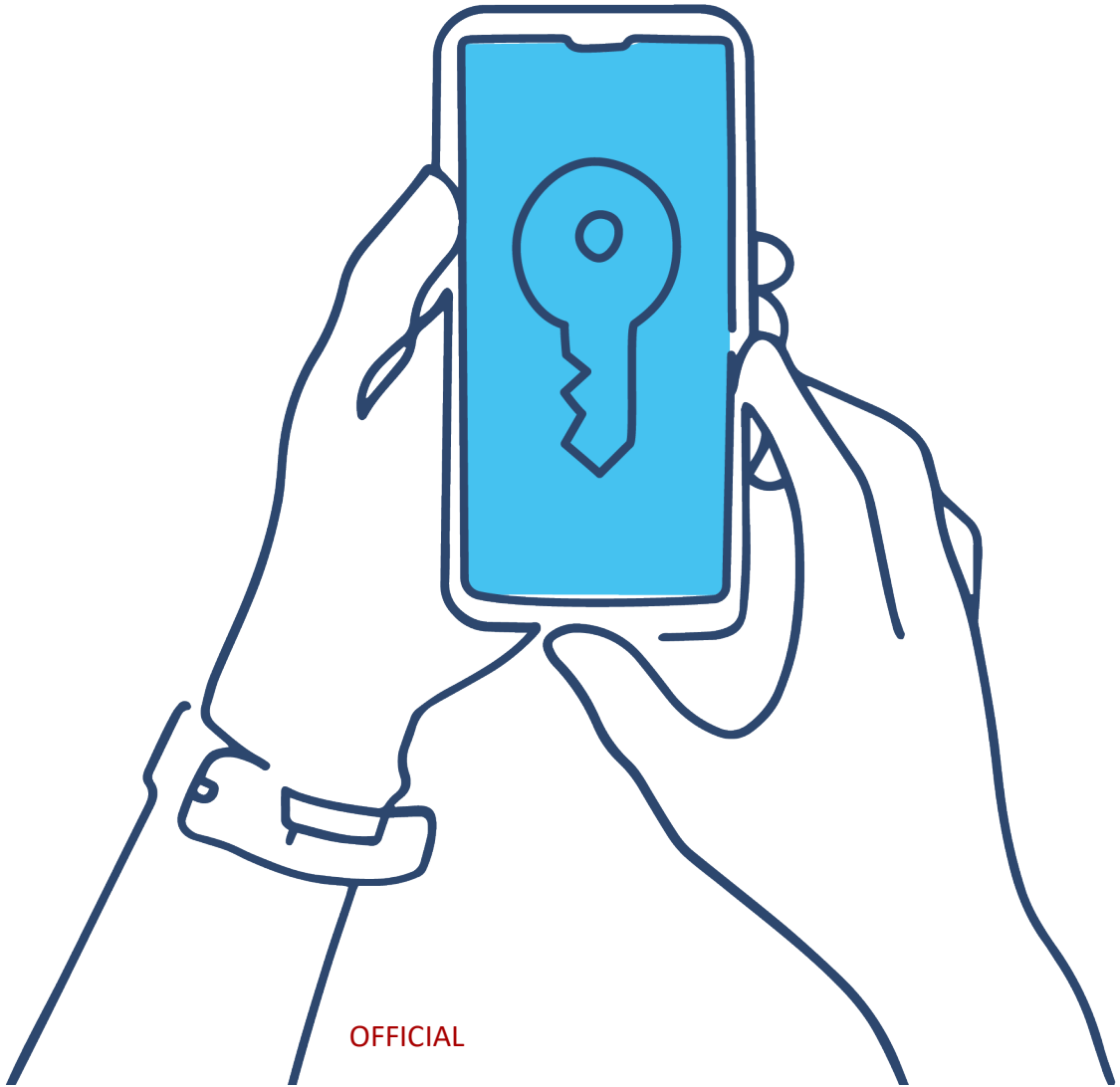
Australian Government | Digital Identity

03 Accreditation Process

Trusted Digital Identity Framework

Release 4 October 2021, version 1.3

PUBLISHED VERSION



Digital Transformation Agency (DTA)

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 Provider*, 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

The *DTA* 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 digitalidentity@dta.gov.au.

Document management

The *DTA* has endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	Aug 2019	SJP	Initial version
0.2	Sep 2019	SJP	Updated to incorporate feedback provided by stakeholders during the first round of collaboration on TDIF Release 4
0.3	Dec 2019	SJP	Updated to incorporate feedback provided by stakeholders during the second round of collaboration on TDIF Release 4
0.4	Mar 2020	SJP	Updated to incorporate feedback provided during the public consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	Mar 2021	JK, SJP	Consultation version
1.2	June 2021	JK, SJP	CRID0009, CRID0012 – Requirements changes, additional guidance text added, new requirements added (See Change Log for full list of requirements changes). Templates removed (now available on TDIF Framework Website).
1.3	Oct 2021	SJP	CRID0027 – Updated ACCRED-03-01-01, to require Applicants to submit a '*Statement of Claims*' as part of their TDIF application.

