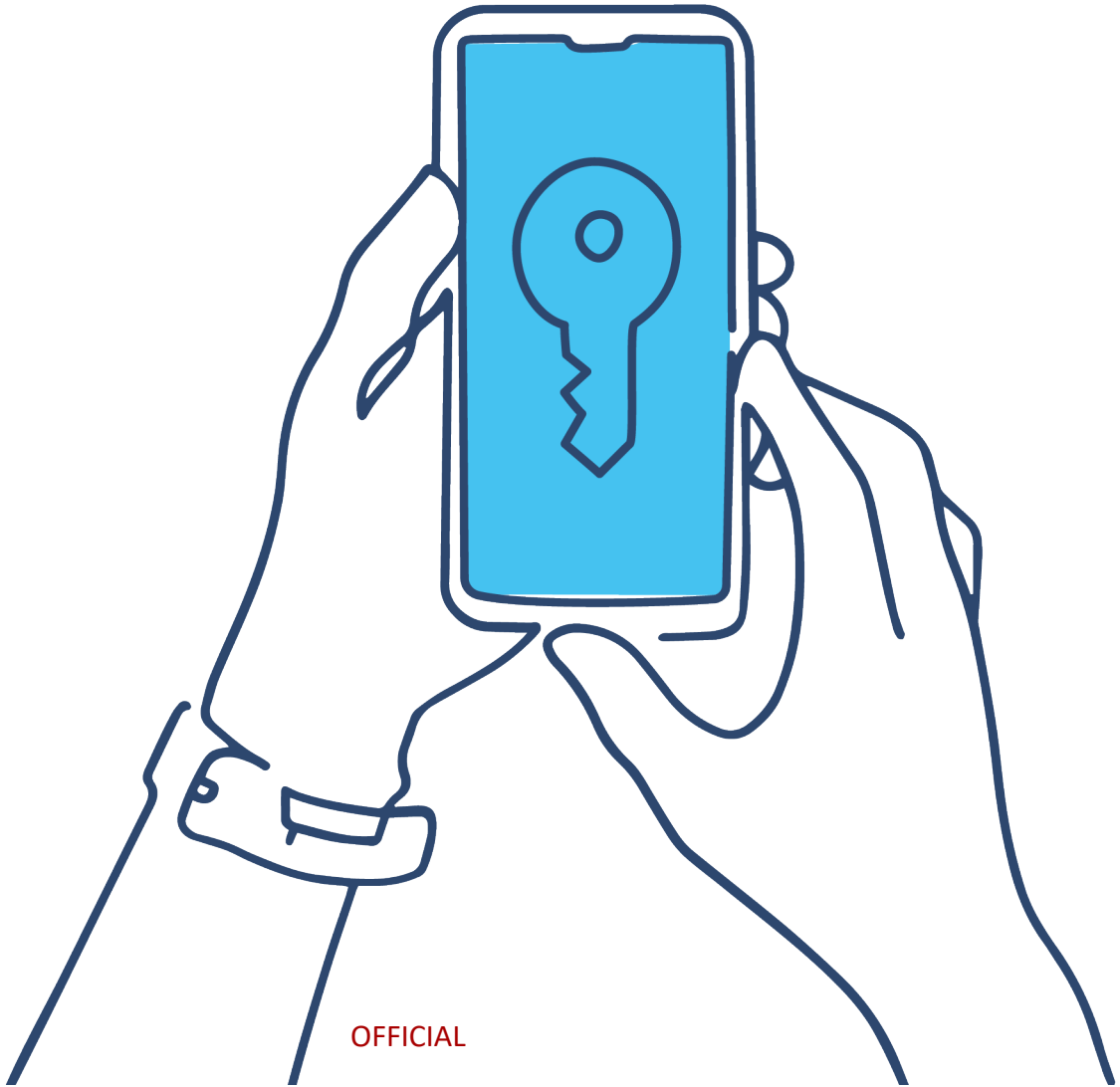
Australian Government | Digital Identity

03 Accreditation Process

Trusted Digital Identity Framework

Release 4.8 - Feb 2023

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

Document Version	Release 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	4.0	May 2020		Published version
1.1	4.3	Mar 2021	JK, SJP	Consultation version
1.2	4.4	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	4.5	Oct 2021	SJP	CRID0027 – Updated ACCRED-03-01-01, to require Applicants to submit a '*Statement of Claims*' as part of their TDIF application.
1.4	4.6	Mar 2022	JK, AV, MS, SJP, DN	Applicability of requirements added. Improvements to structure and clarity. Guidance updated. See TDIF Change Log for full list and description of changes
NA	4.7	June 2022		No changes to document
NA	4.8	Feb 2023		No changes to document

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

Contents

List of Figures

1 Introduction

This document sets out the details of the *TDIF Accreditation Process,* including:

- An overview of the preliminary preparations an organisation is expected to make before applying for TDIF accreditation
- Instructions and requirements for how to apply for TDIF accreditation
- Guidance for evidence types and assessment expectations during Initial accreditation and requirements for the finalisation of accreditation.
- An overview of the ongoing obligations a TDIF Accredited Provider is expected to meet in order to maintain its accreditation.

TDIF accreditation assessment involves a combination of evidence-based requirements, third party evaluations and operational testing that *Applicants* must complete to the satisfaction of the *DTA.* 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:

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

2 Overview of the TDIF Accreditation Process

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:** TDIF Accreditation Process Overview provides an overview of the *TDIF Accreditation Process* and **Error! Reference source not found.**, Page **Error! Bookmark not defined.** provides a detailed description of the accreditation activities.

Figure 1: *TDIF Accreditation Process Overview*

There are two phases of the TDIF Accreditation Process:

- **Initial accreditation** (this document) – the processes and activities to be undertaken by the *Applicant* to achieve TDIF accreditation. This phase covers the 'Preliminary Preparations', 'Request Accreditation', 'Meet TDIF Requirements' and 'Complete Accreditation' processes. To become accredited, the *Applicant* will need to meet all applicable TDIF requirements.
- **Maintaining Accreditation** - the processes and activities to be met by *Accredited Providers* to maintain their *TDIF accreditation*. This phase is the focus of the document titled *TDIF 07 Maintain Accreditation* and includes the continuing obligations and requirements *Accredited Providers* will be annually assessed on to maintain their accreditation.

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.

