identifier for the identity record.
- IP Level. Achieved IP level for the attributes verified.
- Documents used to verify the identity attributes. The IdP will need to store key information for each of the documents used in an identity verification events including:
    - Document Type.

- Document Issuer.
- Document Identifiers.
- Identity data used in the verification process, e.g. names, date of birth.

To provide an audit trail for a verified identity, an Identity Service Provider need only provide a persistent store for the successful document verifications. An Identity Service Provider may also store failed verifications for the purposes of service monitoring and fraud monitoring.

The document data recorded by the Identity Service Provider corresponds to the data that is required to be sent to the attribute verification service for that document type, e.g. DVS.

There will be no storage of any biometric data used for identity proofing by an Identity Service Provider.

2.10.2.3 Audit History

All access to or use of identity records must be recorded. The access could be by Individuals themselves, or an authorised administrator at the Identity Service Provider.

This audit history will include a:

- Timestamp.
- Unique Identity Record Id. Each authentication event must have a unique identifier.
- User Identifier. The user who accessed the identity record.
- Unique authentication event id.
- Access Type. Generally CRUD-type operations - Create, Read, Update, Delete.

2.10.3 Functional Data held by an Identity Exchange

2.10.3.1 Identity Mapping

An Identity Exchange maintains the following identity mappings:

- Relying Party to Identity Exchange Mapping. This identifier is referred to as the Relying Party Link (RP Link).
- Identity Service Provider to Identity Exchange Mapping. This identifier is referred to as the Identity Service Provider Link (IdP Link).

This identity mapping is described in Section 2.3.2.

2.10.3.2 Federation Metadata

Federation Metadata is the data stored by an Identity Exchange used to support the technical integration standards that support the TDIF identity federation. Federation metadata is defined by the federation standards such as OpenID Connect 1.0 and SAML 2.0. Federation Metadata includes:

- Identifiers for the entities (RP, Exchange, IdP) in the federated identity interactions.
- Standard configuration metadata for the federated identity interactions.
- Any cryptographic keys to support the federation protocols, e.g. the keys used to sign the assertions that contain identity attributes.

2.10.3.3 Consent

An Identity Exchange manages the authorisation to share attributes with a Relying Party. An Identity Exchange stores any user consent decisions (grant or deny) that an Individual makes in relation to sharing attributes from an Identity Service Provider or Attribute Provider with a Relying Party.

The Consent data includes:

- Timestamp.
- Duration of Consent. Any time limit on the consent.
- Relying Party. The RP that requested to receive the attributes.
- RP Link. The link to RP that is authorised to receive the attributes.
- IdP/Attribute Provider. The source of the attributes.
- IdP Link/Attribute Provider Link. The link to the identity at the source of the attributes.
- Name of any attribute or attribute set authorised.
- Consent Decision. This may be “grant”, “deny”, or “ongoing”.

In general, consent records are historical records, with the exception of consent that is ongoing. An ongoing consent may be revoked by an individual.

2.10.3.4 Audit History

An Identity Exchange provides a historical record of all federated identity interactions that relate to an individual. This includes any requests and responses between:

- A Relying Party and the Identity Exchange.
- An Identity Service Provider and the Identity Exchange.

The Audit History includes:

- Timestamp.
- Interaction Type. E.g. OIDC authentication request.
- Unique interaction identifier. The Identity Exchange will need to be able to correlate the requests and responses in an interaction.
- Entity. An Identity Service Provider or a Relying Party.
- Entity Link. Any identity link used in the interaction, such as the RP Link or IdP Link.
- Names of any attributes requested or returned.
- Any level of assurance requested or returned.

No identity attribute values are stored in the audit history. An individual will be able to view the audit history by authenticating with the Identity Service Provider that was involved in the interaction.