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

Contents

List of Figures

Introduction

This document sets out the *TDIF Accreditation Process* which involves a combination of documentation requirements, third party evaluations and operational testing that *Applicants* must complete to the satisfaction of the *DTA* to achieve *TDIF* accreditation. The intent of accreditation is to determine whether the *Applicant's Identity System* meets the requirements set out in the *TDIF*.

The intended audience for this document includes:

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

TDIF Accreditation Process

2.1 Overview

The *TDIF Accreditation Process* is a formal process through which *Applicants* demonstrate their ability to meet applicable accreditation requirements to the satisfaction of the *DTA*. **Figure 1** provides an overview of the *TDIF Accreditation Process* and **Figure 2** (page 12) provides a detailed description of the accreditation activities.

Figure 1**:** TDIF Accreditation Process.

The TDIF Accreditation Process includes two phases:

- **Initial accreditation** (this document) – sets out the processes and activities to be met by the *Applicant* to achieve TDIF accreditation. This phase covers the 'Preliminary Preparations', 'Request Accreditation', 'Meet TDIF Requirements' and 'Complete Accreditation' processes.
- **Annual accreditation obligations** - sets out the processes and activities to be met by the *Accredited Providers* to maintain its *TDIF accreditation*. This phase covers the fifth accreditation process, 'Maintain Accreditation', which is the focus of the document titled *TDIF 07 - Annual Assessment*.

The *TDIF Accreditation Process* is managed by a series of decision gates. These decision gates are used by the *DTA* to evaluate the *Applicant's* progress towards *TDIF* accreditation and their ability to meet ongoing accreditation obligations. In **Figure 2's** detailed breakdown, arrows show the relationships between accreditation activities. All activities can be iterated.

2.2 Who can apply for TDIF accreditation?

TDIF accreditation can be sought by organisations that:

- Participate in the open market and choose to undergo the *TDIF Accreditation Process* to increase the perceived assurance of their identity. This includes organisations that operate their own *Identity System* (single entity) and organisations that provide components of an *Identity System* that work together (multi-entity).
- Are members of an existing community of interest and choose to undergo the *TDIF Accreditation Process* to increase the perceived assurance of their *Identity System* to other members of the community of interest.
- Are required to meet the *TDIF 06 Federation Onboarding Requirements* prior to joining the *Australian Government's identity federation*.

2.3 TDIF accreditation pathways

The *TDIF* supports two accreditation pathways:

1. Organisations that do NOT connect to the *Australian Government's identity federation*
2. Organisations that do want to connect to the *Australian Government's identity federation*.

The number of *TDIF* requirements that apply is dependent on the pathway chosen and the accreditation role being sought (e.g. *Identity Service Provider*). The table below lists the *TDIF* documents that apply to the accreditation pathways.

Not connected to the *Australian Government identity federation*	Connected to the *Australian Government identity federation*
Initial accreditation	**Initial accreditation**
TDIF 03 - Accreditation Process	*TDIF 03 - Accreditation Process*
TDIF 04 - Functional Requirements	*TDIF 04 - Functional Requirements*
TDIF 05 - Role Requirements	*TDIF 05 - Role Requirements*
	TDIF 06 - Federation Onboarding Requirements
	TDIF 06B - OpenID 1.0 Connect Profile
	TDIF 06C - SAML 2.0 Profile (if supported)
Annual accreditation obligations	**Annual accreditation obligations**
TDIF 07 - Annual Assessment	*TDIF 07 - Annual Assessment*

2.4 Reuse of audit work for Functional Assessments

For initial accreditation, and in accordance with the *TDIF 04 - Functional Requirements,* the *Applicant's Identity System* is required to undergo *Functional Assessments* by independent *Assessors* with the relevant skills, experience, and qualifications to perform the *Functional Assessments*. These *Functional Assessments* cover protective security, privacy, accessibility, and usability.

Applicants may have recently undergone assessments on their *Identity System* which cover similar requirements to those listed in *TDIF*. The *Applicant* may, as per its *TDIF Application Letter*, submit evidence of audit work conducted in the previous 12 months and request the *DTA* consider it as a substitute for a *Functional Assessment*.

At its discretion, the *DTA* may accept prior audit work conducted on the *Applicant's Identity System* as a substitute to a *Functional Assessment* required by the *TDIF*. In such instances the *DTA* will advise the *Applicant* in writing the adequacy of prior assessments relative to the degree to which they cover *TDIF* requirements.

Where the *DTA* determines a prior assessment:

- Fully addresses a *Functional Assessment,* then no further action will be required by the *Applicant* for that *Functional Assessment*.
- Partially addresses a *Functional Assessment,* then the *Applicant* will need to undergo a partial *Functional Assessment* for the requirements it does not meet.
- Does not address a *Functional Assessment,* then the *Applicant* will need to undergo the *Functional Assessment* as described in the *TDIF 04 - Functional Requirements*.

2.5 Using Assessors for TDIF Functional Assessments

The *DTA* does not maintain a list of *Assessors*. As part of good corporate governance, the *Applicant* should be able to research, identify and obtain appropriate *Assessors* with the relevant skills, experience, independence and qualifications to undertake *Functional Assessments*.

