Australian Government
Digital Transformation Agency

05 - Role Requirements

Trusted Digital Identity Framework Release 4
March 2021, version 1.5

PUBLISHED VERSION

dta

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

Contact us

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 the Director, Digital Identity Policy at identity@dta.gov.au.

Document management

The *DTA* has reviewed and endorsed this document for release.

Change log

Version	Date	Author	Description of the changes
0.1	July 2019	SJP	Initial version
0.2	Oct 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 third consultation round on TDIF Release 4
1.0	May 2020		Published version
1.1	Aug 2020	MC	Minor updates to Tables 1 and 5
1.2	Sep 2020	MC	Minor update to IP3 wording and Table 1 Operation Objective and update to Appendix A UiTC Document Concession Card.
1.3	Jan 2021	JK	CRID0005 – Emergency Change to CSP-04-01-05a – referenced requirement that did not exist. Corrected.
1.4	Feb 2021	JK	CRID0008 – Emergency Change to IDP-03-07-03 – referenced incorrect requirement.
1.5	Mar 2021	JK	CRID0017 – Emergency Change to IDP-03-08-21 – Temporary error while waiting for legislation to pass to implement.

Document review

The next scheduled review of this document will occur by July 2022. Any changes made to the document prior to this date will be recorded in a *TDIF* change management document and published to the *DTA* website.

Contents

List of tables

1 Introduction

This document sets out the *TDIF* role requirements to be met by *Applicants* in order to achieve *TDIF* accreditation.

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

The intended audience for this document includes:

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

2 Common Role Requirements

2.1 User terms

2.1.1 Usage terms

TDIF Req: ROLE-02-01-01; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have user terms that include:

a) A description of the nature of the identity system (consistent with the *TDIF*) provided to the *User* by the *Applicant*.

b) A general acknowledgment by the *User* that their use of the identity system provided by the *Applicant* is governed by the user terms.

c) The *Applicant's* identity system is provided on an 'as is' and 'as available' basis.

d) The scope of the *User's* right to access and use the identity system must be consistent with the *TDIF*.

e) The *User* is responsible for its use of the *Applicant's* identity system, including any *Identity Documents* it provides to the *Applicant*, and will use the service in compliance with all applicable laws.

f) The *User* is responsible to provide accurate *Identity Documents* and *Attributes* to the *Applicant*.

g) The *User* does not share *Attributes*, *Personal information* or *Sensitive information*, or *Credentials* with third parties without the *Consent* of the *Individual*.

h) The *User* reports unauthorised use of their *Digital Identity* or *Credential* to the *Applicant* as soon as they become aware of it.

i) The *Applicant* may suspend, cancel or terminate the *User's* access to the identity system at any time.

j) That the *Applicant* may make changes to the user terms at any time without prior notice and if the user terms are changed, the *User's* continued use of the identity system will be subject to their acceptance of the updated user terms.

2.1.2 Disclaimer and liability

TDIF Req: ROLE-02-01-02; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have user terms, including:

a) The *Applicant* gives no express or implied warranties or makes any representation (and to the full extent permitted by law excludes all statutory warranties) in relation to any part of its identity system, including as to its or their availability, performance, security or fitness for a particular purpose and in respect of the availability, accuracy, completeness or correctness of any information.
b) To the extent permitted by law, the *Applicant* will not be liable to the *User* or any third party for any loss or damage arising from or in connection with the availability, use or performance of the identity system or any part of the identity system.

2.1.3 Third party service providers

TDIF Req: ROLE-02-01-03; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have user terms, including:

a) The *User's* access to the identity system may be facilitated by third party services or software and the provider may require, enable or facilitate access to third party services or software.
b) The *User* is responsible for complying with any terms of any such third-party service provider, including any other *Accredited Participant*.
c) To the extent permitted by law, the *Applicant* is not liable to the *User* for any damage or loss arising in connection with User's access to the service, either directly or through a third-party provider.

2.1.4 Intellectual Property and use of information

TDIF Req: ROLE-02-01-04; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have user terms, including:

a) All title, rights and interest in and to the intellectual property of the *Applicant*, including any modifications, corrections or enhancements thereto, will remain vested in the *Applicant*, in accordance with the *TDIF*.
b) The *User* is liable for breaches of intellectual property caused by the User's use of the service other than in accordance with the *TDIF*.
c) The *User* must not use, reproduce, amend or alter intellectual property rights in the service.
d) The user consents to the *Applicant* using their information as required by the *TDIF*, including to detect, manage and investigate fraud.
e) The *User* must comply with security requirements or instructions provided to it by the *Applicant*.

2.1.5 Fees and general terms

TDIF Req: ROLE-02-01-05; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* have user terms, including:

a) That the *Applicant* will not be responsible for any fees charged by any other *Accredited Participant* or a third-party provider used by the *User* to access the service.
b) The governing law of the user terms.
c) Provisions setting out a process for dispute resolution.
d) A whole of agreement provision (i.e. that the terms represent the entire agreement between the *User* and *Applicant*).
e) A severability provision.

TDIF Req: ROLE-02-01-06; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST NOT* have user terms that are inconsistent with the user terms required under the *TDIF*.

2.2 Operations Manual

TDIF Req: ROLE-02-02-01; **Updated**: Mar-20; **Applicability**: A, C, I, X
The *Applicant* *MUST* establish and maintain an *Operations Manual*.

TDIF Req: ROLE-02-02-01a; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Operations Manual* *MUST* include:

a) The roles and responsibilities of the *Applicant's Personnel*.
b) The processes, procedures and workflows used to support the *Applicant's* lifecycle management functions.
c) All interactions with *Accredited Participants*.

TDIF Req: ROLE-02-02-01b; **Updated**: Mar-20; **Applicability**: A, C, I, X

The *Applicant* *MUST* ensure that all information included in the *Operations Manual* is consistent with information included in its *Protective security documentation*.

