Australian Government

Digital Identity

06 Federation Onboarding Requirements

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

Contact us

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		Oct 2019	AV	Initial version
0.2		Dec 2019	AV	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4		Mar 2020	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 2021	AV, SJP	CRID0018 – Moved content to the TDIF Functional and Role Requirements documents: See the Change Log for full list of requirements changes.
1.2	4.6	Mar 2022	AV	CRID0028 – FED-02-01-12 – Requirement changed from MAY to MUST
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 tables

Introduction

This document sets out the *TDIF* federation onboarding requirements to be met by an *Applicants* in order to achieve *TDIF* accreditation if they are also seeking to connect to the *Australian Government Digital Identity System*.

These *TDIF* federation onboarding requirements do not replace, remove or diminish existing obligations imposed on government agencies or organisations through other policies, legislation or regulations, or by any other means. These *TDIF* federation onboarding requirements supplement existing obligations and apply specifically to identity services that undergo the *TDIF Accreditation Process*.

The intended audience for this document includes:

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

Technical requirements

2.1 Common functional requirements

2.1.1 Technical integration standards

TDIF Req: FED-02-01-01**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MUST* implement the following profiles as specified in the *TDIF: 06B - OpenID Connect 1.0 Profile*:

a) *Relying Party* to *Identity Exchange* Profile.
b) *Identity Exchange* to *Identity Service Provider* Profile.

TDIF Req: FED-02-01-02**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MAY* implement the following profiles as specified in the *TDIF: 06C - SAML 2.0 Profile*:

a) *Relying Party* to *Identity Exchange* Profile.
b) *Identity Exchange* to *Identity Service Provider* Profile.

TDIF Req: FED-02-01-03**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MUST* implement the *Relying Party* to *Identity Exchange* profile specified in either the:

a) TDIF: 06B - OpenID Connect 1.0 Profile; or
b) The TDIF: 06C - SAML 2.0 Profile.

TDIF Req: FED-02-01-04**; Updated:** Mar-20**; Applicability:** I
The *Applicant* *MUST* implement the *Identity Exchange* to *Identity Service Provider* profile specified in either the:

a) TDIF: 06B - OpenID Connect 1.0 Profile; or
b) The TDIF: 06C - SAML 2.0 Profile.

TDIF Req: FED-02-01-05**; Updated:** Mar-20**; Applicability:** A**,** I, X
The *Applicant* *MUST* test their implementation of a *Federation Protocol* in accordance with the *Technical Testing* requirements set out in section 6 of the *TDIF: 04 – Functional Requirements*.

2.1.2 Security considerations

TDIF Req: FED-02-01-06**; Updated:** Mar-20**; Applicability**: A, C, I X
The *Applicant* ***MUST*** conform to the applicable recommendations in the security considerations section set out in [RFC 6749] and those set out in the 'OAuth 2.0 threat model and security considerations' document [RFC 6819].

TDIF Req: FED-02-01-06a**; Updated:** Mar-20**; Applicability**: A, C, I X
The *Applicant's* conformance with the security considerations ***MUST*** be considered as part of its *System Security Plan* as per PROT-04-01-11a.

2.1.3 Functional data requirements

This section operates in addition to the requirements for *Audit Logs* outlined in section 4.2.6 of the *TDIF 04 – Functional requirements*.

TDIF Req: FED-02-01-07; **Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to PRIV-03-09-03.

TDIF Req: FED-02-01-07a; **Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-02-01.

TDIF Req: FED-02-01-08; **Updated:** Jun-21; **Applicability:** X
The *Applicant's Audit logs* ***MUST*** store a record of all federated identity interactions that relate to an *Individual,* including any requests and responses between a *Relying Party* and an *Identity Exchange*, or an *Identity Service Provider* and an *Identity Exchange*.

TDIF Req: FED-02-01-08a; **Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to PROT-04-02-22e.

2.1.4 Reporting to the Oversight Authority

This section lists requirements to be met by *Applicants* in relation to their reporting obligations to the *Oversight Authority*. These requirements **replace** similar requirements set out in *TDIF 04: Functional Requirements* and *TDIF 05: Role Requirements*. Each requirement below lists the requirement it replaces.

TDIF Req: FED-02-01-09; **Updated:** Jun-21; **Applicability:** A, C, I, X
The *Applicant* ***MUST*** develop and use procedures to report incidents of *fraud* or suspected *fraud* to the *Oversight Authority*

TDIF Req: FED-02-01-09a; **Updated:** Jun-21; **Applicability:** A, C, I, X
As soon as they become aware the *Applicant* ***MUST*** report incidents of *fraud* or suspected *fraud* to the *Oversight Authority* (this replaces FRAUD-02-05-06).

TDIF Req: FED-02-01-09b; **Updated:** Jun-21; **Applicability:** A, C, I, X
The *Applicant* ***MUST*** include the following information when reporting on incidents of *fraud* or suspected fraud:

a) Date and time of the *fraud* incident.
b) Quantity of *fraud* incidents and their level of severity.
c) Time taken to respond to the *fraud* incident.
d) Measures taken in response to the *fraud* incident.

e) Type(s) of fraud.
f) If applicable, the *Identity Proofing Level* and *Credential Level* of the impacted identity record(s).
g) Any other supporting information (e.g. attack vectors used by the fraudster).

Depending on the nature of the *fraud* incident and legal advice obtained, the *Oversight Authority* may advise impacted stakeholders of the outcome of a *fraud* investigation (this replaces FRAUD-02-05--06a).

TDIF Req: FED-02-01-10; **Updated:** Jun-21; **Applicability:** A, C, I, X
An *Applicant*, covered by the *Privacy Act, MUST* report eligible data breaches to affected individuals and the *Information Commissioner* as required under the *Privacy Act*[1] and also report the eligible data breach to the *Oversight Authority* (this replaces PRIV-03-04-01).

TDIF Req: FED-02-01-10a; **Updated:** Jun-21; **Applicability:** A, C, I, X
An *Applicant*, not covered by the *Privacy Act, MUST* report eligible data breaches as defined in the *Privacy Act 1988* to affected individuals and the *Oversight Authority* (this replaces PRIV-03-04-01a).