2.1 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 work together to provide *Identity System* components to form a *Digital Identity System* (multi-entity). For example, an *Applicant* accredited as a *Credential Service Provider* and a separate *Applicant* accredited as an *Identity Service Provider* may work together to provide a single product.
- 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 be TDIF accredited and must meet the *TDIF 06 Federation Onboarding Requirements* prior to joining the *Australian Government's Digital Identity System*.

In addition, to seek accreditation, the organisation must be able to meet the requirements set out in **Section 3.2 Request Accreditation** of this document.

Applicants for *TDIF Accreditation* should be aware that the TDIF prescribes a narrower scope of information sharing requirements than those in the *Privacy Act 1998* in order to support the TDIF principles as outlined in *TDIF 02 Overview*.

2.2 TDIF accreditation pathways

The *TDIF* supports two accreditation pathways:

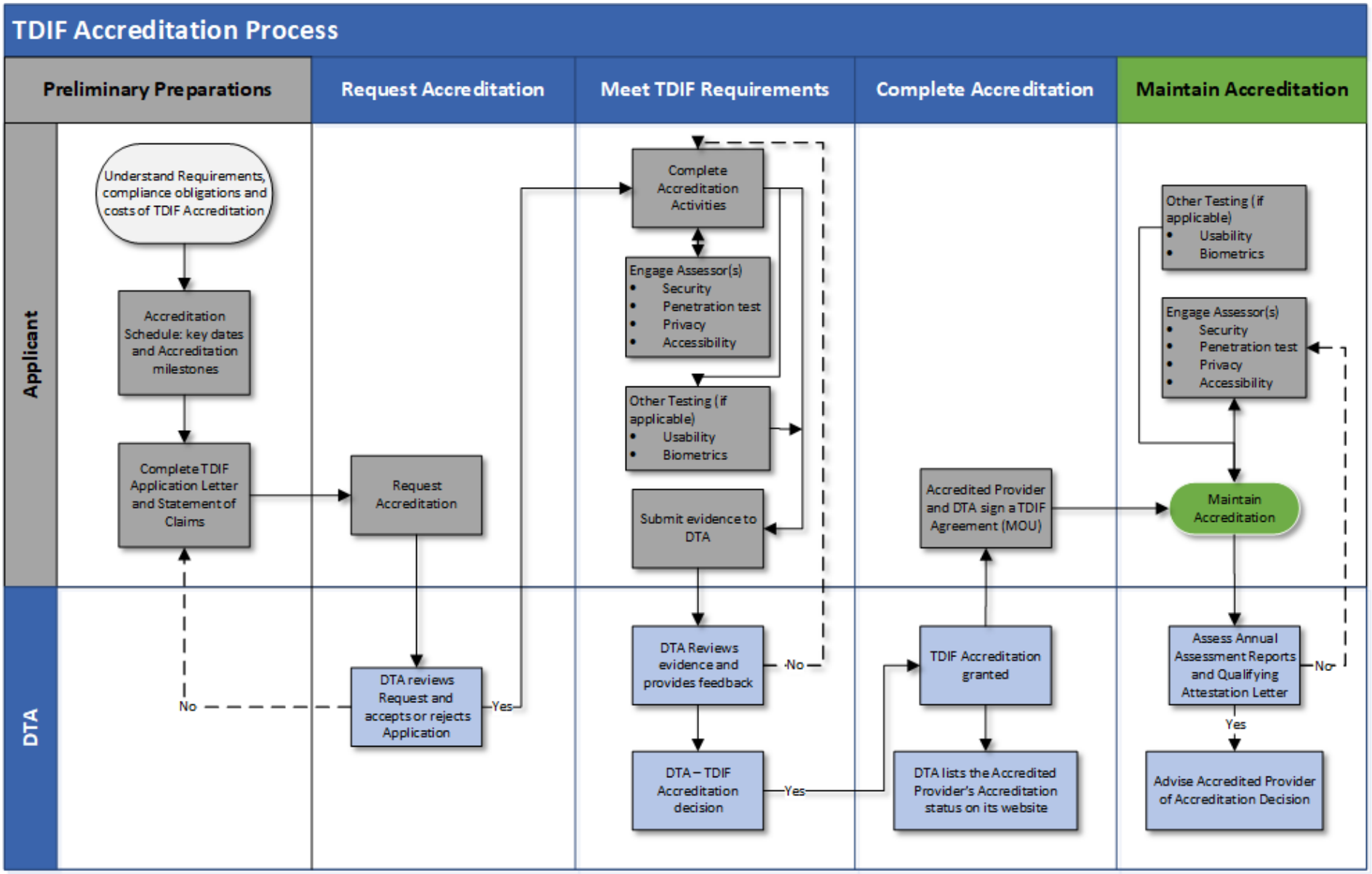
1. Organisations that do NOT connect to the *Australian Government's Digital Identity System.*
2. Organisations that connect to the *Australian Government's Digital Identity System*.
    a. NOTE: Joining the *Australian Government's Digital Identity System* is subject to a decision of Government.

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.

Table 1: TDIF Documents for Accreditation Pathway

Not connected to the *Australian Government's Digital Identity System*	Connected to the *Australian Government's Digital Identity System*
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 Assessment obligations	**Annual Assessment obligations**
TDIF 07 – Maintain Accreditation	*TDIF 07 – Maintain Accreditation*

Figure 2 - *TDIF Accreditation Process (detailed description)*



3 Initial accreditation Activities

The Accreditation Process follows the process outlined in Figure 2 on the previous page.

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 prepared 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[1]?
- 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 will 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*)

[1] 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?[2]
    - Are you aware that the TDIF requirements may be more prescriptive than existing legislative obligations or other frameworks? For example, the TDIF sets out narrower requirements for the handling of biometric information, as compared to the *Privacy Act 1988* (Cth).
    - 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*?
- Have you organised other relevant testers to conduct required testing? (i.e. *User Researcher* for *Usability Testing*, or a *Biometrics Testing Entity* for *Presentation Attack Detection* or *Biometric Matching* algorithm testing)
- 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 *TDIF Application Letter* and *TDIF Statement of Claims* has been accepted by the DTA**.**
- An *Applicant* should be able to achieve *TDIF* accreditation within 12 months of this acceptance to commence accreditation. Are you aware of the continuing obligations on *Accredited Providers*, as outlined in *TDIF 07 Maintaining Accreditation*?