3 Identity Service Provider Requirements

3.1 Identity proofing concepts

3.1.1 Identity Proofing Objectives

Identity Proofing refers to the process of collecting, verifying, and validating sufficient *Attributes* (and supporting evidence) about a specific *Individual* to confirm their *Identity*. *Relying Parties* and digital services require varying levels of confidence in a *Digital Identity* based on the consequence of incorrectly identifying an *Individual* in the provision of their services. To achieve this *Identity Service Providers* (*IdP*) undertake an *Identity Proofing* process that tests the veracity of claims. The veracity of claims about an *Individual's Identity* is established through evidence, i.e. *Evidence of Identity* (*EoI*), provided to meet some or all of the following five *Identity Proofing* objectives.

***Uniqueness Objective* - confirm uniqueness of the identity in the IdP context** to ensure that *Digital Identities* can be distinguished from one another in the *IdP* context and that the right service is delivered to the right *person*. This reduces risks such as doubling up on service provision[1]. This would include a check that another *Individual* has not previously claimed ownership of the *Identity* (i.e. there is a sole claimant), for example by checking the *IdP's* database for records with the same *Attributes*.

***Legitimacy Objective* - confirm the claimed identity is legitimate** to ensure the *Identity* has been genuinely created (i.e. the *Identity* is that of a real *person*) through evidence of *Commencement of Identity* (*CoI*) creation in Australia. Where greater confidence in the claimed *Identity* is required, this objective may also include a check that the *Identity* has not been recorded as deceased (through either internally or external sources, such as law enforcement agencies or comparing *Attributes* against a *Fact of Death File*).

This objective also includes a check that there is continuity in an *Individual's Attributes* where there have been changes. Increased confidence in the legitimacy of

[1] *Individuals* are legally allowed to operate in the community using different names. An *Individual* can use legitimate verifiable *Identity Documents* in one or more names which relate to them to create one or more legitimate *Digital Identities* at one or more *IdPs*.

an *Individual's Identity* is achieved through verifying *EoI documents* and verifying *Linking Documents* where name or date of birth details differ between different *EoI*. This reduces risks such as the registration of imposters or non-genuine identities.

***Operation Objective* - confirm the operation of the identity in the Australian community over time** to provide additional confidence that an *Individual's Identity* is legitimate in that it is being used in the Australian community (including online where appropriate). Even where a *person* can obtain genuine *Identity Documents* in a fictitious name, it will be harder to provide evidence that the identity has been active in the Australian community. Particularly over an extended period and if evidence reflects the breadth of an *Individual's* life, such as:

- Completing schooling, attending university or receiving support or services provided by government.
- Providing evidence that demonstrates the *person's* financial or working life.
- Providing evidence that demonstrates the *person's* family situation, where they live and what they consume.

***Binding Objective* - confirm the link between identity and the individual claiming the identity** to provide confidence that the *Individual's Identity* confirmed through the *Legitimacy Objective* and *Operation Objective* is not only legitimate, but that the *Individual* currently claiming the *Identity* is its legitimate holder. This has traditionally be done by comparing a *person's* face against a *Photo ID document*, although there is an increasing range of technologies and approaches that can provide alternative methods, such as comparison of a biometric captured during the *Identity Proofing* process against a biometric previously captured using an *Identity Matching Service*. The TDIF supports the use of *Biometric verification* to satisfy the *Binding Objective*.

***Fraud Control Objective* - confirm the identity is not known to be used fraudulently** to provide additional confidence that a fraudulent (either fictitious or stolen) identity is not being used. This could be through checks against internal registers of known fraudulent identities or against 'dummy biographical records' recorded in the *IdP's* identity system. This could include checks against information provided by external sources, such as law enforcement agencies.

3.1.2 Evidence of Identity

Evidence of Identity may be a physical or electronic *Identity Document* or non-documentary identity data held in a repository accessible by an *IdP*. *Evidence of Identity* can have widely varying strength in relation to the *Authoritative Source* and *Identity Document* security. In addition, there may be different *Attributes* contained within the evidence, including *Attributes*, document identifiers and contact information.

The TDIF supports four *EoI document* categories:

- **Commencement of Identity** is a government issued *Identity Document*:
  - Which anchors an *Individual's Identity* and provides evidence of its establishment or creation in Australia.
  - Which is the product of high integrity business processes which create and issue the *Identity Document* and manage it throughout its lifecycle.
  - With *Attributes* contained in or printed on the *Identity Document* able to be securely verified through an *Identity Matching Service*.
- **Linking document** is a government, or court issued *Identity Document*:
  - Which provides a link that shows the continuity of the claimed Identity where *Identity Attributes* have changed.
  - With Attributes contained in or printed on the *Identity Document* that can be verified through an *Identity Matching Service*.
- **Use in the Community (UitC)** is a verifiable *Identity Document* issued by a reliable source which:
  - Includes *Attributes* either contained in or printed on the *Identity Document*, or within a repository that provides reasonable confidence that they cannot be modified after the fact.
  - Can be used to confirm the activity or provide historical evidence of an *Identity* operating in the Australian community over time.
  - This check can review either physical *Identity Documents* or non-documentary identity data held in a repository accessible by an *IdP*, that provides a degree of confidence that the date has not been modified after the fact.
- **Photo ID** is an *Identity Document*:

- Which allows binding between the presented *Attributes* and the *Individual* claiming the *Identity*.
- Which allows *Visual Verification* or *Biometric verification* between the *Individual* and the *Photo ID*.
- Where the biometric image of the *individual* is securely contained in or printed on the *Identity Document*.
- Where high integrity business processes are followed when creating, issuing and managing the document throughout its lifecycle.
- In which the *Attributes* contained in or printed on the *Identity Document* are able to be securely verified through an *Identity Matching Service*.
- Where the image of the holder contained in or printed on the *Identity Document* can undergo *Biometric verification* through an *Identity Matching Service*, undergo *Technical Verification* or undergo *Visual Verification* by a trained operator.

3.1.3 Verification methods

Within the *Identity Proofing* process, the actions associated with checking the veracity of the claims about an *Individual's Identity* are heavily dependent on *EoI document* verification. Whilst verifying an *Identity Document* depends upon their format (physical or electronic), they can be checked using various methods which all have respective strengths and weaknesses. As such the *TDIF* supports three verification methods.