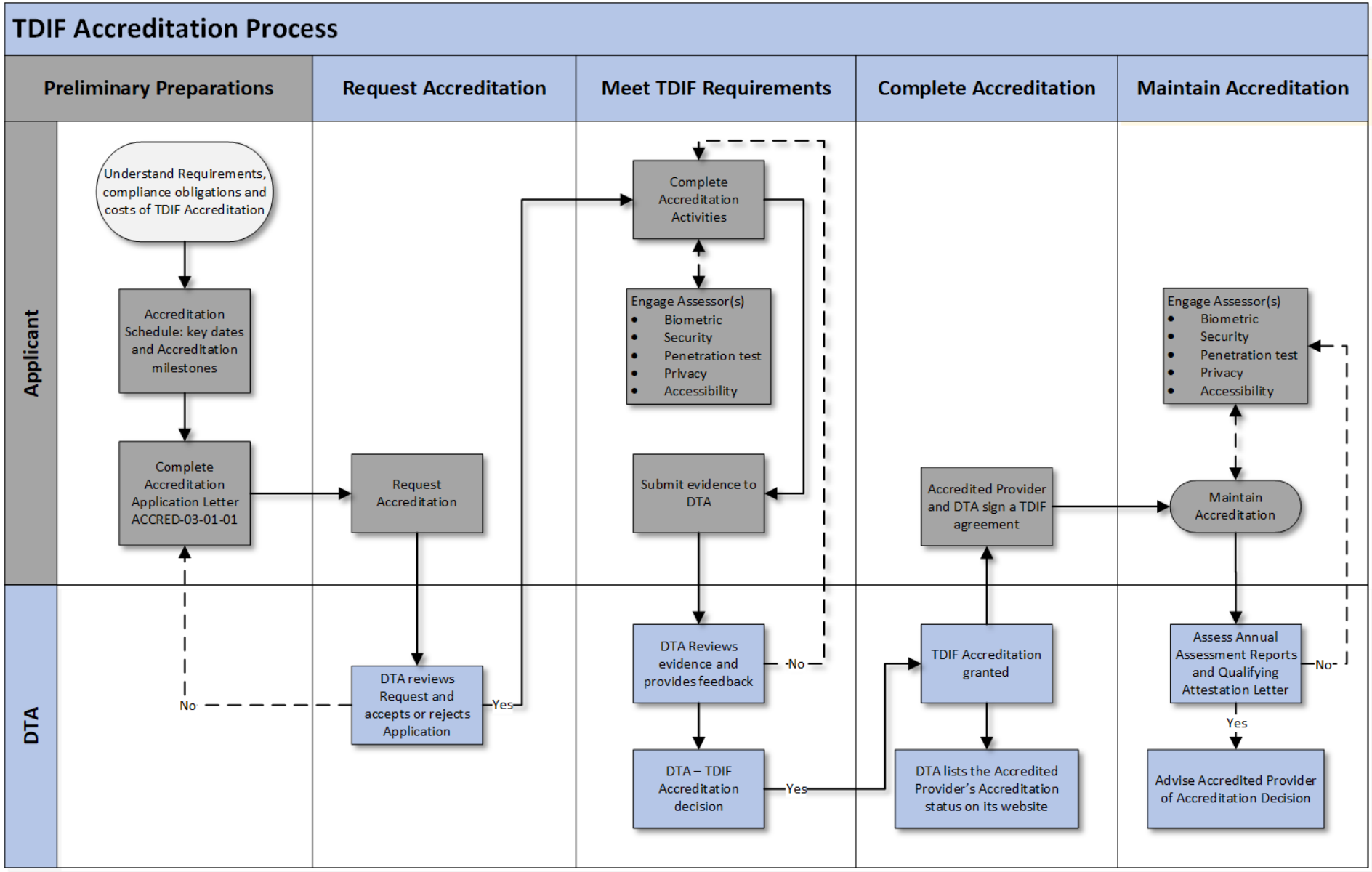
Depending on the complexity and timeliness of the evaluation to be performed, the potential cost to the *Applicant* could be more than expected. *Applicants* are encouraged to contact several *Assessors* to get a sense of the cost, duration and complexity of the work to be undertaken to meet a *Functional Assessment* prior to engaging an *Assessor*.

The *TDIF Accreditation Process* requires *Applicants* to engage the following *Assessors*:

- *Security Assessments* can be undertaken by a security advisor, *IRAP assessor* or other security professional that has relevant, reasonable and adequate experience, training and qualifications to undertake the assessment.
- *Penetration tests* must be undertaken by organisations or individuals with relevant experience in *penetration testing*. See the *Functional Assessments Guidance* sections of *TDIF 04A Functional Guidance* for further information about *penetration testing assessors*.
- *Privacy Impact Assessments* (PIA) and *Privacy Assessments* can be undertaken by the *Applicant* or an external assessor in accordance with the Office of the Australian Information Commissioner (OAIC) guidelines. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.
- *Accessibility Assessments involve* an *assessment* against the *Web Content Accessibility Guidelines* (WCAG). There is currently (at time of publication) no advice for approved lists of *Accessibility Assessors*. *Applicants* should present evidence of the *Assessor's* skills, experience, qualifications and independence when engaging an assessor for an *Accessibility assessment*.
- Organisations that seek TDIF accreditation for *Identity System*s that include the collection of biometrics[1] are required to undergo an *assessment*, which must be undertaken by a qualified third-party testing entity with experience in biometric testing and *ISO 30107*.