Applicant Readiness:

The DTA will assess whether an *Applicant's Identity System* is mature enough to meet the TDIF requirements within the first three months of their accreditation. An

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

Applicant's Identity System does not need to be operational at the time of application, however, the *DTA* will only grant accreditation to an *Applicant* with a fully operational *Identity System* which meets all applicable *TDIF* requirements.

If an *Applicant's Identity System* is not able to meet the TDIF requirements according to the *Applicant's* set out accreditation schedule (submitted as part of the *TDIF Application Letter*), then the DTA may suspend the accreditation effort until such a time as the *Applicant* is deemed sufficiently ready or can produce the required evidence. Further information about suspended accreditation is provided in section 3.3.4 below.

The *DTA* does not grant partial accreditations.

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.

3.2.1 Application 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*[3].

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[4].

TDIF Req: ACCRED-03-01-01b; **Updated:** Mar-22**; Applicability:** A, C, I, X
The *Applicant* ***MUST*** have a registered and active ABN or ABRN.

TDIF Req: ACCRED-03-01-01c; **Updated:** Mar-22**; Applicability:** A, C, I, X
The Applicant ***MUST*** demonstrate that it is one of the following:

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

4 The DTA may request the original documents if they are in a language other than English.

- a body corporate incorporated by or under a law of the Commonwealth or a State or Territory
- a registered foreign company (within the meaning of the *Corporations Act 2001*)
- a Commonwealth entity, or a Commonwealth company, within the meaning of the *Public Governance, Performance and Accountability Act 2013*
- a person or body that is an agency within the meaning of the *Freedom of Information Act 1982*
- a body specified, or the person holding an office specified, in Part I of Schedule 2 to the *Freedom of Information Act 1982*
- a department or authority of a State
- a department or authority of a Territory.

TDIF Req: ACCRED-03-01-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *TDIF Application Letter* MUST specify all *Accredited Roles* being sought.

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*[5].

TDIF Req: ACCRED-03-01-02b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *TDIF Application Letter* MUST specify whether the *Identity System* supports:

- web responsive design (e.g. can be accessed through an internet browser)
- a mobile application (e.g. the *Identity System* is a mobile application)
- a component of either of the above (e.g. a white label service[6])

TDIF Req: ACCRED-03-01-02c; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *TDIF Application Letter* MUST specify whether the *Applicant* wants to connect to the *Australian Government's Digital Identity System*[7].

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

6 A white-label product is a product or service produced by one organisation that other organisations can rebrand to make it appear as if they had made it.

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

***TDIF* Req:** ACCRED-03-01-02d **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Application Letter* ***MUST*** include evidence which describes the architecture of the *Applicant's Identity System* and how it operates.[8]

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).

TDIF Req: ACCRED-03-01-04; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *TDIF Application Letter* ***MUST*** include an accreditation schedule which includes:

a. Estimated dates when *Functional Assessments* and any other required testing will be undertaken
b. Estimated dates when *Functional Assessment Reports* will be provided to the *DTA*
c. Estimated dates when the *Applicant's* other required evidence addressing *TDIF* requirements will be provided to the *DTA*[9].

[8] This is intended to support the DTA in its accreditation activities and assist it in determining the scope of *Functional Assessments*. The evidence should explain how the Applicant's Identity Facility operates, and provide the DTA with a sufficient understanding to enable it to work with the *Applicant* to determine whether a requirement has been met.

[9] The TDIF Application Letter template on the TDIF Website provides a list of applicable documentation. This list is also included at Appendix B: Accreditation Evidence of this document.

TDIF Req: ACCRED-03-01-04a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *TDIF Application Letter* ***MUST*** propose a commencement date and a date by which *TDIF* accreditation is expected to be completed[10].

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)[11] to manage their *TDIF* accreditation[12].

3.2.2 Exemption Requests

TDIF Req: ACCRED-03-01-06; **Updated**: Mar-22; **Applicability**: A, C, I, X
If an *Applicant* seeks a *TDIF Exemption Request* against an applicable *TDIF Requirement,* then it ***MUST*** submit a *TDIF Exemption Request* in accordance with ACCRED-03-01-06a and the process set out in **Appendix A:** TDIF exemption process.

TDIF Req: ACCRED-03-01-06a; **Updated**: Mar-22; **Applicability**: A, C, I, X
Each *TDIF Exemption Request* ***MUST*** include all information as described in **Appendix A:** TDIF exemption process and, at a minimum:

- A filled out *TDIF Exemption Request Form* signed by the *Applicant's Accountable Executive*
- A date of expiry or review of the Exemption Request that is not more than 12 months from the date of the request; and
- Any supporting information or statements for the risk assessment and mitigation measures.

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

11 For multi-entity accreditation, *personnel* across participating organisations will be required.

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

3.2.3 Alternative assessment reports

TDIF Accreditation requires that an *Applicant's Identity System* undergoes:

- *Functional Assessments* conducted by independent *Assessors*,
- (if applicable) a *Usability Test* conducted by a *User Researcher*, and
- (if applicable) biometrics testing conducted by a *Biometric Testing Entity*.

The DTA recognises that some of the *TDIF Functional Assessments* and other testing requirements may be equivalent to assessments an Applicant may have conducted on their *Identity System* prior to seeking TDIF Accreditation.

The *Applicant* may, as per its *TDIF Application Letter* and in accordance with the requirements below, submit an *Alternative Assessment Report* and request the *DTA* consider it as a substitute for a *Functional Assessment* or as evidence to meet other TDIF requirements.

Alternative Assessment Reports may also be submitted to meet an *Accredited Provider's Annual Assessment* obligations (further information can be found in *TDIF 07 Maintain Accreditation*).

Acceptance of *Alternative Assessment Reports*

At its discretion, the *DTA* may accept an *Alternative Assessment Report* conducted on the *Applicant's Identity System* as a substitute for a *Functional Assessment* required by the *TDIF*. Where an *Alternative Assessment Report* is submitted, the *Applicant* must also submit a *Requirements Traceability Matrix*, which sets out how the scope of the *Alternative Assessment Report* covers the relevant *TDIF* requirements.

Any decisions made by the DTA to reject an *Alternative Assessment Report* will be made in writing to the *Applicant*.

Where the *DTA* determines an *Alternative Assessment Report*:

- 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*.

In general, the DTA accreditation team will consider *Alternative Assessment Reports* that have been prepared according to standards or guides issued by a recognised body[13], or where such work has been prepared as part of an assessment or accreditation processes that follows a recognised framework[14].