TDIF Req: FED-02-01-11; **Updated:** Jun-21; **Applicability:** A, C, I, X
The *Applicant MUST* include a statement in their privacy notices advising that the *Applicant* may use the *Individual's* information as required by the *Oversight Authority,* including to detect, manage and investigate fraud (this replaces PRIV-03-05-02).

TDIF Req: FED-02-01-12; **Updated:** Jun-21; **Applicability:** A, C, I, X
The *Applicant MUST* include a statement in their privacy notices advising that the *Applicant* may provide the *Individual's system metadata* to the *Oversight Authority* to enable it to perform the *Oversight Authority*'s functions related to fraud management.

[1] See Part IIIC of https://www.legislation.gov.au/Details/C2019C00025 for the definition of an eligible data breach including exceptions to reporting.

TDIF Req: FED-02-01-13; **Updated:** Jun-21; **Applicability:** A, C, I, X

If it discloses *Personal information* to an overseas recipient that is not the individual, the *Applicant* MUST demonstrate to the *Oversight Authority's* reasonable satisfaction it has appropriate contractual and practical measures to ensure the overseas recipient complies with these *TDIF* privacy requirements (this replaces PRIV-03-10-02a).

TDIF Req: FED-02-01-14; **Updated:** Jun-21; **Applicability:** A, C, I, X

The *Applicant* MUST develop and use procedures that ensure:

a) All elements of the *Applicant's System Security Plan* are achieved.
b) *Cyber security incidents* are investigated, responded to and reported to the *Oversight Authority*.
c) Relevant security policy or legislative obligations are met.

(This replaces PROT-04-01-06).

TDIF Req: FED-02-01-15; **Updated:** Jun-21; **Applicability:** A, C, I, X

The *Applicant* MUST develop and use procedures to report *Cyber security incidents* to the *Oversight Authority*.

TDIF Req: FED-02-01-15a; **Updated:** Jun-21; **Applicability:** A, C, I, X

As soon as they become aware the *Applicant* MUST report *Cyber security incidents* to the *Oversight Authority* (this replaces PROT-04-02-14).

TDIF Req: FED-02-01-15b; **Updated:** Jun-21; **Applicability:** A, C, I, X

The *Applicant* MUST include the following information when reporting *Cyber security incidents*:

a) Date and time of the *Cyber security incident*.
b) Quantity of *Cyber security incidents* and their level of severity.
c) Time taken to respond to the *Cyber security incident*.
d) Measures taken in response to the *Cyber security incident*.
e) If applicable, the *Identity Proofing Level* and *Credential Level* of the impacted identity record(s).
f) Any other supporting information (e.g. attack vectors used).

Depending on the nature of the *Cyber security incident* and legal advice sought, the *Oversight Authority* may advise impacted stakeholders of the outcome of a security investigation (this replaces PROT-04-02-14a).

2.2 Technical testing requirements

TDIF Req: FED-02-02-01**; Updated:** Mar-20**; Applicability:** A, C, I, X
For all the requirements in this document, the *Applicant* *MUST* demonstrate conformance with the *Technical Testing* requirements set out in section 6 of the *TDIF: 04 – Functional Requirements*.

2.3 Feature-specific technical integration requirements

The section sets out the technical integration requirements for specific features of the *Identity Federation*.

2.3.1 Identity resolution

2.3.1.1 Pairwise Identifiers

TDIF Req: FED-02-03-01**; Updated:** Mar-20**; Applicability:** I, X
The *Applicant* *MUST* generate *Pairwise Identifiers* in accordance with section 8.1 of the OpenID Connect Core 1.0 specification [OpenIDCore] and use these to interact with Relying Parties regardless of the *Federation Protocol* the Applicant is using to communicate with other Participants in the *Australian Government Digital Identity System*.

TDIF Req: FED-02-03-02**; Updated:** Mar-20**; Applicability:** I, X
The *Applicant* *MUST* send through a *Pairwise Identifier* in response to a successful *Authentication Request*.

TDIF Req: FED-02-03-03**; Updated:** Mar-20**; Applicability:** X
The Applicant *MUST* use a different *Pairwise Identifier* to an *Identity Service Provider* to identify the subject of an *Authentication* to the *Relying Party*.

TDIF Req: FED-02-03-04**; Updated:** Mar-20**; Applicability:** X

An *Identity Exchange* *MUST* implement an identity mapping process that maps the *Pairwise Identifier* presented by an *IdP* in response to an authentication request to the *Pairwise Identifier* for the user at the *Relying Party* that initiated the *Authentication* interaction.

TDIF Req: FED-02-03-05**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MUST* be able to receive *Pairwise Identifiers* of up to 255 ASCII characters.

TDIF Req: FED-02-03-06**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MUST* support the configuration of a sector identifier for a *Relying Party* in accordance with Section 8.1 of the [OpenIDCore].

TDIF Req: FED-02-03-07**; Updated:** Mar-20**; Applicability:** X
The process for the registration of *OIDC* clients by the *Applicant* *MUST* ensure that only valid and authorised clients for the *Relying Party* can use the same configured sector_identifier_uri.

TDIF Req: FED-02-03-08**; Updated:** Mar-20**; Applicability:** I
The *Applicant* *MUST NOT* generate *Pairwise Identifiers* greater than 255 ASCII characters.

TDIF Req: FED-02-03-09; **Archived:** Jun-21
This requirement has been archived in version 1.1.

2.3.1.2 Deduplication

TDIF Req: FED-02-03-10; **Updated:** Jun-21; **Applicability:** X
The *Applicant* *MUST* have a process to conduct *Deduplication* of *Digital Identities* which pass through an *Identity Exchange* to ensure that a *User* with multiple *Digital Identities* is presented as the same user to a *Relying Party*.

TDIF Req: FED-02-03-11; **Updated:** Jun-21; **Applicability:** X
The *Applicant* *MUST* only deduplicate *Digital Identities* which have been proved to the same *Identity Proofing Level*.

TDIF Req: FED-02-03-12 **Updated:** Mar-20; **Applicability:** I
If the TDIF EDI attribute is requested by an *Identity Exchange*, the *Applicant* *MUST*

return an *EDI* constructed using the document specified in Table 1 (as updated by *Finance* from time to time) according to the *Identity Proofing Level* used in the authentication context.