- ***Source Verification*** - the act of verifying physical or electronic *EoI* directly with the issuing body (or their representative, e.g. via an *Identity Matching Service*). *Source Verification* generally provides the most accurate, up to date information, however it may not be able to prove physical possession of a document (e.g. a licence number may be written down) and it may not have all the details of an original document (e.g. birth certificate information is often a summary of the original).
- ***Technical Verification*** – the act of verifying physical or electronic evidence using an *Australian Signals Directorate Approved Cryptographic Algorithm* bound to a secure chip or appended to it (e.g. via *Public Key Technology*). *Technical Verification* is generally very accurate but is dependent of the issuer's revocation

processes (e.g. a stolen passport yet to be revoked may still pass *Technical Verification*).

- ***Visual Verification*** - the act of a trained operator visually confirming, either electronically or in-*person*, that the *EoI* presented, with any security features, appears to be valid and unaltered, and/or making a facial comparison check. Generally, *Visual Verification* is less secure than *Source Verification* or *Technical Verification* as it introduces the possibility of operator error; however, it also allows for a more detailed human evaluation of the *Individual* and *Identity Document*.

These methods may be combined; for example, the details of a particular *Identity Document* may be able to *Source Verification*, however the photo on the document might require *Visual Verification*.

In all cases, regardless of verification method used, the *IdP* must be satisfied that a particular *Identity Document* can be reasonably and securely verified. This may mean rejecting an *Identity Document*, if for example, it is known that the associated database is compromised (invalidating *Source Verification*), or a cryptography protocol is broken (invalidating *Technical Verification*), or a particular document has few or no physical security features or is damaged (invalidating *Visual Verification*).

Appendix A: describes the approved *EoI documents* that an *IdP's* identity system may support and the verification methods that must be used by the *IdP* for each *EoI document* within the *Identity Proofing* process.

3.2 Identity Proofing Levels

The *TDIF's Identity Proofing Levels* are:

- **Identity Proofing Level 1** is used when no identity verification is needed or when a very low level of confidence in the claimed *Identity* is needed. This level supports self-asserted identity (I am who I say I am) or pseudonymous *Identity*. The intended use of *Identity Proofing Level 1* is for services where the risks of not undertaking identity verification will have a negligible consequence to the *Individual* or the service. For example, to pay a parking infringement or obtain a fishing licence.

- **Identity Proofing Level 1 Plus** is used when a low level of confidence in the claimed *Identity* is needed. This requires one *Identity Document* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 1 Plus* is for services where the risks of getting *identity* verification wrong will have minor consequences to the *Individual* or the service. For example, the provision of loyalty cards.
- **Identity Proofing Level 2** is used when a low-medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity*. The intended use of *Identity Proofing Level 2* is for services where the risks of getting identity verification wrong will have moderate consequences to the *Individual* or the service. For example, the provision of utility services. An *Identity Proofing Level 2* identity check is sometimes referred to as a "100-point check".
- **Identity Proofing Level 2 Plus** is used when a medium level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 2 Plus* is for services where the risks of getting identity verification wrong will have moderate-high consequences to the *Individual* or the service. For example, undertaking large financial transactions.
- **Identity Proofing Level 3** is used when a high level of confidence in the claimed *Identity* is needed. This requires two or more *Identity Documents* to verify someone's claim to an existing *Identity* and requires the *Binding Objective* to be met. The intended use of *Identity Proofing Level 3* is for services where the risks of getting identity verification wrong will have high consequences to the *Individual* or the service. For example, access to welfare and related government services.
- **Identity Proofing Level 4** is used when a very high level of confidence in the claimed *Identity* is needed. This requires four or more *Identity Documents* to verify someone's claim to an existing *Identity* and the *Individual* claiming the *Identity* must attend an in-person interview as well as meet the requirements of *Identity Proofing Level 3*. The intended use of *Identity Proofing Level 4* is for services where the risks of getting identity verification wrong will have a very high consequence to the *Individual* or the service. For example, the issuance of government-issued documents such as an Australian passport.

For each *Identity Proofing Level*, Table 1 below outlines the applicable *Identity Proofing* objectives, the *EoI* required and activities to be undertaken by the IdP.

TDIF Req: IDP-03-02-01; **Updated**: Mar-20; **Applicability**: I

At a minimum, the *Applicant's* identity system *MUST* support *Identity Proofing Level 1 Plus* as described in Table 1 below.

TDIF Req: IDP-03-02-02; **Updated**: Mar-20; **Applicability**: I

For each supported *Identity Proofing Level*, the *Applicant MUST* implement it as described in Table 1 below.

Table 1: Identity Proofing Levels

IP 1	***IP 1 Plus***	***IP 2***	***IP 2 Plus***	***IP 3***	***IP 4***
Uniqueness Objective - confirm uniqueness of the *Identity* in the *IdP* context					
Identifier chosen by the *Individual* is unique	Checks *MUST* be undertaken by the *IdP* to establish that the *Individual* is the sole claimant of the *Identity*. This *MAY* be through checking internal organisation records for *Identity* with the same *Attributes*.				
Legitimacy Objective - confirm the claimed *Identity* is legitimate					
Nil	The IdP *MUST* verify the Individual's name and date of birth, using *attributes* collected from either a *UITC Document* or a *Photo ID.*	Verification of a *Photo ID* or a *CoI document* MUST be undertaken by the *IdP*. An Australian Passport *MAY* be accepted as evidence of *CoI*. Verification of a *Linking document MUST* be undertaken by the *IdP* if *Attributes* vary across *EoI* documents.		Verification of a *CoI Document* and a *Photo ID MUST* be undertaken[2]. A check that the *Identity* is not that of a deceased *person MUST* also be undertaken by the *IdP*.	Verification of a *CoI Document* and a *Photo ID MUST* be undertaken. An Australian Passport *MUST NOT* be accepted as evidence of *CoI.* A check that the *Identity* is not that of a deceased *person MUST* also be undertaken by the *IdP*.
Operation Objective – confirm the operation of the *Identity* in the Australian community over time					
Nil	Nil	Verification of one *UitC document MUST* be undertaken by the *IdP*[3][4].			Verification of two *UitC documents MUST* be undertaken by the *IdP*.
Binding Objective – confirm the link between the *Identity* and the *Individual* claiming the *Identity*					

[2] An Australian Passport *MAY* be accepted as evidence as both CoI and Photo ID.