Alternative Assessment Reports that will be considered for *Security Assessments* include, but is not limited to:

- ISO/IEC 27001 – Information Security Management
- SOC 2 (Service Organisation Control 2) Type 2 reports
- IRAP assessments
- Payment Card Industry (PCI) Data Security Standard.

Alternative Assessment Reports that will be considered for *Privacy Impact Assessment*s includes, but is not limited to, Data Protection Impact Assessments (conducted in accordance with relevant GDPR law).

3.2.3.1 Alternative assessment reports Requirements

TDIF Req: ACCRED-03-01-07; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant* *MAY* submit an *Alternative Assessment Report,* which it requests the *DTA* consider as a substitute for a relevant *Functional Assessment* or as evidence to meet other TDIF requirements. If the Applicant submits an Alternative Assessment Report, it *MUST* do so in accordance with the following requirements.

TDIF Req: ACCRED-03-01-07a; **Updated**: Mar-22; **Applicability**: A, C, I, X
Any request made to the *DTA* to consider *Alternative Assessment Reports* *MUST* include:

a) Which *Functional Assessment* or TDIF requirements it is provided as evidence for

[13] For example, standards bodies such as ISO or Standards Australia; government bodies such as ACSC/ASD, NIST (United States) GCHQ (UK based); industry associations, such as IETF, W3C, FIDO, PCI DSS.

[14] For example, assessments completed based on ISO 19011 audit principles, ASD's IRAP, or NATA accreditation.

b) A rationale for why the *Alternative Assessment Report* should be considered as equivalent to a *Functional Assessment* or as appropriate evidence to meet the TDIF Requirements, and
c) A *Requirements Traceability Matrix*, which sets out:
    i. each TDIF requirement the *Alternative Assessment Report* addresses,
    ii. a reference to where the *Alternative Assessment Report* addresses that TDIF requirement (e.g. page number or section), and
    iii. any supporting statements for why that section of the Alternative Assessment Report addresses the TDIF requirements (if needed).

TDIF Req: ACCRED-03-01-07b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Alternative Assessment Report* *MUST* have been produced no more than 12 months prior to the date it is assessed by the DTA and *MUST* cover the latest *Major Production Release* of the *Applicant's Identity System* (if any)

3.2.4 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 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*.

Once the *Applicant's* request for accreditation has been accepted, the Applicant will then be required to submit evidence to meet the TDIF Requirements.

3.3 Meet TDIF Requirements

The 'Meet TDIF Requirements' activity requires the *Applicant* to demonstrate how it meets all applicable *TDIF* requirements. The DTA will assess the *Applicant's* submitted evidence and statements and decide whether it satisfies the TDIF requirements.

3.3.1 TDIF Requirement Applicability

The *TDIF* requirements are written for a broad spectrum of *Identity Systems*. As described in *TDIF 02 Overview*, each requirement has an applicability indicator, which indicates the accredited roles to which a requirement applies.

However, requirements may be deemed non-applicable to an *Applicant's* role if the requirement does not apply to its *Identity System*. This may be because the requirement is for a feature or function which is not implemented by the *Applicant's Identity System*, such as a particular *Credential Type* (e.g. the *Applicant's Identity System* only supports *Multi-factor Cryptographic Software* and not any other *Credential Type*), or an *Identity Proofing level* (e.g. the *Applicant's Identity System* only supports *IP 2*).

Sections of requirements that contain features or functions which may be considered non-applicable are indicated by a qualifying requirement

For example:

> **TDIF Req:** CSP-04-02-01; **Updated**: Jun-21; **Applicability**: C
> If *Memorised Secrets* are supported, then the *Applicant* *MUST* implement the following requirements for the operation of *Memorised Secrets*.

If the Applicant's *Identity System* does not support the described feature, then the DTA may seek additional information from the Applicant to review the scope and applicability of the relevant TDIF requirements for that feature.

3.3.2 Assessment

The TDIF is a risk-based accreditation framework and as such, the assessment process involves the DTA using a risk-based approach to determining compliance with the TDIF accreditation framework, and to determine whether the Applicant's *Identity System* can meet the standards required by the TDIF. The *DTA* uses a variety of methods to assess evidence submitted by *Applicants* to ensure they meet applicable requirements, including a review of:

- The *Applicant's Statement of Claims*
- the *Application Letter, Statement of Applicability* and accreditation schedule
- risk management and organisational governance material
- architectural and network diagrams and system information
- policies, plans and procedures
- training materials provided to staff
- test plans, test scripts and source code reviews
- independent *Assessors'* reports (*Functional Assessments* and other test material)

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 to assist with meeting the TDIF 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.

The DTA will assist the *Applicant* meet its accreditation schedule (provided with the *Application Letter*) by, setting up regular accreditation check in meetings and, where required, targeted workshops to assist the *Applicant* to meet any outstanding requirements. However, certain factors may impact on the time taken to complete an accreditation activity. These may 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 recommendations, risks or non-compliance issues to the satisfaction of the *DTA*.

The DTA will work with the Applicant in an open and transparent manner throughout the accreditation process. Any information shared is handled by the relevant personnel on a need-to-know basis. Unless otherwise agreed between the *Applicant* and the *DTA*, all evidence provided to the *DTA* will be treated as *OFFICIAL information*[15].

3.3.3 Assessors and Functional Assessments

As part of Accreditation for both initial and annual requirements an *Applicant* will need to obtain appropriate *Assessors* to conduct *Functional Assessments* and depending on the other functions of the *Applicant's Identity System*, other required testing. The *DTA* does not maintain a list of *Assessors*. As part of good corporate governance, the *Applicant* must research, identify and obtain appropriate *Assessors* with the relevant skills, experience, independence and qualifications to undertake *Functional Assessments* and other required testing. Requirements for *Assessors* are in *TDIF 04 Functional Assessments* and *TDIF 07 Maintain Accreditation*.

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*.

Applicants are required 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.

15 Note 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.

- *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 may be required to engage the following testers:

- *Usability Testing* must be undertaken by an appropriately qualified *User Researcher*.
- *Identity Service Providers* and *Credential Service Providers* that seek TDIF accreditation for *Identity Facilities* that include the collection of biometrics[16] may be required to undergo biometric testing, which must be undertaken by a qualified, third-party *Biometric Testing Entity* as outlined in Section 3.8 in TDIF 05 Role Requirements.