TDIF Req: FED-02-03-13 **Updated:** Mar-20; **Applicability:** I
The *Applicant* *MUST* return an *EDI* constructed using only such documents specified in Table 1 (as updated by *Finance* from time to time) as are bound to the current authentication context.

TDIF Req: FED-02-03-14 **Updated:** Mar-20; **Applicability:** I
The *Applicant* *MUST* ensure that the documents and attributes used to construct an *EDI* reflect the most up to date documents and attributes bound to the current authentication context.

TDIF Req: FED-02-03-15; **Updated:** Mar-20; **Applicability:** I
When constructing an *EDI* using a document the *Applicant* *MUST* concatenate the document type code *URN* from section 6.1 of the *TDIF: 06D - Attribute Profile* and the attributes specified in Table 2 in the order specified in Table 2, for that document, using the attribute formats specified in Table 3.

TDIF Req: FED-02-03-15a **Updated:** Mar-20; **Applicability:** I
If the *User* has not verified any of the documents in Table 1 (as updated by *Finance* from time to time), the *Applicant* *MUST* construct an EDI by concatenating the *IP Link* for the *User* and a suitable globally-unique identifier for the *Applicant* (e.g. OIDC Issuer URI).

TDIF Req: FED-02-03-15b; **Updated:** Mar-20; **Applicability:** I
The string resulting from either TDIF Req FED-02-03-15 or TDIF Req FED-02-03-15a *MUST* then be encoded using UTF-8, before being hashed using the SHA-256 algorithm.

Table 1: Documents used to build an *EDI*

IP Level	Details
IP 1	The first available document from the following list: 1. Verified Email Address 2. Verified Mobile Number
IP 1 PLUS IP 2 IP 2 PLUS	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa 4. Passport 5. Driver Licence 6. ImmiCard 7. Medicare Card
IP 3	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa 4. Passport
IP 4	The first available document from the following list: 1. Birth Certificate 2. Citizenship Certificate 3. Visa

Table 2: Document Attributes used to build an *EDI*

Document type	Specified Attributes
Passport	• Passport Number
NSW Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
ACT Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
NT Birth Certificate	• Certificate Number if available, else use Registration number

Document type	Specified Attributes
	• Document Date of Birth • Document Issuer State
QLD Birth Certificate	• Certificate Number if Available • Document Date of Birth • Document Issuer State • Registration Date
WA Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • State or Territory of Issue
SA Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State
TAS Birth Certificate	• Certificate Number if available, else use Registration number • Document Date of Birth • Document Issuer State • Registration Date
VIC Birth Certificate	• Registration Number • Document Date of Birth • Document Issuer State
Citizenship Certificate	• Document Date of Birth • Stock Number
Visa	• Document Date of Birth • Foreign Passport Number
Driver Licence	• Licence Number • Document Issuer State
Medicare Card	• Medicare Card Number • Individual Reference Number • Card Colour
ImmiCard	• ImmiCard Number

Table 3: Specified attribute data format

Attribute/sub-attribute	Type	Format	Maximum Length
Document Issuer State	String	Values are “NSW’, “QLD”, “VIC”, “TAS”, “WA”, “SA”, “ACT”, “NT”	3
Document Identifier	String	0 or more characters. This includes Certificate Number, Passport Number, Registration Number, Stock Number, Licence Number and Foreign Passport Number.	50
Document Date of Birth	String	ISO 8601:2004 format: YYYY-MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	10
Registration Date	String	ISO 8601:2004 format: YYYY-MM-DD. Note partial dates are also valid, i.e. YYYY, YYYY-MM	10
Document Country of Issue	String	1 or more characters	50

TDIF Req: FED-02-03-16; **Updated:** Mar-20; **Applicability:** I
The *Applicant* MUST NOT provide access to an *EDI* to any party other than an *Identity Exchange*.

TDIF Req: FED-02-03-17; **Updated:** Mar-20; **Applicability:** X
The *Applicant* MUST NOT store an *EDI* received from an *Identity Service Provider* or use it as their *Pairwise Identifier* for the *User* being authenticated.

TDIF Req: FED-02-03-18; **Updated:** Mar-20; **Applicability:** X
The *Applicant* MUST NOT provide access to an *EDI* to any other party in the *Australian Government Digital Identity System*.

TDIF Req: FED-02-03-19; **Updated:** Mar-20; **Applicability:** X
If the *Applicant* uses the *EDI* to conduct *Deduplication*, it MUST NOT do so across the *Identity Federation*, but instead only conduct deduplication at a sector identifier level.

TDIF Req: FED-02-03-20; **Updated:** Mar-20; **Applicability:** X
The *Applicant* *MAY* request an *EDI* to conduct *Deduplication* as part of an authentication request made to an *Identity Service Provider*.

2.3.2 *Single Sign-on/Single Logout*

TDIF Req: FED-02-03-21**; Updated:** Jun-21**; Applicability:** X
If the *Applicant* supports *Single Sign-on*, it *MUST* support the ability for a *Relying Party* to request *Authentication* for a particular *User* using the method specified in the *Federation Protocol* being used. See section 4.2 for more detail on how an *Identity Exchange* can support this.

TDIF Req: FED-02-03-22; **Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-03-02.

TDIF Req: FED-02-03-23**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-03-02a.

TDIF Req: FED-02-03-24**; Updated:** Mar-20**; Applicability:** C I, X
If the *Applicant* is using securely cached attributes for *Single Sign-on*, and the *Applicant* receives an *Authentication Request* which cannot be fulfilled using the cached information and can't retrieve additional *Attributes* without further requiring user interaction, it *MUST* send an *Authentication Request* to an *Identity Service Provider*.

TDIF Req: FED-02-03-25**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-03-03a.

TDIF Req: FED-02-03-26**; Archived:** Jun-21
This requirement has been archived in version 1.1.

TDIF Req: FED-02-03-27**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-03-03.

TDIF Req: FED-02-03-28**; Archived:** Jun-21

This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-03-04.

TDIF Req: FED-02-03-29**; Archived:** Jun-21
This requirement has been archived in version 1.1.

TDIF Req: FED-02-03-30**; Archived:** Jun-21
This requirement has been archived in version 1.1.