[3] To satisfy the *Operation Objective* at *Identity Proofing Level 1 Plus*, the *Individual's* name and date of birth *MUST* be verified.

[4] Which may include any UitC document or any document listed in another category. (See Appendix A, Table 7 for more information).

IP 1	***IP 1 Plus***	***IP 2***	***IP 2 Plus***	***IP 3***	***IP 4***
Nil	Nil	Nil	Verification of the link between the *Individual* and the claimed *Identity* <u>*MUST*</u> be undertaken. This <u>*MAY*</u> occur through either *Visual Verification* of one *Photo ID*, or *Biometric verification* using *Source Verification* or *Technical Verification*[5]. When a *Photo ID* is used it <u>*MUST*</u> be verified. The *Photo ID* <u>*MAY*</u> be the same document used to meet the legitimacy objective.		As per *IP 3* requirements, with the addition that original physical documents <u>*MUST*</u> also be provided in-*person*
Fraud Control Objective – confirm the *Identity* is not known to be used fraudulently					
Nil	Checks <u>*MUST*</u> be undertaken against information or records held within the *IdP*, such as checks against internal registers of known fraudulent identities or vulnerable identities. Checks <u>*MAY*</u> be undertaken against information on known fraudulent identities from other *Authoritative Sources*, such as law enforcement or other government agencies.				
Other requirements					
Nil	Nil	Documents in languages other than English <u>*MAY*</u> be accompanied by a *NAATI*[6] accredited translation		Documents in languages other than English <u>*MUST*</u> be accompanied by a NAATI accredited translation	
		Personnel involved in *Identity Proofing* processes <u>*MAY*</u> be provided with tools and training to detect fraudulent *Attributes* and *Identity Documents*, such as recognition of document security features, particularly for foreign document		*Personnel* involved in *Identity Proofing* processes <u>*MUST*</u> be provided with tools and training to detect fraudulent *Attributes* and *Identity Documents*, such as recognition of document security features, particularly for foreign documents.	

[5] Section 3.8 sets out requirements to confirm the link between the *Individual* and the Identity being claimed using *Biometric verification*.

[6] National Accreditation Authority for Translators and Interpreters. Further information is available at https://www.naati.com.au/

3.3 Individuals unable to meet Identity Proofing requirements

Although most *Individuals* should be able to meet the requirements set out in Table 1, in some cases *Individuals* may face genuine difficulty in providing the necessary *EoI documents* themselves to the required *Identity Proofing Level*. The *IdP* may develop alternative *Identity Proofing* processes for these exception cases.

Exception cases are those where an *Individual* does not possess, and is unable to obtain, the necessary information or *EoI documents* to the required *Identity Proofing Level*. This may include:

- *Individuals* whose birth was not registered.
- *Individuals* who are homeless or displaced.
- Undocumented arrivals to Australia.
- *Individuals* living in remote areas.
- *Individuals* who do not have enough *Identity Documents*, for example, foreign nationals living in Australia or Australians living in other countries.
- *Individuals* who do not have any *Identity Documents* but need a *Digital Identity*, for example, foreign nationals living outside Australia who need to access government systems or services.
- *Individuals* who are transgender or intersex.
- *Individuals* effected by natural disasters.
- *Individuals* with limited access to *Identity Documents*, for example, *Individuals* who were raised in institutional or foster care.
- *Individuals* with limited participation in society.
- Young people and those over 18 years who are yet to obtain *EoI documents*.

TDIF Req: IDP-03-03-01; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MAY* implement alternative *Identity Proofing* processes to the requirements set out in Table 1 to support exceptions cases.

TDIF Req: IDP-03-03-01a; **Updated**: Mar-20; **Applicability**: I
The alternative *Identity Proofing* processes *MAY* include:

- Acceptance of alternative types of *EoI* (for example, evidence of the operation of an *Identity* in a non-Australian community over time).
- Verification of an *Individual's* claimed *Identity* with a trusted referee whose *Identity* has been verified to an equal or greater *Identity Proofing Level*.
- Verification of an *Individual's* claimed *Identity* with reputable organisations or bodies known to them (for example, Aboriginal and Torres Strait Islander organisations may hold, or be able to verify, the *Identity* of *Individuals* where no prior government record exists).
- Reliance on the *Identity Proofing* processes of other organisations that have verified the *Identity* of the *Individual* (i.e. *Known Customer*)
- A detailed interview with the *Individual* about their life story to assess the consistency and legitimacy of their claims.
- Alternative methods of providing *Attributes* or *Identity Documents* (such as the provision of certified copies by trusted third parties instead of attending an in-person interview where an *Individual* can demonstrate they live in a very remote area).
- Providing support for *Individuals* to obtain evidence (such as assisting the *Individual* to register their birth with a *RBDM*)

TDIF Req: IDP-03-03-01b; **Updated**: Mar-20; **Applicability**: I
All alternative *Identity Proofing* processes an *Applicant* implements to support exceptions cases *MUST* be informed by a risk assessment. Evidence of these alternative processes and risk assessment will be requested by the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

3.4 Identity proofing lifecycle management

This section sets out the requirements for *Identity Proofing* lifecycle management activities undertaken by the *Applicant*. As part of this process the *Applicant* may collect *Personal information* from *Identity Documents* listed in Table 7 (**Appendix A**) with the *Individual's Consent*.
TDIF Req: IDP-03-04-01; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST* allow *Individuals* to update their *Attributes* held by the *Applicant*.

TDIF Req: IDP-03-04-01a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** verify updates to the *Individual's Identity* prior to making changes to the *Individual's Digital Identity*. This includes any status changes made to the *Individual's Digital Identity* (e.g. temporary suspension or reactivation).

TDIF Req: IDP-03-04-01b; **Updated**: Mar-20; **Applicability**: I
Where unusual transactions are detected the *Applicant* ***MUST*** verify the *Digital Identity* is still under the control of its legitimate account holder.

TDIF Req: IDP-03-04-02; **Updated**: Mar-20; **Applicability**: I
When requested to do so, the *Applicant* ***MUST*** prevent the continued use of a *Digital Identity* (e.g. temporary suspension while traveling abroad).