[1] In accordance with PRIV-03-08-02.

Figure 2: TDIF Accreditation Process (detailed description)



Accreditation Activities

3.1 Preliminary Preparations

The organisation should understand the requirements, likely timeframes, costs, and ongoing compliance obligations of *TDIF* accreditation before they commit to undergo the *TDIF Accreditation Process*. The *DTA* can work with the organisation during this stage to ensure they understand their obligations regarding accreditation and are preprepared if they choose to undergo the *TDIF Accreditation Process*.

An organisation should consider the following points before committing to undergo the *TDIF Accreditation Process*:

- Do you understand how to read *TDIF* requirements and applicability indicators[2]?
- Do you know what information is required to be submitted to the DTA as part of the *TDIF Application Letter*?
- You will need to provide the DTA with your responses to the *TDIF Statement of Claims*. Have you considered the responses you'll provide?
- Which accredited roles your identity system will perform:
    - For *Identity Service Providers* - what verification methods and *Identity Proofing Levels* does your *Identity System* support? Does your *Identity System* support *Identity Proofing Step Up*?
    - For *Credential Service Providers* – what *Credential Levels* and *credential* types does your *Identity System* support? Does your *Identity System* support *Credential Step Up*?
    - For Attribute Service Providers – what *Attribute Classes* does your *Identity System* support?
    - For Identity Exchanges – what kind of features does your exchange support? (e.g. *IdP Selection*, *User Dashboard*)

[2] Applicability indicators are set out in *TDIF 02 Overview*.

- Does your *Identity System* support web-responsive design, mobile applications, or both?
- Have you considered all applicable *TDIF* requirements for your *Identity System*?
    - How many *TDIF* requirements do you think will apply?[3]
    - Do you have everything in place or is work required to meet *TDIF* requirements?
    - Will you seek any exemptions? If so, what supporting evidence is needed?
- Do you have a dedicated team in the organisation to undertake TDIF accreditation?
- Have you organised *Assessors* to undertake the *Functional Assessments*?
- How long do you think it will take to achieve *TDIF* accreditation?
    - The DTA does not define maximum periods that activities or the *TDIF Accreditation Process* itself is likely to take, as this is largely driven by the organisation once their application for TDIF accreditation has been accepted by the DTA.
    - The *Applicant* should be able to achieve *TDIF* accreditation within 12 months following the DTA's acceptance of their *TDIF Application Letter* and *TDIF Statement of Claims*.

An organisation can apply to undergo the *TDIF Accreditation Process* at any stage in the development life cycle of their *Identity System*. However, the *DTA* will only grant accreditation to a fully operational *Identity System* which meets all applicable *TDIF* requirements. The *DTA* does not grant partial accreditations.

[3] The 'TDIF Accreditation Requirements' spreadsheet includes all requirements across the four accreditation roles and both pathways. See TDIF documents website for further information.

3.2 Request Accreditation

The organisation must submit an *TDIF Accreditation Application Letter* to the *DTA* to formally begin the *TDIF Accreditation Process* (hereafter referred to an *Applicant*). The details that must be included in this letter are set out in this section.

Requirements

TDIF Req: ACCRED-03-01-01; **Updated**: Oct-21; **Applicability**: A, C, I, X
The *Applicant* ***MUST*** formally request *TDIF* accreditation by submitting to the DTA a completed *TDIF Application Letter* and response to the *TDIF Statement of Claims*[4].

TDIF Req: ACCRED-03-01-01a; **Updated:** Jun-21**; Applicability:** A, C, I, X
All information provided to the *DTA* for the purpose of *TDIF* accreditation ***MUST*** be in English[5].

TDIF Req: ACCRED-03-01-01b; **Updated:** Jun-21**; Applicability:** A, C, I, X
The *Applicant* ***MUST*** have a registered and active ABN.

TDIF Req: ACCRED-03-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *TDIF Application Letter* ***MUST*** specify *Accredited Roles* being sought, or a combination of these.

TDIF Req: ACCRED-03-01-02a; **Updated**: Mar-20; **Applicability**: C, I
The *TDIF Application Letter* ***MUST*** specify the assurance levels supported by their identity service. For *Identity Service Providers* this means *Identity Proofing Levels*. For *Credential Service Providers* this means *Credential Levels*[6].

TDIF Req: ACCRED-03-01-02b; **Updated**: Jun-21; **Applicability**: C, I
The *TDIF Application Letter* ***MUST*** specify whether the *Identity System* supports web responsive design, mobile apps or a combination of these. This information will determine the scope of the *Accessibility Assessment*.

TDIF Req: ACCRED-03-01-02c; **Updated**: Jun-21; **Applicability**: A, C, I, X

4 See TDIF documents website for the *TDIF Application Letter* and *TDIF Statement of Claims* templates.

5 The DTA ***MAY*** request the original documents if they are in a language other than English.

6 See the *TDIF: 05 - Role Requirements* for further information on *Identity Proofing* and *Credential Levels*.

The *TDIF Application Letter* *MUST* specify whether the *Applicant* is seeking to connect to the *Australian Government's identity federation*[7].