Attribute Service Provider requirements

This section sets out the unique technical requirements that *Attribute Service Providers* must comply with to onboard onto the *Identity Federation* in addition to the other applicable requirements set out in this document.

3.1 Technical requirements

TDIF Req: FED-03-01-01**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MUST* publish a schema for any *Attributes* it provides. This schema must enumerate the valid values for any *Attributes* that have a defined set of values, and be done in a format which complies with the platform through which it provides access to an *Identity Exchange*, and the *Federation Protocols* which a *Relying Party* may use to request the *Attributes* from an *Identity Exchange*.

TDIF Req: FED-03-01-02**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MUST* use the *Pairwise Identifiers* generated by an *Identity Exchange* for it as a *Relying Party* to associate the attributes that it provides with the *Digital Identity* brokered by an *Identity Exchange*.

TDIF Req: FED-03-01-03**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MUST* provide an *API* that enables the attributes it provides to be shared with *Relying Parties*.

TDIF Req: FED-03-01-04**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MUST* authorise an accredited *Identity Exchange* to securely access the *API* it provides.

TDIF Req: FED-03-01-05**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MAY* implement the *API* as a REST *API*.

TDIF Req: FED-03-01-06**; Updated:** Mar-20**; Applicability:** A
Where the *Applicant* provides a *REST API*, the *Applicant* *MAY* authorise access in accordance with the JSON Web Token Profile for OAuth 2.0 Client Authentication and Authorization Grants [RFC 7523].

TDIF Req: FED-03-01-07**; Updated:** Mar-20**; Applicability:** A
The *Applicant* *MAY* allow *Attributes* to be directly requested from it by a *Relying Party* using a security token returned by an *Identity Exchange* to the *Relying Party*.

3.2 Audit logging

These requirements operate in addition to the requirements outlined in the *TDIF 04 – Functional Requirements* specifying what needs to be included in an *Attribute Service Providers audit log*.

TDIF Req: FED-03-02-01**; Updated:** Jun-21**; Applicability:** A
The *Applicant's Audit Log* *MUST* include any *User Consent* managed by the *Applicant* that enables the sharing of attributes with a *Relying Party*.

TDIF Req: FED-03-02-02**; Updated:** Jun-21; **Applicability:** A
The *Applicant's Audit Log* *MUST* include the value of the RP Audit Id *Attribute* received from an *Identity Exchange* for the following events:

- The retrieval of *Attributes* by an Identity Exchange.
- The binding of any *Attributes* to a *Digital Identity* brokered by an *Identity Exchange.*

TDIF Req: FED-03-02-03**; Archived:** Jun-21
This requirement has been archived in version 1.1.

Identity Exchange requirements

This section sets out the unique technical requirements that *Identity Exchanges* must comply with to onboard onto the *Australian Government Digital Identity System* in addition to the applicable requirements throughout the rest of this document.

4.1 Integration requirements

4.1.1 Audit IDs

TDIF Req: FED-04-01-01**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-01-01.

TDIF Req: FED-04-01-01a**; Updated:** Jun-21**; Applicability:** X
In addition to the requirements in section 6.1 of the *TDIF 05 – Role Requirements*, the *Applicant* *MUST* implement the following requirements.

TDIF Req: FED-04-01-02**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-01-02.

TDIF Req: FED-04-01-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* provide the unique audit id described in IDX-06-01-01 to the *Relying Party* using the RP_audit_id *Attribute* in response to every logical interaction between a *Relying Party* (including an *Attribute Service Provider*) and an *Identity Exchange*.

TDIF Req: FED-04-01-04**; Updated:** Jun-21**; Applicability:** X
When the *Applicant* calls an *API* provided by an *Attribute Service Provider*, they *MUST* include the value of the unique audit id that has been generated by the *Identity Exchange* for the *Relying Party* that requested the *Attributes*.

TDIF Req: FED-04-01-05**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST NOT* send the unique audit id that has been generated by the *Identity Exchange* for the *Relying Party* that requested the *Attributes* to an *Identity Service Provider*.

4.1.2 Audit history, consumer history and user dashboard

TDIF Req: FED-04-01-06**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* implement a *User Dashboard* in accordance with the requirements in section 6.4 of the TDIF 05 – Role Requirements.

TDIF Req: FED-04-01-07**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-04-02.

TDIF Req: FED-04-01-08**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-04-03.

4.1.3 Attribute Service Provider integration

TDIF Req: FED-04-01-09; **Updated:** Mar-20; **Applicability:** X
When the *Applicant* receives an *Authentication Request* from a *Relying Party* that includes *Attributes* supplied by an *Attribute Service Provider* then it *MUST* call the *API* provided by the *Attribute Service Provider* to make these *Attributes* available to the *Relying Party* in the *Authentication* response.

TDIF Req: FED-04-01-10; **Updated:** Mar-20; **Applicability:** X
The *Applicant* *MAY* make *Attributes* requested by a *Relying Party* available by authorising the *Relying Party* to directly retrieve the *attributes* from the *Attribute Service Provider* using a security token, if a *Relying Party* has requested to do so.

TDIF Req: FED-04-01-11; **Updated:** Mar-20; **Applicability:** X
Security tokens issued by the *Applicant* to a *Relying Party* *MUST NOT* reveal the *Pairwise Identifier* of the *User* at the *Attribute Service Provider*.

TDIF Req: FED-04-01-12**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MUST* call an *Attribute Service Provider's API* using the *Pairwise Identifier* it has issued to assist in identifying the required *Attributes*.

4.1.4 IdP selection

TDIF Req: FED-04-01-13**; Archived:** Jun-21**; Applicability:** X
The *Applicant* *MUST* implement *IdP Selection* in accordance with the requirements in section 6.5 of the *TDIF 05 – Role Requirements*.

TDIF Req: FED-04-01-14**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-05-01b.

TDIF Req: FED-04-01-15**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-05-02a.

TDIF Req: FED-04-01-16**; Archived:** Jun-21
This requirement has been archived in version 1.1. The content of this requirement has been moved to IDX-06-05-02.

4.2 Federation protocol mapping requirements

The following requirements describe how an *Identity Exchange* performs mapping of *Federation Protocols*. Applicability of these requirements is dependent on what *Federation Protocols* the *Identity Exchange* supports.