TDIF Req: IDP-03-04-02a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** confirm the legitimacy of any request by a *User* to prevent the continued use of their *Digital Identity* in accordance with IDP-03-04-02, prior to preventing the continued use of that *Digital Identity*.

TDIF Req: IDP-03-04-02b; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** notify the *User* that a *Digital Identity* can no longer be used in accordance with IDP-03-04-02 and the reason why it can no longer be used (e.g. deactivated, suspended, etc).

3.5 Identity proofing Step-Up

The requirements in this section only apply to an *Applicant* if their identity system supports *Step-Up* of *Identity P*roofing from one *Identity Proofing Level* to another. *Step-Up* is supported for all *Identity Proofing Levels*.

TDIF Req: IDP-03-05-01; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** achieve all the requirements of the higher *Identity Proofing Level*.

TDIF Req: IDP-03-05-02; **Updated**: Mar-20; **Applicability**: I
The *Applicant* ***MUST*** ensure that an *Individual* can prove ownership of their existing *Identity* by authenticating with their *Credential* to their account prior to commencing the *Identity Proofing Step-Up* process.

3.6 Attributes to be verified, validated and recorded

TDIF Req: IDP-03-06-01; **Updated**: Mar-20; **Applicability**: I

For each *EoI document* used, the *Applicant* MAY collect and verify, and create and record the *Attributes* listed in Table 2.

TDIF Req: IDP-03-06-02; **Updated**: Mar-20; **Applicability**: I

The *Applicant* MAY collect, validate and record the *Individual's* mobile phone number, email address, or both.

Table 2: *Attributes* to be collected, verified and recorded

Attributes to be verified and recorded	*Attributes* to be recorded
Identity attributes	
All verified names – family name(s), given name(s), surname(s), full name(s), previous name(s) as recorded on the *EoI document*	Date and time *Attributes* last updated (i.e. verified names and date of birth)
Verified date of birth as recorded on the *EoI document*	Date and time email address was last validated (if collected)
	Date and time mobile phone number was last validated (if collected)
EoI* document *attributes	
EoI document type name	Verification method used for each *EoI document* (i.e. S, T, V)
EoI document type code	Date and time the *EoI document* was verified
EoI document issuer	
EoI document identifier(s) (e.g. registration, document, licence, or card numbers)	
Card type (for Medicare Cards)	
Digital *identity attributes*	
	Identity Proofing Level achieved
	Date and time the *Digital Identity* was created
	Digital Identity (user identifier)

TDIF Req: IDP-03-06-03; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MAY* collect and record the *Attributes* listed on *EoI documents* as described in Table 3.

TDIF Req: IDP-03-06-04; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST NOT* collect, create, verify or record *Attributes* beyond that which is listed in Table 2 or Table 3.

Table 3: *Attributes* that may be collected and recorded

Attributes that may be collected and recorded
Preferred name(s)
Physical address

3.7 Attribute disclosure

TDIF Req: IDP-03-07-01; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MAY* disclose the *Attributes* listed in the "Attributes to be collected, verified and recorded" column of Table 2 and the *Attributes* listed in Table 3 for the purpose of having them verified (i.e. with the issuer of the associated *EoI document*).

TDIF Req: IDP-03-07-01a; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MUST NOT* disclose *Attributes* beyond those listed in IDP-03-07-01 for the purpose of having them verified.

TDIF Req: IDP-03-07-02; **Updated**: Mar-20; **Applicability**: I

The *Applicant* *MAY* disclose all of the following *Attributes*:

- Verified name(s).
- Verified date of birth.
- Validated contact details it collects.
- *Identity Proofing Level* achieved.
- Date and time the *Digital Identity* was created.

to a *Relying P*arty via an *Identity Exchange* or *Attribute Service Provider*).

TDIF Req: IDP-03-07-03; **Updated**: Feb-21; **Applicability**: I

The *Applicant* *MAY* seek permission from the *DTA* to request the sharing of more *Attributes* than those listed in TDIF req: IDP-03-07-02.

TDIF Req: IDP-03-07-03a; **Updated**: Mar-20; **Applicability**: I
The *Applicant* *MUST NOT* disclose *Attributes* beyond those listed in IDP-03-07-01 for the purpose of service delivery, unless approved by the *DTA* to do so.

3.8 Biometric verification requirements

This section sets out requirements to confirm the link between the *Individual* and the *Identity* being claimed using *Biometric verification.*

3.8.1 Requirements for online biometric binding

TDIF **Req:** IDP-03-08-01; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* restrict access to the control of any aspects of the Biometric Capability exclusively to *Assessing Officers* that have completed the appropriate training pertaining to the exercise of such control.

TDIF **Req:** IDP-03-08-02; **Updated**: Mar-2020; **Applicability**: I
To complete *Online Biometric binding* the *Applicant* *MUST* either:

- capture and send the *Acquired image* to the Photo ID Authoritative Source (or proxy) in the case of *source biometric matching*; or,
- capture and perform *document biometric matching* of the *Acquired Image* against the image read directly from the Photo ID RFID chip.

TDIF **Req:** IDP-03-08-03; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* incorporate *presentation attack detection* when performing *Online Biometric binding.*

TDIF **Req:** IDP-03-08-04; **Updated**: Mar-2020; **Applicability**: I
The *Applicant* *MUST* complete the image capture and *presentation attack detection* processes as part of the same process before submission to *Online Biometric binding*. This is to prevent attacks that would exploit the separation of the *presentation attack detection* and the image acquisition.

3.8.2 Requirements for presentation attack detection

***TDIF* Req:** IDP-03-08-05; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* employ *presentation attack* detection technology to determine if the *Acquired image* is of a living human subject present at the point of capture.

***TDIF* Req:** IDP-03-08-06; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* include liveness detection processes as part of *presentation attack* detection.

***TDIF* Req:** IDP-03-08-07; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* employ *presentation attack* detection technology that includes data capture and system level monitoring as described by ISO 30107-1.

***TDIF* Req:** IDP-03-08-08; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* ensure that the presentation attack detection technology meets the requirements of at least Evaluation Assurance Level 1 as described by ISO 30107-3.