TDIF Req: ACCRED-03-01-03; **Updated**: Jun-21; **Applicability**: A, C, I, X
The Application Letter *MUST* include a *Statement of Applicability* which describes the scope of the *Applicant's Identity System*.

TDIF Req: ACCRED-03-01-03a; **Updated**: Jun-21; **Applicability**: A, C, I, X
At a minimum, the *Statement of Applicability* *MUST*:

a) Be written for an operational *Identity System*, regardless of whether the *Applicant's Identity System* is operational or not.
b) summarise the fraud control, privacy, protective security and user experience features of the *Identity System*.
c) Provide a high-level summary of how the *Applicant* will meet the fraud control, privacy, protective security and user experience requirements set out in *TDIF 04 Functional Requirements*.
d) Include the version of the *Australian Government Information Security Manual* used as its basis (i.e. month and year).

The *Statement of Applicability* forms the basis of the *Applicant's Functional Assessments*.

TDIF Req: ACCRED-03-01-03b; **Updated**: Jun-21; **Applicability**: A, C, I, X
For *multi-entity Identity Systems*, the *Statement of Applicability* *MUST* also include all fraud control, privacy, protective security, and user experience controls, which directly contribute to meeting *TDIF* requirements.

TDIF Req: ACCRED-03-01-04; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *TDIF Application Letter* *MUST* include an accreditation schedule which at a minimum includes:

a. Estimated dates when *Functional Assessments* will be undertaken
b. Estimated dates when *Functional Assessment Reports* will be provided to the *DTA*
c. Estimated dates when the *Applicant's* evidence addressing *TDIF* requirements will be provided to the *DTA*.

[7] This indicates the Applicant will need to meet the *TDIF 06* series of documents.

TDIF Req: ACCRED-03-01-04a; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *TDIF Application Letter* MUST propose a commencement date and a date by which *TDIF* accreditation is anticipated[8].

TDIF Req: ACCRED-03-01-05; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *TDIF Application Letter* MUST include the names and contact details of people responsible within the *Applicant's* organisation(s)[9] to manage their *TDIF* accreditation[10].

TDIF Req: ACCRED-03-01-06; **Updated**: Jun-21; **Applicability**: A, C, I, X

The *TDIF Application Letter* MAY include any relevant *TDIF Exemption Requests* in accordance with the process set out in **Appendix A:** TDIF exemption process.

TDIF Req: ACCRED-03-01-06a; **Updated**: Jun-21; **Applicability**: A, C, I, X
Each *TDIF Exemption Request* MUST include all information as described in **Appendix A:** TDIF exemption process.

TDIF Req: ACCRED-03-01-07; **Updated**: Jun-21; **Applicability**: A, C, I, X
The *Applicant* MAY include a copy of prior audit work which it requests the *DTA* consider as a substitute for relevant *Functional Assessments*.

TDIF Req: ACCRED-03-01-07a; **Updated**: Jun-21; **Applicability**: A, C, I, X
Any request made to the *DTA* to consider prior audit work MUST include:

a. An indication of which *Functional Assessment* it is provided as a substitute for.
b. A rationale why it is being provided.
c. A summary of which *TDIF* requirements the *Applicant* believes will be addressed by the prior audit work.

Receipt of Letter

On receiving a *TDIF Application Letter, TDIF Statement of Claims,* and supporting information, the DTA will acknowledge the *Applicant's* request to undergo the *TDIF*

8 Based on *DTA* experience, the average time to complete the *TDIF Accreditation Process* ranges from 9 – 12 months.

9 For multi-entity accreditation requests it is likely that multiple teams across participating organisations will be required.

10 The *DTA* recommends a central person or area be responsible within each organisation supporting the *Applicant's TDIF* accreditation. This will greatly aide in coordination and management of accreditation activities.

Accreditation Process in writing. The *DTA* will subsequently review the *TDIF Application Letter, TDIF Statement of Claims,* and supporting information.

The *DTA* will either:

- Approve the *Applicant's* request to continue with *TDIF* accreditation activities where the *DTA* is satisfied with the information provided. In such instances the *DTA* will advise the *Applicant* of its decision; or
- Reject the *Applicant's* request to continue with *TDIF* accreditation if the *DTA* is not satisfied with the information provided. Where a request for *TDIF* accreditation has been rejected, the *DTA* will advise the *Applicant* of its decision, the reasons why and the actions to be taken by the *Applicant* for their *TDIF Application Letter* to be reconsidered by the *DTA*.

3.3 Meet TDIF Accreditation

The 'Meet TDIF Requirements' activity requires the *Applicant* to demonstrate how it and its *Identity System* meet all applicable *TDIF* requirements. The *DTA* uses a variety of methods to assess evidence submitted by *Applicants* to ensure they meet applicable requirements, including a review of:

- the *Application Letter* provided and accreditation schedule
- policies, plans and procedures
- risk management and organisational governance material
- architectural and network diagrams and system information
- training materials provided to staff
- test plans, test scripts and source code reviews
- independent assessors' reports (*Functional Assessments*)

Once the *Applicant's* request for accreditation has been accepted, they then complete their *TDIF* accreditation activities, engaging *Assessors* to complete *Functional Assessments*.