TDIF Req: FED-04-02-01; **Archived:** Jun-21
This requirement has been archived in version 1.1.

4.2.1 Levels of Assurance

Levels of Assurance are special *Attributes* used to describe the *Identity Proofing Level* and *Credential Levels* described in the TDIF. The *Levels of Assurance* used in the *Australian Government Digital Identity System* are defined in Table 4: Level of Assurance Combinations. *Levels of Assurance* are ranked from the lowest degree of confidence in the *Authentication* process to the highest degree. *Relying Parties* are given the option of requesting a minimum level of assurance in both the *TDIF 06B –*

OpenID Connect 1.0 Profile and the *TDIF 06C – SAML 2.0 Profile*, with the rankings of *ACR*s specified in Table 4**:** Level of Assurance Combinations.

Table 4: Level of Assurance Combinations.

IP Level	Credential Level	URN	Ranking (Lowest to Highest)
IP1	CL1	urn:id.gov.au:tdif:acr:ip1:cl1	1
	CL2	urn:id.gov.au:tdif:acr:ip1:cl2	2
	CL3	urn:id.gov.au:tdif:acr:ip1:cl3	3
IP1 PLUS	CL1	urn:id.gov.au:tdif:acr:ip1p:cl1	4
	CL2	urn:id.gov.au:tdif:acr:ip1p:cl2	5
	CL3	urn:id.gov.au:tdif:acr:ip1p:cl3	6
IP2	CL2	urn:id.gov.au:tdif:acr:ip2:cl2	7
	CL3	urn:id.gov.au:tdif:acr:ip2:cl3	8
IP2 PLUS	CL2	urn:id.gov.au:tdif:acr:ip2p:cl2	9
	CL3	urn:id.gov.au:tdif:acr:ip2p:cl3	10
IP3	CL2	urn:id.gov.au:tdif:acr:ip3:cl2	11
	CL3	urn:id.gov.au:tdif:acr:ip3:cl3	12
IP4	CL3	urn:id.gov.au:tdif:acr:ip4:cl3	13

4.2.2 OIDC to OIDC brokering

TDIF Req: FED-04-02-02; **Updated:** Mar-20; **Applicability:** X
When the *Applicant* is accepting *Authentication Requests* from a *Relying Party* using *OIDC* and translating those requests to an *Identity Service Provider* using *OIDC*, the *Applicant* ***MUST*** interact with the *Identity Service Provider* as per the *TDIF: 06B - OpenID Connect 1.0 Profile* [TDIF.OIDC], and the requirements set out below.

4.2.2.1 Mapping claims and scopes

TDIF Req: FED-04-02-03; **Updated:** Jun-21; **Applicability:** X
Scopes and claims that are received from the *Relying Party* ***MUST*** be included by the *Applicant* in the *Authentication Request* to the *Identity Service Provider* in accordance with the following processing rules

a. All *Attributes* included in the *Relying Party*'s *Authentication Request* which are found in section 3 of the *TDIF: 06D – Attribute Profile* ***MUST*** be included in the *Authentication Request* sent to the *Identity Service Provider* in either scopes or claims.

b. Scopes that are defined in the *Authentication Request* ***MAY*** be expanded into the underlying claims described in section 4.1 of the *TDIF: 06D – Attribute Profile*.

c. If the `sub` (subject) claim is specified then it ***MUST*** be processed as per the requirements in section 4.2.2.2.

TDIF Req: FED-04-02-04; **Updated:** Mar-20; **Applicability:** X
Scopes and claims not in the *TDIF: 06D – Attribute Profile* ***MUST*** be ignored by the *Applicant*.

TDIF Req: FED-04-02-04a; **Updated:** Mar-20; **Applicability:** X
Where scopes or claims are ignored, the *Applicant* ***MUST*** ***NOT*** raise an error.

4.2.2.2 Handling of sub claim

TDIF Req: FED-04-02-05; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MUST*** resolve a *Pairwise Identifier* included in the `sub` (subject) claim in the *Authentication Request* from a *Relying Party* to an existing *Pairwise Identifier* for the *User* at the required *Identity Service Provider*.

TDIF Req: FED-04-02-06; **Updated:** Mar-20; **Applicability:** X
If no *Pairwise Identifier* for the *User* at the *Identity Service Provider* can be resolved then the *Applicant* ***MAY*** return an error.

TDIF Req: FED-04-02-07; **Updated:** Mar-20; **Applicability:** I, X
The *Applicant* ***MAY*** support the `sub` (subject) claim.

4.2.2.3 Mapping Assurance Levels

TDIF Req: FED-04-02-08; **Updated:** Mar-20; **Applicability:** X
Where the `acr_values` or `acr` claim received from the *Relying Party* is a single value the *Applicant* ***MUST*** pass the set of *ACR* values that meet or exceed the value

of the requested *ACR* value to the *Identity Service Provider* in the generated *Authentication Request* according to the ranking in **Table 4**.

TDIF Req: FED-04-02-09; **Updated:** Mar-20; **Applicability:** X
Where the `acr` claim is marked as essential within the *Authentication Request* from the *Relying Party* it *MUST* be marked as essential when the *Applicant* sends the request to an *Identity Service Provider*.

TDIF Req: FED-04-02-10; **Updated:** Jun-21; **Applicability:** X
The *Applicant MUST* evaluate the *ACR* returned from the *Identity Service Provider* and if the *ACR* meets or exceeds the originally requested value(s), return one of the originally requested values.

4.2.2.4 Other OIDC request parameters

The following sections specify processing rules for *OIDC* parameters that a *Relying Party* may include in an *OIDC Authentication Request* to an *Identity Exchange*.

4.2.2.4.1 Prompt parameter

TDIF Req: FED-04-02-11; **Updated:** Mar-20; **Applicability:** X
The *Applicant MUST* implement the processing rules for *OIDC* prompt parameters described in Table 5.