***TDIF* Req:** IDP-03-08-08a; **Updated**: Mar-2020; **Applicability**: I

If the comprehensive risk assessment undertaken by the *Applicant* indicates that the *presentation attack detection* technology used in the capability must exceed these standards, the *Applicant* *MUST* meet the requirements described in the risk assessment.

***TDIF* Req:** IDP-03-08-09; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* capability *MUST* have been tested by a qualified third-party testing entity with experience in biometric testing and ISO 30107 to determine that the *presentation attack detection* technology meets the requirements for at least Evaluation Assurance Level 1 of ISO 30107-3.

***TDIF* Req:** IDP-03-08-09a; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* have determined *presentation attack detection* outcomes in a trusted computing environment.

***TDIF* Req:** IDP-03-08-09b; **Updated**: Mar-2020; **Applicability**: I

All testing performed *MUST* have been performed on a solution that incorporates all hardware and software involved in the *biometric binding* process including the *presentation attack detection* technology and *biometric matching*.

***TDIF* Req:** IDP-03-08-09c; **Updated**: Mar-2020; **Applicability**: I

Any determinations made by manual processes *MUST* be recorded separately to the *biometric matching* or *presentation attack detection* systems.

***TDIF* Req:** IDP-03-08-10; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* provide a report to the *DTA* as part of initial accreditation from the qualified third-party testing entity outlining that the *Applicant*'s *presentation attack detection* technology has been suitably tested to the specifications of at least Evaluation Assurance Level 1 of ISO 30107-3.

***TDIF* Req:** IDP-03-08-10a; **Updated**: Mar-2020; **Applicability**: I

The report *MUST* describe the completed *presentation attack detection* evaluation and corresponding results for each presentation attack type with the closest possible adherence to reporting specifications as described in ISO 30107-3.

***TDIF* Req:** IDP-03-08-10b; **Updated**: Mar-2020; **Applicability**: I

The report *MUST* be completed annually thereafter and provided to the *DTA* as part of the *Annual Assessment*.

3.8.3 Requirements for document biometric matching

***TDIF* Req:** IDP-03-08-11; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* verify the authenticity of the image read from the Photo ID RFID chip according to the Photo ID Issuing Authority instructions.

***TDIF* Req:** IDP-03-08-12; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* only process Claimed Photo ID through *document biometric matching* that contain a government issued and cryptographically signed image, such as an ePassport.

***TDIF* Req:** IDP-03-08-13; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* use a *biometric matching* algorithm to perform one-to-one verification matching between the *Acquired image* and the Photo ID image.

***TDIF* Req:** IDP-03-08-14; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST NOT* use a *biometric matching* algorithm to perform one-to-many matching against a database of reference images as part of the *biometric binding* process.

***TDIF* Req:** IDP-03-08-15; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* ensure their *biometric matching* algorithm is tested by a qualified third-party testing entity to determine the failure to enroll rate (if applicable), failure to acquire rate, false match rate and false non-match rate of the capability as per the reporting specification described in ISO 19795.

***TDIF* Req:** IDP-03-08-15a; **Updated**: Mar-2020; **Applicability**: I

This *MUST* be tested under production-like conditions.

***TDIF* Req:** IDP-03-08-15b; **Updated**: Mar-2020; **Applicability**: I

The minimum number of subjects for the testing *MUST* be 245, as described in FIDO Biometric Requirements.

***TDIF* Req:** IDP-03-08-15c; **Updated**: Mar-2020; **Applicability**: I

The testing *MUST* be performed in a verification scenario with comparable image types to production expectations.

***TDIF* Req:** IDP-03-08-16; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* achieve a false match rate equivalent to or lower than FIDO Biometric Requirements. This requires a false match rate of not more than 0.01% and a false non-match rate of not more than 3%.

***TDIF* Req:** IDP-03-08-016a; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* record *biometric matching* outcomes in a trusted computing environment.

3.8.4 Photo ID specific requirements

***TDIF* Req:** IDP-03-08-17; **Updated**: Mar-2020; **Applicability**: I

Where the Photo ID used has an RFID chip that is available and functional, the *Applicant* *MUST* perform a biometric match of the *Acquired image* only against the image read directly from the Photo ID RFID chip.

***TDIF* Req:** ID-03-09-17a; **Updated**: Mar-2020; **Applicability**: I

Where an RFID chip is not available, the Photo ID image used for *biometric matching* *MUST NOT* be from a scan of a physical document.

***TDIF* Req:** IDP-03-08-18; **Updated**: Mar-2020; **Applicability**: I

Where the Photo ID used is an Australian ePassport, the *Applicant* *MUST* check the Country Signing Certification Authority (CSCA) Certificate as per ICAO document validation guidelines OR perform a DVS check. Where the Australian ePassport security certificate is checked, the Australian Certificate Revocation List must also be checked.

***TDIF* Req:** IDP-03-08-18a; **Updated**: Mar-2020; **Applicability**: I

Where an RFID chip is not available, non-functional or the document security is lower than that of the Australian ePassport, a DVS check *MUST* be performed by the *Applicant*.

***TDIF* Req:** IDP-03-08-18b; **Updated**: Mar-2020; **Applicability**: I

A DVS check *MUST* be performed by the *Applicant* where the Photo ID used is a foreign ePassport to ensure that the foreign ePassport is linked to a current visa.

***TDIF* Req:** IDP-03-08-18c; **Updated**: Mar-2020; **Applicability**: I

Where the Photo ID used is a foreign ePassport and an RFID chip is not available or non-functional the *Applicant* *MUST* attempt to perform a biometric match against the corresponding image recorded against that identity from the Photo ID Authoritative Source.

***TDIF* Req:** IDP-03-08-18d; **Updated**: Mar-2020; **Applicability**: I

Where the Photo ID used is a foreign ePassport and an RFID chip is not available or non-functional and the corresponding image recorded against that identity from the Photo ID Authoritative Source is unavailable, the *Applicant* *MUST* perform Local *Biometric binding*.

3.8.5 Image quality specific requirements

***TDIF* Req:** IDP-03-08-19; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* produce an *Acquired image* quality profile informed by the properties and characteristics described by ISO 29794-5 which details a set of minimum standards that the *Acquired image* must meet before *biometric matching*.

***TDIF* Req:** IDP-03-08-20; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* include automated quality controls and appropriate user-interface instructions that directs Users to provide an image that meets the *Acquired image* quality profile.