Guidance and further information regarding *Assessors* for *Functional Assessments* and *User Researchers* for the *Usability Testing* is available in *TDIF 04A Functional Guidance.* Guidance for biometric testing is available in *TDIF 05A Role Guidance*.

3.3.4 Forward Work Plans

Further information regarding *Forward Work Plans*, including requirements, timeframes and activities required is available in Section 7 Functional Assessments of *TDIF 04 Functional Assessments* and Section 2.8 Annual Assessment Reports of *TDIF 07 Maintain Accreditation*.

Where an *Assessor,* the *Applicant* or *Accredited Provider* has identified risks, recommendations or non-compliances as part of its submitted evidence to the DTA

[16] In accordance with Section 3.8 of TDIF 05 Role Requirements or Section 3.4.4 of TDIF 05 Role Requirements respectively.

for its *Functional Assessments*, the *Accountable Executive* must respond with a timeframe for mitigation actions to be taken and implemented to address the risk, recommendation or non-compliance. The DTA will record all ongoing remediation activities in a *Forward Work Plan* and follow up on outstanding items with the *Applicant* on or around the date recorded for remediation.

A *Forward Work Plan* does not substitute and will not replace an *Applicant's* or *Accredited Provider's* obligations to meet all applicable *TDIF* requirements covered by the *Functional Assessments* to be accredited or maintain accreditation, respectively.

3.3.5 TDIF Updates and Versions

The TDIF is updated regularly in accordance with the TDIF Variance Standard Operating Procedure (available on the TDIF website). The version of the TDIF that an *Applicant* is accredited against will be the version currently published on the TDIF website at the time of the DTA's acceptance to commence accreditation.

Accredited Providers will be required to meet any new or amended requirements in the newest version of the TDIF, published on the TDIF website, within 12 months of that version being published. These requirements will be assessed as part of the *Accredited Provider's Annual Assessment.*

3.3.6 Suspending Initial accreditation

If an *Applicant* fails to submit evidence to support their accreditation or meet their accreditation obligations, the DTA may suspend the accreditation effort until the *Applicant* is deemed sufficiently ready or can produce the required evidence.

Prior to resuming the accreditation effort, the Applicant will need to submit an updated Accreditation Schedule (as per ACCRED-03-01-04).

In reviewing an Applicant's request to resume the accreditation effort, the DTA will also consider its own capacity to resume the accreditation. This may result in the DTA exercising its discretion to delay the accreditation, in order to appropriately allocate time and resources to review the Applicant's accreditation evidence.

Applicants should note that the DTA has discretion to terminate the request for accreditation if the Applicant continues to delay submitting evidence to meet their accreditation obligations for assessment.

3.3.7 Varying Accreditation during Initial accreditation

An Applicant may seek to vary aspects of its accreditation during the initial accreditation process. This may be because they have implemented additional features or wish to be accredited for another Role. A variation in accreditation will result in a rescoping activity to ensure any requirements previously marked as non-applicable are captured in the assessment, and a reassessment of any TDIF requirements and any previously submitted evidence already marked as complete. For example, if an Applicant has sought accreditation as an Identity Service Provider for Identity Proofing Level 1 Plus and then wishes to adjust this to Identity Proofing Level 3, it will now have to meet Section 3.8 Biometric Binding Requirements in TDIF 05 Role Requirements and reassess any other documentation that the introduction of biometrics will impact upon (likely all of the TDIF 04 Functional Assessment evidence).

In reviewing an Applicant's request to vary its accreditation, the DTA will also consider its own capacity to assess the varied accreditation evidence. This may result in the DTA exercising its discretion to delay the accreditation, in order to appropriately allocate time and resources to review the Applicant's accreditation evidence

TDIF Req: ACCRED-03-03-01; **Updated**: Mar-22; **Applicability**: A, C, I, X
If a Provider seeks to vary its accreditation, then it *MUST* apply for a *Variation to Accreditation* and submit an updated *TDIF Application Letter*, and other required evidence, as per requirements ACCRED-03-01-01 to ACCRED-03-01-05 and the following requirements.

TDIF Req: ACCRED-03-03-01a; **Updated**: Mar-22; **Applicability**: A, C, I, X
The *Applicant MUST* submit a *Requirements Traceability Matrix* and identify all applicable TDIF requirements that may be impacted by the variation of accreditation.

NOTE: the DTA will assess the *Requirements Traceability Matrix* and may identify additional applicable requirements that an *Applicant* must submit evidence for.

TDIF Req: ACCRED-03-03-01b; **Updated**: Mar-22; **Applicability**: A, C, I, X
The Applicant *MUST* include and submit to the DTA a review of the applicable evidence required for variation of accreditation, **as outlined in Appendix C.**

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[17]

3.4.1 Finalisation of Accreditation Requirements

TDIF Req: ACCRED-03-04-01; **Updated**: Jun-21; **Applicability**: A, C, I, X
Once the applicant has achieved all applicable requirements, the *Applicant MUST* submit a *Qualifying Attestation Letter* signed by the *Applicant's Accountable Executive* that contains the following information to support its claim that its operations are in accordance with *TDIF* requirements:

- The name, role/position and contact details of the *Accountable Executive*
- A statement that the *Accredited Provider's Identity System* complies with the assessed TDIF requirements
- The version of the TDIF the Accredited Provider is assessed and accredited under for the Initial Assessment[18].
- a statement confirming it has provided the DTA with all relevant documents, materials and evidence to the accreditation as part of its review
- A statement confirming that the evidence provided is a fair and accurate representation of its *Identity System*
- If the *Applicant* has risks, recommendations or non-compliances identified in its *Forward Work Plan*, then the *Qualifying Attestation Letter MUST* contain a

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

18 An Accredited Provider's obligations to comply with the latest version of the TDIF published on the TDIF website is outlined in the TDIF Agreement (MOU)

summary of these risks, implementation dates and any further information as per ASSESS-07-04-02 and ASSESS-07-04-03.

A template for the Qualifying Attestation Letter is available from the TDIF website.

TDIF Req: ACCRED-03-04-02; **Updated**: Mar-22; **Applicability**: A, C, I, X
Once the *Applicant* has achieved all applicable requirements, it ***MUST*** sign a TDIF Agreement (MOU) with the DTA, which sets out the rights, roles and obligations of both parties in relation to the *Accredited Provider's* TDIF accreditation.