Table 5: Processing rules for *OIDC* prompt parameters

Value received in OIDC request from Relying Party	Value sent in OIDC request to Identity Service Provider
None	None
Consent	Ignored. The *Identity Exchange* must implement *Consent* for the release of *Attributes* in accordance with the *Attribute Sharing Policy* defined within the *TDIF: 06D – Attribute Profile*
Login	Login

4.2.2.4.2 id_token_hint parameter

TDIF Req: FED-04-02-12 **Updated:** Mar-20; **Applicability:** X
If the `id_token_hint` mechanism defined in [TDIF.OIDC] is supported the following processing rules ***MUST*** apply:

a. Where the *Identity Exchange* receives an `id_token_hint` within an *Authentication Request* from a *Relying Party* the *Identity Exchange* is required to validate the *Identity Token* and extract the subject. The *Identity Exchange* must resolve this to a subject identifier at the Identity Service Provider as per section 4.2.2.2.

b. The *Identity Exchange* must include the resolved subject identifier in the *Authentication Request* to the *Identity Service Provider* using the `sub` (subject) Claim as per section 5.5 of the [OpenID.Core] with `essential=true`.

TDIF Req: FED-04-02-13; **Archived:** Jun-21
This requirement has been archived in version 1.1.

TDIF Req: FED-04-02-14; **Archived:** Jun-21
This requirement has been archived in version 1.1.

4.2.3 OIDC to SAML brokering

TDIF Req: FED-04-02-15; **Updated:** Mar-20; **Applicability:** X
When the *Applicant* is accepting *Authentication Requests* from a *Relying Party* using *OIDC* and translating those *Authentication Requests* to an *Identity Service Provider* using *SAML*, the *Identity Exchange* ***MUST*** interact with the *Identity Service Provider* as per the *TDIF: 06C – SAML 2.0 Profile* [TDIF.SAML] with the following processing rules.

4.2.3.1 Mapping Claims to Scopes

TDIF Req: FED-04-02-16; **Updated:** Mar-20; **Applicability:** X
Scopes and claims that are received from the *Relying Party* ***MUST*** be included by the *Applicant* in the *Authentication Request* to the *Identity Service Provider* in accordance with the following processing rules:

a. All *Attributes* included in the *Relying Party's Authentication Request* which are found in section 3 of the *TDIF: 06D – Attribute Profile* ***MUST*** be included in the *Authentication Request* sent to the *Identity Service Provider* in either scopes or claims.

b. Scopes that are defined in the *Authentication Request* ***MAY*** be expanded into the underlying claims described in section 4.1 of the *TDIF: 06D – Attribute Profile* and then mapped according to section 4.3.1 of the *TDIF: 06D – Attribute Profile*.

c. If the sub (subject) claim is specified then it ***MUST*** be processed as per section 4.2.2.2. Once it is resolved to a sub claim, then it should include the resolved subject identifier in the *Authentication Request* to the *Identity Service Provider* by including it in a `<saml:Subject>` element in the *SAML* `<AuthnRequest>` message.

d. Scopes and claims not in the *TDIF: 06D – Attribute Profile* ***MUST*** be ignored. Where scopes or claims are ignored, the *Identity Exchange* ***MUST*** ***NOT*** raise an error.

4.2.3.2 Mapping Assurance Levels

TDIF Req: FED-04-02-17; **Updated:** Mar-20; **Applicability:** X
Where the `acr_values` or `acr claim` received from the *Relying Party* is a single value the *Applicant* ***MUST*** pass 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* according to the ranking described in **Table 4**.

TDIF Req: FED-04-02-18; **Updated:** Mar-20; **Applicability:** X
Where the `acr` claim is marked as essential within the request from the *Relying Party* the `<samlp:RequestedAuthnContext>` `comparison` *Attribute* ***MUST*** be set to `minimum` when sent to the *Identity Service Provider*.

TDIF Req: FED-04-02-19; **Updated:** Jun-21; **Applicability:** X
The *Applicant* ***MUST*** evaluate the `<saml:AuthnContextClassRef>` returned from the *Identity Service Provider* and if the `<saml:AuthnContextClassRef>` meets or exceeds the originally requested *ACR* value(s), return one of the originally requested values.

4.2.3.3 Other OIDC Request Parameters

The following sections provide information on the transformation and passing of specific *Attributes* from the *OIDC Authentication Request* from a *Relying Party* to an *Identity Service Provider* using the *SAML Federation Protocol*.

4.2.3.3.1 Prompt parameter

TDIF Req: FED-04-02-20; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MUST*** implement the processing rules for *OIDC* prompt parameters as specified in **Table 6**.

Table 6: Processing rules for *OIDC* prompt parameters

Value received in OIDC request from Relying Party	Value sent in OIDC request to Identity Service Provider
`none`	`isPassive` attribute is set to true on the `<AuthnRequest>` message
`consent`	Ignored. The Identity Exchange ***MUST*** implement consent for the release of attributes in accordance with the Attribute Sharing Policy defined within *TDIF: 06D - Attribute Profile*
`login`	`ForceAuthn` attribute is set to true on the `<AuthnRequest>` message
`select_account`	Ignored.

4.2.3.3.2 id_token_hint Parameter

TDIF Req: FED-04-02-21; **Updated:** Mar-20; **Applicability:** X
A *Relying Party* ***MAY*** include an *ID Token* previously issued by an *Identity Exchange* in the *Authentication Request* to identify a specific *User* that requires *Authentication*.

TDIF Req: FED-04-02-22; **Updated:** Mar-20; **Applicability:** X
This specification does not require support for this mechanism by an *Identity Exchange*, but where it is supported the following processing rules ***MUST*** apply:

a. Where the *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. The *Identity Exchange* must resolve this to an *IP Link* at the *Identity Service Provider* as per 4.2.2.2.

b. The Identity Exchange should include the resolved subject identifier in the authentication request to the Identity Service Provider by including it in a `<saml:Subject>` element in the SAML 2.0 `<AuthnRequest>` message.

4.2.3.3.3 max_age Parameter

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 Connect Core specification [OpenID.Core].

TDIF Req: FED-04-02-23; **Updated:** Mar-20; **Applicability:** X
In order to support this functionality the *Identity Exchange* MUST implement the following processing:

a. On receiving the authentication response, an *Identity Exchange* must calculate the elapsed time since the *User* was *Authenticated* using the value of the AuthInstant attribute in the *SAML* response from the *Identity Service Provider*.

b. If the elapsed time is greater than the max_age value requested by the *Relying Party* then the *Identity Exchange* must generate a fresh *Authentication Request* with the ForceAuthn *Attribute* is set to true on the <AuthnRequest> message.