3.8.6 Requirements for Local Biometric Binding

***TDIF* Req:** IDP-03-08-21; **Updated**: Mar-2021; **Applicability**: I

The *Applicant* *MAY* perform source *biometric matching* to supplement *Manual Face Comparison* by performing a biometric match against the corresponding image recorded against that identity from the *Photo ID Authoritative Source.*

***TDIF* Req:** IDP-03-08-22; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* perform a DVS check as part of the Local *Biometric binding* process to confirm the authenticity of a Photo ID.

***TDIF* Req:** IDP-03-08-23; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* train relevant Assessing Officer's on Manual Face Comparison techniques including, but not limited to:

- Techniques for *Individual* feature comparison
- Awareness of racial and cognitive biases
- Presentation attack indicators
- Guided matching examples

The training material *MUST* be provided by the *Applicant* to the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

3.8.7 Requirements for logging and data retention

***TDIF* Req:** IDP-03-08-24; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* maintain the information associated with each *Individual* transaction, including a log of activities that details which Assessing Officer collected data, what data was collected, when and where the data was collected.

***TDIF* Req:** IDP-03-08-24a; **Updated**: Mar-2020; **Applicability**: I

This log *MUST NOT* include Biometric Samples.

***TDIF* Req:** IDP-03-08-25; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* have in place audit or random checking procedures to help detect fraud or inadequate Manual Face Comparison and verification by *Assessing Officers*.

***TDIF* Req:** IDP-03-08-26; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST NOT* retain any Personally Identifiable Information captured in *biometric binding* processes.

***TDIF* Req:** IDP-03-08-27; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* ensure that it is responsible for the destruction of all Biometric Samples, including all copies, caches, and intermediary databases, including any subcontractors or third-party components.

***TDIF* Req:** IDP-03-08-27a; **Updated**: Mar-2020; **Applicability**: I

This destruction process *MUST* be documented by a specific audit log.

***TDIF* Req:** IDP-03-08-27b; **Updated**: Mar-2020; **Applicability**: I

The *Acquired image* *MUST*, unless required by law, then be destroyed consistent with *TDIF* Req: PRIV-03-08-02.

3.8.8 Manual Face Comparison specific requirements

***TDIF* Req:** IDP-03-08-28; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MAY* utilise manual processors performed by *Assessing Officers* to complete Local *Biometric binding* or Online *Biometric binding* processes.

***TDIF* Req:** IDP-03-08-29; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MAY* utilize manual processors to review and/or adjust decisions made by the *Applicant* Capability, including biometric match results and *presentation attack detection*.

***TDIF* Req:** IDP-03-08-30; **Updated**: Mar-2020; **Applicability**: I

The *Acquired image* *MUST NOT* be retained after completion of the *Local Biometric Binding* or Online *Biometric binding* processes by the Assessing Officer.

***TDIF* Req:** IDP-03-08-31; **Updated**: Mar-2020; **Applicability**: I

If the *Applicant* utilises any manual processes, The *Applicant* *MUST* include this in their risk assessment for *biometric binding* processes.

***TDIF* Req:** IDP-03-08-32; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* maintain an audit log of manual processes that meets the requirements of the *TDIF*. This includes records of transactions in production and the training activities of *Assessing Officers*. The audit log *MUST* be auditable by the *DTA*.

***TDIF* Req:** IDP-03-08-33; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* only perform remote Manual Face Comparison for Online *Biometric binding* after attempting a Biometric Match.

***TDIF* Req:** IDP-03-08-34; **Updated**: Mar-2020; **Applicability**: I

The *Applicant* *MUST* only undertake remote Manual Face Comparison utilizing *Assessing Officers* located within Australia.

4 Credential Service Provider Requirements

These *credential service provider* requirements incorporate the National Institute of Standards and Technology (*NIST*), Special Publication (*SP*) 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management[7] (*NIST SP* 800-63B).

*Applicant*s that undergo the *TDIF Accreditation Process* should note the following:

- 'SHALL' and '*MAY*' statements in *NIST* should be read to mean to '*MUST'* and '*MAY'* statements in the *TDIF*, respectively. 'SHOULD' statements in *NIST* should also be read as '*MAY'* statements in the *TDIF*.
- *NIST* Authenticator Assurance Levels (AAL) should be read as *TDIF Credential Level* (*CL*).
- *NIST* 'authenticator' requirements should be read as *TDIF* credential requirements.
- And time Records management requirements in *NIST* 800-63B are subject to applicable Australian laws, regulations and policies including those set out in the Archives Act 1983 (Cth).
- All requirements in *NIST* 800-63B are subject to the requirements set out in *TDIF: 04 - Functional Requirements*.
- The permissible combinations of *Identity Proofing* and *Credential Levels* is described in Table 4 below.

Table 4: Permissible combinations of IPs and CLs.

Permissible combinations		*Credential Level*		
		CL 1	*CL 2*	*CL 3*
Identity Proofing Level	*IP 1* *IP 1 Plus*	Allowed	Allowed	Allowed
	IP 2 *IP 2 Plus*	Not Allowed	Allowed	Allowed
	IP 3	Not Allowed	Allowed	Allowed
	IP 4	Not Allowed	Not Allowed	Allowed

[7] A copy of NIST 800-63B is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

4.1 Credential Levels

TDIF Req: CSP-04-01-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* support at least one approved *Credential* at a *Credential Level* as described in Table 4.

TDIF Req: CSP-04-01-02; **Updated**: Mar-20; **Applicability**: C

For each supported *Credential Level*, the *Applicant* *MUST* implement it to meet all requirements as described in Table 5.

Table 5: Credential Levels

Requirement	*CL 1*	*CL 2*	*CL 3*
Permitted authenticator types	Refer to *NIST* SP-800-63B in relation to approved *Credentials* and applicable requirements.		
Man-in-the-Middle resistance	Required	Required	Required
Verifier-impersonation resistance	Not required	Not required	Required
Verifier-compromise resistance	Not required	Not required	Required
Replay resistance	Not required	Required	Required
Authentication intent	Not required	Not required	Required

4.1.1 Credential Lifecycle Management

TDIF Req: CSP-04-01-03; **Updated:** Mar-20; **Applicability:** C

The *Applicant* *MUST* ensure that *Credentials* presented are valid or active and that they are not expired or revoked prior to authenticating the *Individual*.