The *Applicant* will submit the evidence that they have met their requirements to the *DTA.* The *DTA* will review the evidence and mark off requirements as they have been met. For requirements that may require additional evidence or further

clarification before they can be accepted as compliant, the DTA will provide feedback to the *Applicant* on what is required to meet them.

Appendix B: Accreditation Evidence **Table 2** lists all requirements that require evidence to be submitted to the *DTA*.

The *DTA* has developed templates for some of the evidence required (e.g. the *TDIF Application Letter* and some *Functional Assessments*) to assist with meeting these requirements. These templates are supplied as guidance material only and may not suit the *Applicant's* needs. An *Applicant* may submit their own documentation that will meet the *TDIF* requirements.
Templates are available on the Digital Identity TDIF documents website.

Factors that impact on the time taken to complete an activity or achieve accreditation include:

- The *Applicant's* understanding of the *TDIF Accreditation Process* and *TDIF* requirements.
- The nature and maturity of the *Identity System* being accredited.
- The *Applicant's* business needs, threat environment and risk tolerance.
- The degree to which the *Applicant's Identity System* is straightforward, easy to use, secure and privacy preserving.
- The time taken by the *Applicant* to complete the required *Functional Assessments* from *Assessors* and address any non-compliance issues to the satisfaction of the *DTA*.

3.4 Complete Accreditation

Successful completion of the *TDIF Accreditation Process* will result in the *DTA* granting accreditation to the *Applicant.* Both parties will sign a *TDIF* agreement, and the *Applicant* will be listed as an *Accredited Provider* on the Digital Identity website[11]

11 See the TDIF documents website for further information on *Accredited Participants*.

Upon successfully completing the 'Meet TDIF Requirements' activity, the *Applicant* and its *Identity System* will be listed on the *DTA's* website as an *Accredited Provider* and the *DTA* will update the *TDIF Accreditation Register*.

Following accreditation, the *Accredited Provider* must, if required by the *DTA*, enter into an agreement with the *DTA* which sets out the rights, roles and obligations of both parties in relation to the *Accredited Provider's TDIF* accreditation.

The *Accredited Provider* is required to undergo an *Annual Assessment* by the anniversary of their initial accreditation date. Further information on the *Annual Assessment* is set out in the *TDIF: 07 - Annual Assessment.*

3.5 Maintain Accreditation

Once accredited, the *Accredited Provider* is required to demonstrate its ability to maintain *TDIF* accreditation. Each year the *Accredited Provider* is required to complete an *Annual Assessment* by the anniversary of its initial accreditation date and meet its annual accreditation obligations as outlined in *TDIF 07 Annual Assessments.*

The *Accredited Provider* may be directed by the *DTA* to undergo *TDIF Reaccreditation* following a cyber security or fraud incident, serious or repeated breaches related to privacy or data, or as a result of a changing threat or operating environment which materially impacts the *Identity System* risk profile. If *TDIF Reaccreditation* is required, the *DTA* will determine whether it replaces the requirement for the *Accredited Provider's Annual Assessment*.