3.4.2 Accredited Providers Register

The DTA will list the following information on the TDIF website:

- The Accredited *Identity System*'s service name
- The *Accredited Provider's* name
- For *Identity Service Providers*:
    - The Service Type (mobile application or web-based)
    - Accredited *Identity Proofing* Levels
    - *Verification* Type (reusable identity or one-off verification)
- For *Credential Service Providers*:
    - Accredited *Credential Levels*
    - Accredited *Credential Types*
- For *Identity Exchanges*: An Interoperability Statement
- For *Attribute Service Providers*:
    - Accredited Attribute Class
    - Attribute(s) Name or Description
- The Initial accreditation Date
- The Accreditation Status (Active, Suspended, Terminated)

Summary of Accreditation:

The DTA will complete a high-level Summary of Accreditation, which may be listed on the TDIF website. The report will cover all sections of TDIF requirements the Accredited Provider is accredited against and any conditions of its accreditation.

4 Maintain Accreditation

Once accredited, the *Accredited Provider* must satisfy certain obligations in order to maintain its *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 Maintain Accreditation.*

In addition, an *Accredited Provider* must continue to meet its ongoing obligations in the *TDIF*. These include requirements to report Digital Identity Fraud Incidents and Cyber Security Incidents and maintain its compliance with the *TDIF* while accredited.

4.1 Varying an Accreditation

Detailed information regarding variations in TDIF accreditation including triggers, requirements, timeframes and activities required is available in *TDIF 07 Maintain Accreditation.*

An *Accredited Provider* may seek to vary its accreditation in response to changes to its architecture, a new feature implementation, step-up of *Identity Proofing* or *Credential levels*, or if it is seeking to be accredited for an additional role.

A change in architecture or feature implementation is likely to have impacts on other TDIF requirements, such as the *Accredited Provider*'s System Security Plan, Fraud Control Plan and Privacy arrangements and documentation. These circumstances may result in the DTA assessing the *Accredited Provider* for reaccreditation.

4.2 TDIF Reaccreditation

Detailed information regarding *TDIF Reaccreditation*, including triggers for reaccreditation, requirements, timeframes and activities required is available in *TDIF 07 Maintain Accreditation.*

TDIF Reaccreditation is a process where an *Accredited Provider* is directed by the DTA to complete accreditation activities in addition to their ongoing obligations to maintain accreditation. It encompasses a review and rescoping of all applicable initial

accreditation requirements to assess whether any further evidence statements or updates to documentation is required in response to the reason the *Accredited Provider* has been directed to complete a Reaccreditation Activity.

4.3 Suspension and Termination of Accreditation

Detailed information about suspension or termination of *Accreditation* is available in *TDIF 07 Maintain Accreditation*.

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.

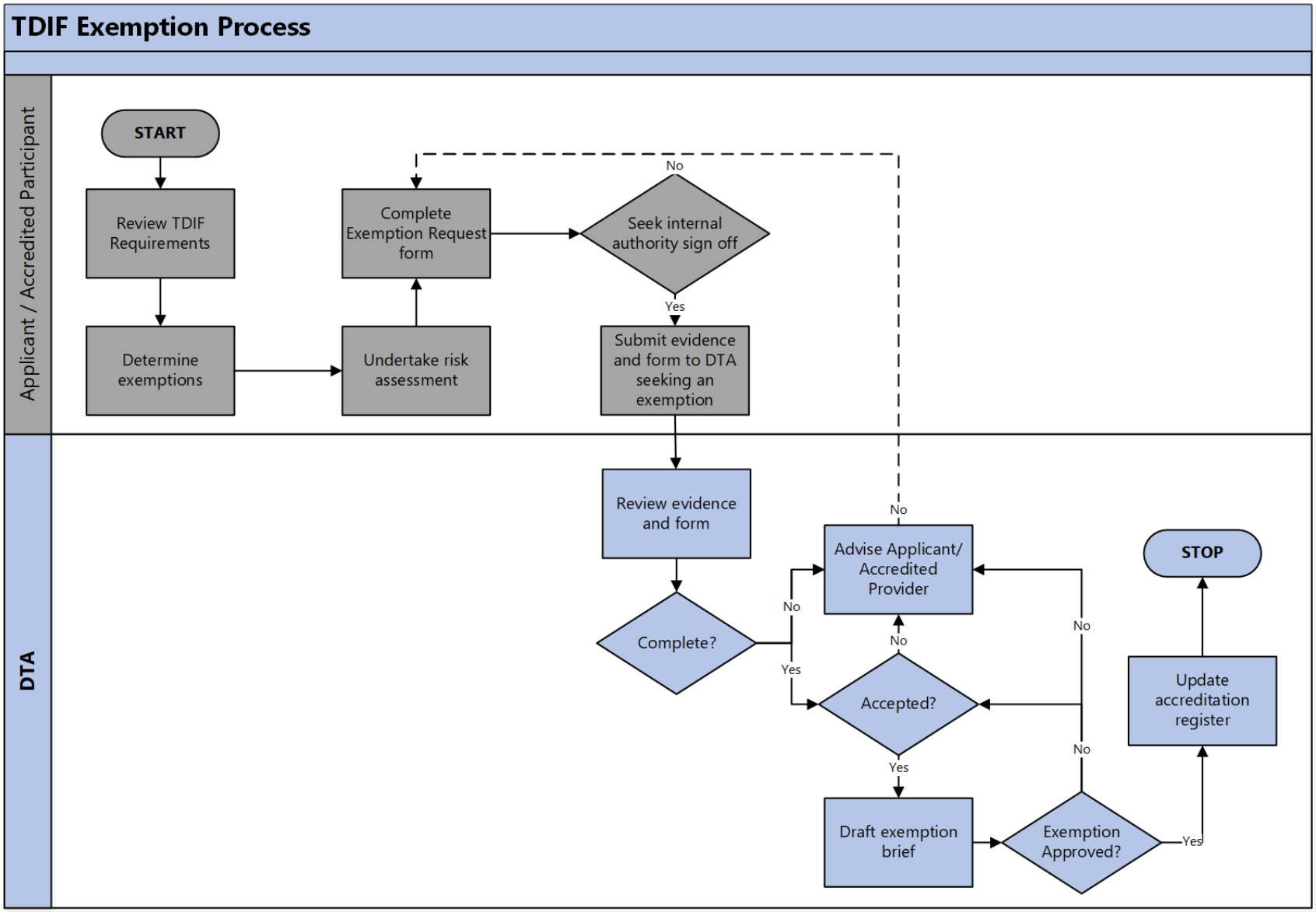
An Applicant or Accredited Provider must provide a completed *Exemption Request Form* (available from the TDIF website) which contains the following information:

- The TDIF Requirements the *Exemption Request* is sought for
- An end date for the *Exemption Request*
    - Note that *Exemption Request*s will be reviewed as part of the *Accredited Provider's Annual Assessment*
- Justification for the Exemption Request
- Alternative mitigations to support the Applicant's justification for the request
- A Risk Assessment for risks arising out of an Applicant not meeting the exempt TDIF Requirement including:
    - Risk statements
    - Likelihood
    - Consequences
    - A risk rating (according to the Applicant's own risk framework)
    - Treatments in place and any recommended treatments
- Dates for implementation of endorsed mitigation methods or treatment recommendations (these items will be added to the *Applicant's Forward Work Plan*)
- Any supporting evidence or additional information may be appended to the form and submitted for the DTA to review.

The *Applicant's* relevant *Accountable Executive* must review and endorse the Exemption Request.

Figure 3 provides an overview of the key steps in the process.

Figure 3: *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 make an exemption request. *Applicants* must demonstrate that an *Exemption Request* is required to support business needs or address likely, realistic or probable risks. The *DTA* will not support an exemption request where the *Applicant* simply chooses not to meet a *TDIF* requirement.

The *Applicant* is required to conduct a risk assessment on the proposed exemption(s) and collect relevant evidence which supports the exemption request. This information is to be included in a *TDIF Exemption Request* form that is to be submitted to the *Applicant's relevant Accountable Executive*[19] for approval.

A.2.2 Exemption request form

The *Applicant's Accountable Executive* 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.

If supported, the *Applicant's Accountable Executive* 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). These items will be added to the *Applicant's Forward Work Plan.*

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.

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

A.2.3 Assessment validation

Following this internal signoff, the *Applicant* is required to submit its evidence and a 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.

A.2.4 Accreditation conclusion

Upon receipt of the *Exemption Request Form* and supporting documentation the *DTA's* delegate will form an opinion on the evidence provided and decide whether to accept or reject on 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's decision will be provided in writing 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 to achieve accreditation.

As the justification for exemptions may change and the risk environment will continue to evolve over time, *Applicants* are required to 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. Additional information is available in *TDIF 07 Maintain Accreditation.*

Appendix B: Accreditation Evidence

Table 2: 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-03-01-01	A, C, I, X	*Identity System* Architecture documents	No
TDIF 03 Accreditation Process	ACCRED-03-01-06a	A, C, I, X	Exemption Request Form and Evidence	Yes
TDIF 03 Accreditation Process	ACCRED-03-04-01	A, C, I, X	Qualifying Attestation Letter	Yes
TDIF 03 Accreditation Process	ACCRED-03-04-02	A, C, I, X	TDIF Agreement (MOU)	DTA to provide
TDIF 04 Functional Requirements	FRAUD-02-01-02	A, C, I, X	Assessment of the Digital Identity Fraud Risk (incorporated in Fraud Control Plan)	No
TDIF 04 Functional Requirements	FRAUD-02-02-01 FRAUD-02-02-01a	A, C, I, X	Fraud Control Plan	No
TDIF 04 Functional Requirements	FRAUD-02-03-01 FRAUD-02-03-02	A, C, I, X	Fraud awareness training material	No
TDIF 04 Functional Requirements	FRAUD-02-05-06 FRAUD-02-05-06a	A, C, I, X	*Digital Identity Fraud Incidents* Report (quarterly – 3 months)	No
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 Plan	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 PRIV-03-06-05a	X	Annual Transparency Report	No
TDIF 04 Functional Requirements	PRIV-03-10-02a	A, C, I, X	(if applicable) cross-border disclosure agreements	No

TDIF 04 Functional Requirements	PROT-04-01-01		Assessment of the Cyber Security Risks (incorporated in System Security Plan)	No
TDIF 04 Functional Requirements	PROT-04-01-05a PROT-04-01-08	A, C, I, X	Security awareness training material	No
TDIF 04 Functional Requirements	PROT-04-01-11 PROT-04-01-11a	A, C, I, X	System Security Plan	No
TDIF 04 Functional Requirements	PROT-04-01-15a	A, C, I, X	Security maturity monitoring	No
TDIF 04 Functional Requirements	PROT-04-02-09	A, C, I, X	Procedures setting out criteria for Cyber Security Incident investigation processes	No
TDIF 04 Functional Requirements	PROT-04-02-14 PROT-04-02-14a	A, C, I, X	Cyber Security Incident reporting (quarterly – 3 months)	No
TDIF 04 Functional Requirements	PROT-04-02-24	A, C, I, X	Disaster Recovery and Business Continuity Plan (DRBCP)	No
TDIF 04 Functional Requirements	PROT-04-02-27	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-05-04-02 UX-05-04-06b	A, C, I, X	Usability Test Plan and Usability testing	No
TDIF 04 Functional Requirements	TEST-06-01-01 TEST-06-01-02 TEST-06-01-03	A, C, I, X	Technical Testing evidence • Requirements Traceability Matrix • Technical Test Report	No
TDIF 04 Functional Requirements	ASSESS-07-01-01	A, C, I, X	Assessors must conduct a) a Privacy Impact Assessment in accordance with ASSESS-07-05-01 b) a Privacy Assessment in accordance with ASSESS-07-05-03 c) a Penetration Test in accordance with ASSESS-07-06-02 d) a Security Assessment in accordance with ASSESS-07-06-01; and	No

			e) an Accessibility Assessment in accordance with ASSESS-07-07-01.	
TDIF 04 Functional Requirements	ASSESS-07-04-01 ASSESS-07-04-02 ASSESS-07-04-03	A, C, I, X	Functional Assessment Reports (for each functional assessment conducted under ASSESS-07-01-01 and the relevant other requirement number)	Yes
TDIF 05 Role Requirements	ROLE-02-01-01 ROLE-02-01-01a	A, C, I, X	User terms	No
TDIF 05 Role Requirements	IDP-03-08-03	I	Biometric Binding Fraud Risks (can be incorporated into Fraud Control Plan and System Security Plan)	No
TDIF 05 Role Requirements	IDP-03-08-07	I	Biometric Testing Entity qualifications evidence	No
TDIF 05 Role Requirements	IDP-03-08-12 – IDP-03-08-12i	I	Presentation Attack Detection (PAD) test Report	Yes
TDIF 05 Role Requirements	IDP-03-08-18 - IDP-03-08-18d	I	Technical Biometric Matching Algorithm test Report	Yes
TDIF 05 Role Requirements	IDP-03-08-24 - IDP-03-08-24b	I	*Assessing Officer Manual Face Comparison* training materials	No
TDIF 05 Role Requirements	IDP-03-08-54 IDP-03-08-26	I	*Assessing Officer Manual Face Comparison* procedures to detect Fraudulent activities. Quality control and assurance measures for decisions made by *Assessing Officers*.	No
TDIF 05 Role Requirements	CSP-04-03-03g	C	Presentation Attack Detection (PAD) test Report	No
TDIF 05 Role Requirements	ASP-05-02-01a	A	Evidence of the arrangement with an Authoritative Source	No