4.2.3.3.4 Other OIDC parameters

TDIF Req: FED-04-02-24; **Updated:** Mar-20; **Applicability:** X
The *Applicant* MUST implement the processing rules for *OIDC* parameters as specified in Table 7.

Table 7: Other parameters

Value received in OIDC request from Relying Party	Value sent in OIDC request to Identity Service Provider
`display`	No SAML 2.0 equivalent. The Identity Service Provider is responsible for detecting the capabilities of the user agent and presenting the appropriate display.
`login_hint`	Ignored.

4.2.4 SAML to SAML brokering

TDIF Req: FED-04-02-25; **Updated:** Mar-20; **Applicability:** X
When an *Identity Exchange* is accepting *Authentication Requests* from a *Relying Party* using *SAML* and translating those requests to an *Identity Service Provider* using *SAML*, the *Identity Exchange* ***MUST*** interact with the *Identity Service Provider* as per the *TDIF: 06C – SAML 2.0 Profile*.

4.2.4.1 Mapping Attributes

TDIF Req: FED-04-02-26; **Updated:** Mar-20; **Applicability:** X
Where the *Attributes* required are predefined within the *Relying Parties* metadata, the set of required *Attributes* ***MUST*** be included in the *Authentication Request* to the *Identity Service Provider* with the following processing rules:

a. Where the requested *Attributes* contained within the *Relying* Party's metadata are the same as the *Identity Exchanges* requested *Attributes* in its metadata exchanged with the *Identity Service Provider*; the *Identity Exchange* creates a standard *Authentication Request*.

b. Where the requested attributes are not available in the requested *Attributes* as part of the metadata shared with the *Identity Service Provider* by the *Identity Exchange*; the *Identity Exchange* is required to create an *Authentication Request* to the *Identity Service Provider* using extensions to request the *Attributes* required by the *Relying Party*.

TDIF Req: FED-04-02-27; **Updated:** Mar-20; **Applicability:** X
Where the *Attributes* requested by a *Relying Party* are requested via extensions the *Identity Exchange* ***MUST*** copy those *Attributes* into the *Authentication Request* to the *Identity Service Provider* as extensions.

4.2.4.2 Subjects within Requests

TDIF Req: FED-04-02-28; **Updated:** Mar-20; **Applicability:** X
The *Relying Party* ***MAY*** include a *SAML* Subject in the *Authentication Request*.

TDIF Req: FED-04-02-28a; **Updated:** Mar-20; **Applicability:** X
As the subject identifier is the *Pairwise Identifier* for the *User* at the *Relying Party*, the *Identity Exchange* ***MUST*** resolve this *Pairwise Identifier* in any *Authentication Request* to an existing *Pairwise Identifier* for the *User* at the required *Identity Service Provider*. If no *Pairwise Identifier* for the *User* at the *Identity Service Provider* can be resolved then the *Identity Exchange* should return an error.

TDIF Req: FED-04-02-28b; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MAY*** include the resolved *Pairwise Identifier* in the *Authentication Request* to the *Identity Service Provider*.

4.2.4.3 Mapping Assurance Levels

TDIF Req: FED-04-02-29; **Updated:** Mar-20; **Applicability:** X
Where the *Relying Party* includes a `<RequestedAuthnContext>` in the *Authentication Request*, the *Applicant* ***MUST*** send the set of `<AuthnContextClassRef>` to the *Identity Service Provider* that meet or exceed the originally requested `<RequestedAuthnContext>` according to the rankings described in **Table 4**.

TDIF Req: FED-04-02-30; **Updated:** Mar-20; **Applicability:** X
The `Comparison` attribute for the <RequestedAuthnContext> ***MUST*** be set to `exact` or `minimum`.

4.2.4.4 Other SAML Request Parameters

4.2.4.4.1 ForceAuthn Attribute

TDIF Req: FED-04-02-31; **Updated:** Mar-20; **Applicability:** X
When the ForceAuthn *Attribute* is set to true within the *Authentication Request* from the *Relying Party* the *Applicant* ***MUST*** pass this *Attribute* through in the *Authentication Request* sent by the *Applicant* to the *Identity Service Provider*.

4.2.4.4.2 isPassive Attribute

TDIF Req: FED-04-02-32; **Updated:** Mar-20; **Applicability:** X
When the isPassive *Attribute* is set to true within the *Authentication Request* from the *Relying Party* the *Applicant* ***MUST*** pass this *Attribute* through in the *Authentication Request* sent by the *Applicant* to the *Identity Service Provider*.

4.2.5 SAML to OIDC brokering

TDIF Req: FED-04-02-33; **Updated:** Mar-20; **Applicability:** X
When the *Identity Exchange* is accepting *Authentication Requests* from a *Relying Party* using the *SAML Federation Protocol* and translating those requests to an *Identity Service Provider* using the *OIDC Federation Protocol*, the *Applicant* ***MUST*** interact with the *Identity Service Provider* as per the [TDIF.OIDC].

4.2.5.1 Mapping Attributes to Claims or Scopes

TDIF Req: FED-04-02-34; **Updated:** Mar-20; **Applicability:** X
The *Attributes* requested within the *Authentication Request* either through extensions or via the *Relying Party's* metadata ***MUST*** be processed by the *Applicant* in accordance with the following rules:

a. All *Attributes* included in the *Relying Party's Authentication Request* which are found in section 3 of the *TDIF: 06D – Attribute Profile* must be included in the *Authentication Request* sent to the *Identity Service Provider* in either scopes or claims. The *Applicant* ***MUST*** use the mappings between *SAML* and *OIDC* described in section 4.3.1 of the *TDIF: 06D – Attribute Profile.*

b. Where the *Attributes* can be mapped fully into an available scope an *Identity Exchange* ***MAY*** request those scopes from an *Identity Service Provider*.

c. Where the *Attributes* do not map fully into a scope the *Identity Exchange* ***MUST*** request those *Attributes* as claims from the *Identity Service Provider*.