Appendix A : TDIF exemption process

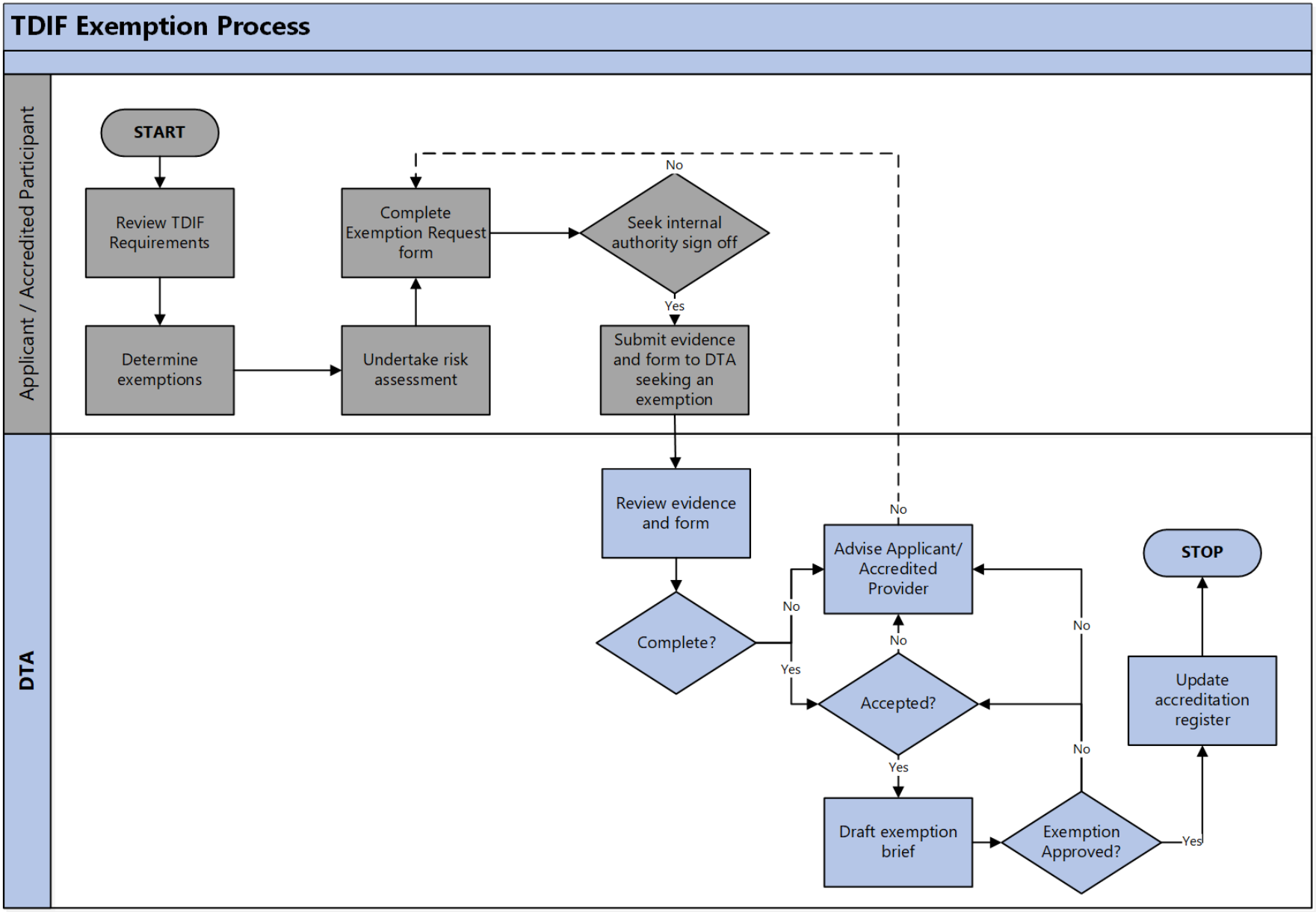
A.1 Purpose

This Appendix outlines the process to be used by an *Applicant* when seeking an exemption against a *TDIF* requirement. Prior to submitting to the *DTA*, an exemption request:

- Is to be signed off by the *Applicant's* relevant *Accountable Authority*.
- Is to include a completed and signed *TDIF Exemption Request* form in the form set out in section A.2.6.
- Is to be supported with relevant evidence.

Figure 2 provides an overview of the key steps in the process.

Figure 2: TDIF exemption process.



A.2 Exemption activities

A.2.1 Exemption determination

The *Applicant* is required to review all applicable *TDIF* requirements and determine the impacts of meeting them. Where compliance with a *TDIF* requirement would negatively impact their *Identity System*, the *Applicant* may determine relevant exemptions[12]. The *Applicant* is required to conduct a risk assessment on the proposed exemptions and collect relevant evidence which supports the exemption request. This information is to be included in a *TDIF Exemption Request* form (see below) that is to be submitted to the *Applicant's Accountable Authority*[13] for approval.

A.2.2 Exemption request form

The *Applicant's Accountable Authority* and the *DTA* can only make risk-based decisions if they are fully informed of the relevant facts. Without this information it cannot make an informed decision on whether to grant an exemption against a *TDIF* requirement.

Applicants seeking an exemption are required to:

- Complete the *TDIF Exemption Request* form in the form set out in section A.2.6.
- Document the justification for exemption against a *TDIF* requirement.
- Undertake a risk assessment.
- Document the alternative mitigation measures to be implemented, if any (including proposed date for remediation).
- Specify the exemption period being sought.
- Obtain endorsement from an appropriate *Accountable Authority* for the non-compliance.

12 The *DTA* will generally support an exemption request where the *Applicant* can demonstrate the request is required to support business needs or address likely, realistic and probable risks. The *DTA* will not support an exemption request where the *Applicant* simply chooses not to meet a *TDIF* requirement.

13 Typically, the *Accountable Authority* within the *Applicant's* organization is the business area responsible for managing the subject matter under question.

If supported, the *Applicant's Accountable Authority* is required to sign the *TDIF Exemption Request* form. This endorsement also confirms the risk assessment outcomes and any proposed mitigation action and associated date for completion of the proposed action(s).

Where an *Applicant* is seeking an exemption against multiple *TDIF* requirements for similar reasons, it may group these together in their report to simplify the reporting process.

A.2.3 Assessment validation

Following this internal signoff, the *Applicant* is required to submit its evidence and signed *TDIF Exemption Request* form to the *DTA* for review. The *DTA* will initially review the *TDIF Exemption Request* to ensure all required information has been provided. The *DTA* will then consider the request along with the evidence. The outcome of this review will be a determination of whether the evidence presented along with any proposed remediations are acceptable and supports the *Applicant* in meeting its *TDIF* accreditation obligations.

Unless otherwise agreed between the *Applicant* and the *DTA*, all evidence provided to the *DTA* will be treated as *OFFICIAL information*[14].

A.2.4 Accreditation conclusion

The *DTA* will form an opinion on the *Applicant's TDIF Exemption Request* and supporting evidence. Upon receipt of the brief and supporting documentation the *DTA* will decide whether to accept or reject the *Applicant's TDIF Exemption Request*. The DTA may request further information from the *Applicant* to assist in its decision making. The outcome of the DTA decision will be provided to the *Applicant*.