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

Appendix C: Variations of Initial accreditation Evidence

Table 3: Variations of Initial accreditation Evidence Review

Document	TDIF Req	Applicability	Evidence Required	Review Required?
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-03-01-01	A, C, I, X	*Identity System* Architecture documents	Yes
TDIF 03 Accreditation Process	ACCRED-03-01-06a	A, C, I, X	Exemption Request Form and Evidence	DTA to Advise
TDIF 03 Accreditation Process	ACCRED-03-04-01	A, C, I, X	Qualifying Attestation Letter	Yes
TDIF 03 Accreditation Process	ACCRED-03-04-02	A, C, I, X	TDIF Agreement (MOU)	DTA to Advise
TDIF 04 Functional Requirements	FRAUD-02-01-02	A, C, I, X	Assessment of the Digital Identity Fraud Risk (incorporated in Fraud Control Plan)	Yes
TDIF 04 Functional Requirements	FRAUD-02-02-01 FRAUD-02-02-01a	A, C, I, X	Fraud Control Plan	Yes
TDIF 04 Functional Requirements	FRAUD-02-03-01 FRAUD-02-03-02	A, C, I, X	Fraud awareness training material	Yes
TDIF 04 Functional Requirements	FRAUD-02-05-06 FRAUD-02-05-06a	A, C, I, X	*Digital Identity Fraud Incidents* Report (quarterly – 3 months)	No
TDIF 04 Functional Requirements	PRIV-03-02-03	A, C, I, X	Privacy Policy	Yes
TDIF 04 Functional Requirements	PRIV-03-02-06	A, C, I, X	Privacy Management Plan	Yes

TDIF 04 Functional Requirements	PRIV-03-02-08	A, C, I, X	Privacy awareness training material	Yes
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 PRIV-03-06-05a	X	Annual Transparency Report	No
TDIF 04 Functional Requirements	PRIV-03-10-02a	A, C, I, X	(if applicable) cross-border disclosure agreements	Yes
TDIF 04 Functional Requirements	PROT-04-01-01	A, C, I, X	Assessment of the Cyber Security Risks (incorporated in System Security Plan)	Yes
TDIF 04 Functional Requirements	PROT-04-01-05a PROT-04-01-08	A, C, I, X	Security awareness training material	Yes
TDIF 04 Functional Requirements	PROT-04-01-11 PROT-04-01-11a	A, C, I, X	System Security Plan	Yes
TDIF 04 Functional Requirements	PROT-04-01-15a	A, C, I, X	Security maturity monitoring	Yes
TDIF 04 Functional Requirements	PROT-04-02-09	A, C, I, X	Procedures setting out criteria for Cyber Security Incident investigation processes	No
TDIF 04 Functional Requirements	PROT-04-02-14 PROT-04-02-14a	A, C, I, X	Cyber Security Incident reporting (quarterly – 3 months)	No
TDIF 04 Functional Requirements	PROT-04-02-24	A, C, I, X	Disaster Recovery and Business Continuity Plan (DRBCP)	Yes
TDIF 04 Functional Requirements	PROT-04-02-27	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*	DTA to Advise

TDIF 04 Functional Requirements	UX-05-04-02 UX-05-04-06b	A, C, I, X	Usability Test Plan and Usability testing	Yes
TDIF 04 Functional Requirements	TEST-06-01-01 TEST-06-01-02 TEST-06-01-03	A, C, I, X	Technical Testing evidence • Requirements Traceability Matrix • Technical Test Report	Yes
TDIF 04 Functional Requirements	ASSESS-07-01-01	A, C, I, X	Assessors must conduct a) a Privacy Impact Assessment in accordance with ASSESS-07-05-01 b) a Privacy Assessment in accordance with ASSESS-07-05-03 c) a Penetration Test in accordance with ASSESS-07-06-02 d) a Security Assessment in accordance with ASSESS-07-06-01; and e) an Accessibility Assessment in accordance with ASSESS-07-07-01.	Yes
TDIF 04 Functional Requirements	ASSESS-07-04-01 ASSESS-07-04-02 ASSESS-07-04-03	A, C, I, X	Functional Assessment Reports (for each functional assessment conducted under ASSESS-07-01-01 and the relevant other requirement number)	Yes
TDIF 05 Role Requirements	ROLE-02-01-01 ROLE-02-01-01a	A, C, I, X	User terms	Yes
TDIF 05 Role Requirements	IDP-03-08-03	I	Biometric Binding Fraud Risks (can be incorporated into Fraud Control Plan and System Security Plan)	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-07	I	Biometric Testing Entity qualifications evidence	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-12 – IDP-03-08-12i	I	Presentation Attack Detection (PAD) test Report	DTA to advise

TDIF 05 Role Requirements	IDP-03-08-18 - IDP-03-08-18d	I	Technical Biometric Matching Algorithm test Report	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-24 - IDP-03-08-24b	I	*Assessing Officer Manual Face Comparison* training materials	DTA to advise
TDIF 05 Role Requirements	IDP-03-08-54 IDP-03-08-26	I	*Assessing Officer Manual Face Comparison* procedures to detect Fraudulent activities. Quality control and assurance measures for decisions made by *Assessing Officers*.	DTA to advise
TDIF 05 Role Requirements	CSP-04-03-03g	C	Presentation Attack Detection (PAD) test Report	DTA to advise
TDIF 05 Role Requirements	ASP-05-02-01a	A	Evidence of the arrangement with an Authoritative Source	DTA to advise

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