4.2.5.2 Mapping Assurance Levels

TDIF Req: FED-04-02-35; **Updated:** Mar-20; **Applicability:** X
Where the *Relying Party* includes a `<RequestedAuthnContext>` in the *Authentication Request*, the *Applicant* ***MUST*** send the set of `acr` values to the *Identity Service Provider* that meet or exceed the originally requested `<RequestedAuthnContext>` according to the rankings described in Table 4.

TDIF Req: FED-04-02-36; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MAY*** use the `acr` claim or the `acr_values` parameter.

TDIF Req: FED-04-02-37; **Updated:** Mar-20; **Applicability:** X
The `Comparison` attribute for the `<RequestedAuthnContext>` ***MUST*** be set to `exact` or `minimum`.

4.2.5.3 Other SAML Request Parameters

4.2.5.3.1 ForceAuthn

TDIF Req: FED-04-02-38; **Updated:** Mar-20; **Applicability:** X
Where the `ForceAuthn` attribute is included in the *Authentication Request* from the *Relying Party*, the *Applicant* ***MUST*** set the `prompt` parameter to `login` in the *OIDC Authentication Request* to the *Identity Service Provider*.

4.2.5.3.2 isPassive

TDIF Req: FED-04-02-39; **Updated:** Mar-20; **Applicability:** X
Where the `isPassive` *Attribute* is included in the *Authentication Request* from the *Relying Party*, the *Identity Exchange* ***MUST*** set the `prompt` parameter to `none` in the *OIDC Authentication Request* to the *Identity Service Provider*.

4.2.5.3.3 Subject

Where a `Subject` is included in the *Authentication Request* from the *Relying Party* the *Identity Exchange* is required to validate the token and extract the subject.

TDIF Req: FED-04-02-40; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MUST*** resolve the value of the subject to a subject identifier at the *Identity Service Provider* as per 4.2.2.2.

TDIF Req: FED-04-02-40a; **Updated:** Mar-20; **Applicability:** X
The *Applicant* ***MAY*** include the resolved subject identifier in the *Authentication Request* to the *Identity Service Provider* using the `sub` (subject) claim.

Attribute Requirements

The *Attributes* passed through the *Australian Government Digital Identity System* are defined in the *TDIF: 06D - Attribute Profile.* This section of the *TDIF: 06 - Federation Onboarding Requirements* references that document as the source of the information required to be shared in the *Australian Government Digital Identity System*.

5.1 Attribute Requirements

TDIF Req: FED-05-01-01**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* support the disclosure of all *Attributes* described in section 3.1 of the *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the *TDIF 06 – Federation Onboarding Requirements***.**

TDIF Req: FED-05-01-02**; Updated:** Jun-21**; Applicability:** I
The *Applicant* *MUST* support the disclosure of all *Attributes* listed as mandatory in section 3.1 of the *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the *TDIF 06 – Federation Onboarding Requirements*.

TDIF Req: FED-05-01-03**; Updated:** Jun-21**; Applicability:** I
The *Applicant* *MAY* support the disclosure of an *Attribute* listed as optional in section 3.1 of *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the *TDIF 06 – Federation Onboarding Requirements*.

TDIF Req: FED-05-01-04**; Updated:** Jun-21**; Applicability:** I
The *Applicant* *MUST* support the disclosure of all *Attributes* listed as mandatory in section 3.2 of the *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the *TDIF 06 – Federation Onboarding Requirements*.

TDIF Req: FED-05-01-05**; Updated:** Mar-20**; Applicability:** X
The *Applicant* *MUST* be able to include any of the *Attributes* described in section 3.2 of *TDIF: 06D - Attribute Profile* in an *Authentication Request* to an *Identity Service Provider*.

TDIF Req: FED-05-01-06**; Updated:** Jun-21**; Applicability:** X
The *Applicant MUST* support the disclosure of all *Attributes* described in section 3.3 of *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the *TDIF 06 – Federation Onboarding Requirements.*

TDIF Req: FED-05-01-07**; Updated:** Jun-21**; Applicability:** X
The *Applicant MUST* support the disclosure of all *Attributes* described in section 3.5 of *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the TDIF 06 – Federation Onboarding Requirements.

5.2 Computed attributes

TDIF Req: FED-05-02-01**; Updated:** Mar-20**; Applicability:** A, I, X
The *Applicant MAY* define support for additional computed Attributes derived from the *Attributes* in an *Attribute Set. Finance* will add any computed attributes to the *TDIF: 06D - Attribute Profile*.

TDIF Req: FED-05-02-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant MUST* support the disclosure of additional computed attributes described in section 3.4 of the *TDIF: 06D - Attribute Profile* using one of the *federation protocols* specified in section 2.1.1 of the TDIF 06 – Federation Onboarding Requirements.

TDIF Req: FED-05-02-03**; Updated:** Mar-20**; Applicability:** X
The *Applicant MAY* source a computed attribute from an *Attribute Service Provider* or *Identity Service Provider*.

5.3 Attribute Service Provider attributes

TDIF Req: FED-05-03-01**; Updated:** Jun-21**; Applicability:** X
The *Applicant MAY* support the disclosure of *Attributes* an *Attribute Service Provider* is accredited to provide. These *Attributes* are defined in section 5 of the *TDIF: 06D - Attribute Profile*.

TDIF Req: FED-05-03-02**; Updated:** Jun-21**; Applicability:** A
The *Applicant MUST* ensure that it only disclosure, or provides to an *Identity Exchange* to be shared, *Attributes* that are relevant to the *Relying Party* requesting the *Attributes*.

5.4 Attribute sharing policies

TDIF Req: FED-05-04-01**; Updated:** Jun-21**; Applicability:** X
The *Applicant* ***MUST*** only disclose *Attributes* with *Relying Parties* in accordance with the *Attribute Sharing Policy* specified for the *Attribute Set* which an *Attribute* is part of as described in section 2.2 of the *TDIF: 06D - Attribute Profile*.

5.5 Attribute data representation

TDIF Req: FED-05-05-01**; Updated:** Jun-21**; Applicability:** A, I, X
When disclosing *Attributes* to other *Participants* in the *Identity Federation*, the *Applicant* ***MUST*** use the attribute data representation for *Attributes* specified in section 6 of the *TDIF: 06D - Attribute Profile*.