If the request is accepted, the *Applicant* will be granted an exemption against the relevant *TDIF* requirement. If the request is rejected, the *Applicant* will not be granted an exemption and will be required to meet the *TDIF* requirement.

14 NB. Some *TDIF* accreditation activities may have a higher security classification and may not be shared with external parties; however, they must be made available to appropriate *DTA* personnel with a need to know.

A.2.5 Update accreditation register

All *TDIF Exemption Requests* and the *DTA's* decisions will be recorded in the *TDIF Accreditation Register*.

The *DTA* may, at its discretion and in consultation with the *Applicant*, advise other *Providers* of its decision to grant or reject a *TDIF Exemption Request*.

As the justification for exemptions may change, and the risk environment will continue to evolve over time, it is important that *Applicants* update their approval for exemptions as part of their *Annual Assessments*. This allows the *DTA* to review the exemption and either continue to approve or, if necessary, reject it if the justification or residual risk is no longer acceptable.

A.2.6 TDIF Exemption Request form template

Refer to the *TDIF 04A Functional Guidance* document or the *Applicant's* own risk management framework for a description of likelihood and consequence ratings.

The TDIF Exemption Request form is available from the TDIF documents website.

Appendix B : Accreditation Evidence

Table 1: Accreditation Evidence

Document	TDIF Req	Applicability	Evidence Required	Template Available?
TDIF 03 Accreditation Process	ACCRED-03-01-01	A, C, I, X	TDIF Application Letter and Statement of Claims	Yes
TDIF 03 Accreditation Process	ACCRED-03-01-06a	A, C, I, X	Exemption Request Form and Evidence	Yes
TDIF 04 Functional Requirements	PRIV-03-02-03	A, C, I, X	Privacy Policy	No
TDIF 04 Functional Requirements	PRIV-03-02-06	A, C, I, X	Privacy Management Place	No
TDIF 04 Functional Requirements	PRIV-03-02-08	A, C, I, X	Privacy awareness training material	No
TDIF 04 Functional Requirements	PRIV-03-03-01	A, C, I, X	Privacy Impact Assessment register	No
TDIF 04 Functional Requirements	PRIV-03-04-02;	A, C, I, X	Data Breach Response Plan	No
TDIF 04 Functional Requirements	PRIV-03-06-05	A, C, I, X	Annual privacy transparency report	No
TDIF 04 Functional Requirements	FRAUD-02-02-01	A, C, I, X	Fraud Control Plan	Yes
TDIF 04 Functional Requirements	FRAUD-02-03-01	A, C, I, X	Fraud awareness training material	No
TDIF 04 Functional Requirements	FRAUD-02-05-10b	A, C, I, X	Fraud Incident Report	No
TDIF 04 Functional Requirements	PROT-04-01-07	A, C, I, X	Security awareness training material	No
TDIF 04 Functional Requirements	PROT-04-01-12	A, C, I, X	System Security Plan	No
TDIF 04 Functional Requirements	PROT-04-02-15	A, C, I, X	Cyber Security Incident reporting (procedures and reports)	No
TDIF 04 Functional Requirements	PROT-04-02-26	A, C, I, X	Disaster Recovery and Business Continuity Plan (DRBCP)	No
TDIF 04 Functional Requirements	PROT-04-02-29	A, C, I, X	Cryptographic Key Management Plan (CKMP)	Yes
TDIF 04 Functional Requirements	UX-05-01-05	A, C, I, X	Individual end-to-end journey map of the Applicant's *Identity System*	No
TDIF 04 Functional Requirements	UX-05-04-01	A, C, I, X	Usability Test Plan	Yes
TDIF 04 Functional Requirements	TEST-06-01-01	A, C, I, X	Technical Test Plan	Yes

Document	TDIF Req	Applicability	Evidence Required	Template Available?
	TEST-06-01-08 TEST-06-03-01		• Requirements Traceability Matrix • Technical Test Report	
TDIF 04 Functional Requirements	ASSESS-07-01-01	A, C, I, X	Functional Assessment - Privacy Impact Assessment	Yes
TDIF 04 Functional Requirements	ASSESS-07-01-04	A, C, I, X	Functional Assessment - Privacy Assessment (against TDIF requirements)	Yes
TDIF 04 Functional Requirements	ASSESS-07-02-01	A, C, I, X	Functional Assessment - Security Assessment	Yes – Use generic Functional Assessment template
TDIF 04 Functional Requirements	ASSESS-07-02-02	A, C, I, X	Functional Assessment – Penetration Test	Yes – Use generic Functional Assessment template
TDIF 04 Functional Requirements	ASSESS-07-03-01	A, C, I, X	Functional Assessment – Accessibility Assessment	Yes – Use generic Functional Assessment template
TDIF 05 Role Requirements	ROLE-02-01-01 to ROLE-02-01-06	A, C, I, X	User terms	No
TDIF 05 Role Requirements	IDP-03-08-10	I	Presentation Attack Detection (PAD) Report	No
TDIF 05 Role Requirements	IDP-03-08-23	I	*Assessing Officer Manual Face Comparison* training material	No

Additional accreditation evidence templates may become available in the future. Templates are available from the TDIF documents website.