TDIF Req: CSP-04-01-04; **Updated**: Mar-20; **Applicability**: C

Where unusual transactions are detected the *Applicant* *MUST* verify the *Credential* is still under the control of its legitimate owner.

TDIF Req: CSP-04-01-05; **Updated**: Mar-20; **Applicability**: C
When requested by its legitimate owner the *Applicant* *MUST* prevent the continued use of a *Credential* (e.g. temporary suspension while traveling abroad).

TDIF Req: CSP-04-01-05a; **Updated**: Mar-20; **Applicability**: C
The *Applicant* *MUST* confirm the legitimacy of the request in accordance with CSP-04-01-05, prior to preventing the continued use of a *Credential*.

TDIF Req: CSP-04-01-05b; **Updated**: Mar-20; **Applicability**: C
The *Applicant* *MUST* notify the *Individual* that a *Credential* can no longer be used in accordance with CSP-04-01-05 and the reason why it can no longer be used (e.g. deactivated, expired, revoked, etc).

4.2 Credential and verifier requirements

4.2.1 Memorised secret

TDIF Req: CSP-04-02-01; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement a “memorised secret” as set out in Section 5.1.1 of *NIST* SP 800-63B.

4.2.2 Look-up secret

TDIF Req: CSP-04-02-02; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement a “*look-up secret*” as set out in Section 5.1.2 of *NIST* SP 800-63B.

4.2.3 Out-of-band device

TDIF Req: CSP-04-02-03; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement an “*out-of-band device*” as set out in Section 5.1.3 of *NIST* SP 800-63B.

4.2.4 Single-factor One-Time Password device

TDIF Req: CSP-04-02-04; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement a "*SF OTP device*" as set out in Section 5.1.4 of *NIST* SP 800-63B.

4.2.5 Multi-factor One-Time device

TDIF Req: CSP-04-02-05; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement a "*MF OTP device*" as set out in Section 5.1.5 of *NIST* SP 800-63B.

4.2.6 Single-factor cryptographic software

TDIF Req: CSP-04-02-06; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement "*SF* crypto software" as set out in Section 5.1.6 of *NIST* SP 800-63B.

4.2.7 Single-factor cryptographic device

TDIF Req: CSP-04-02-07; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement "*SF* crypto device" as set out in Section 5.1.7 of *NIST* SP 800-63B.

4.2.8 Multi-factor cryptographic software

TDIF Req: CSP-04-02-08; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement "*MF* crypto software" as set out in Section 5.1.8 of *NIST* SP 800-63B.

4.2.9 Multi-factor cryptographic device

TDIF Req: CSP-04-02-09; **Updated**: Mar-20; **Applicability**: C
If supported, the *Applicant* *MUST* implement "*MF* crypto device" as set out in Section 5.1.9 of *NIST* SP 800-63B.

4.3 General credential requirements

4.3.1 Physical credentials

TDIF Req: CSP-04-03-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “physical authenticators” as set out in Section 5.2.1 of *NIST* SP 800-63B.

4.3.2 Rate limiting (throttling)

TDIF Req: CSP-04-03-02; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “rate limiting (throttling)” as set out in Section 5.2.2 of *NIST* SP 800-63B.

4.3.3 biometrics (for authentication use)

TDIF Req: CSP-04-03-03; **Updated**: Mar-20; **Applicability**: C

If biometrics are used for *authentication*, the *Applicant* *MUST* implement “biometrics (for *authentication* use)” as set out in Section 5.2.3 of *NIST* SP 800-63B.

4.3.4 Attestation

TDIF Req: CSP-04-03-04; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “*attestation*” as set out in Section 5.2.4 of *NIST* SP 800-63B.

4.3.5 Verifier-impersonation resistance

TDIF Req: CSP-04-03-05; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “*verifier-impersonation resistance*” as set out in Section 5.2.5 of *NIST* SP 800-63B.

4.3.6 Verifier-CSP communications

TDIF Req: CSP-04-03-06; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “*verifier-CSP communications*” as set out in Section 5.2.6 of *NIST* SP 800-63B.

4.3.7 Verifier-compromise resistance

TDIF Req: CSP-04-03-07; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "*verifier-compromise resistance*" as set out in Section 5.2.7 of *NIST* SP 800-63B.

4.3.8 Replay resistance

TDIF Req: CSP-04-03-08; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "*replay resistance*" as set out in Section 5.2.8 of *NIST* SP 800-63B.

4.3.9 Authentication intent

TDIF Req: CSP-04-03-09; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "*authentication* intent" as set out in Section 5.2.9 of *NIST* SP 800-63B.

4.3.10 Restricted Credentials

TDIF Req: CSP-04-03-10; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "restricted authenticators" as set out in Section 5.2.10 of *NIST* SP 800-63B.

4.4 Credential lifecycle management

4.4.1 Credential binding

TDIF Req: CSP-04-04-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "authenticator binding" as set out in Section 6.1 of *NIST* SP 800-63B.

4.4.2 Binding at enrolment

TDIF Req: CSP-04-04-02; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "binding at enrolment" as set out in Section 6.1.1 of *NIST* SP 800-63B.

4.4.3 Post-enrolment binding

TDIF Req: CSP-04-04-03; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MAY* implement “binding of an additional authenticator at existing AAL” as set out in Section 6.1.2.1 of *NIST* SP 800-63B.

TDIF Req: CSP-04-04-04; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MAY* implement “adding an additional factor to a single-factor account” as set out in Section 6.1.2.2 of *NIST* SP 800-63B.

TDIF Req: CSP-04-04-05; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “replacement of a lost *authentication* factor” as set out in Section 6.1.2.3 of *NIST* SP 800-63B.

4.4.4 Binding to a User-provided credential

TDIF Req: CSP-04-04-06; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “binding to a subscriber-provided authenticator” as set out in Section 6.1.3 of *NIST* SP 800-63B.

4.4.5 Renewal

TDIF Req: CSP-04-04-07; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “renewal” as set out in Section 6.1.4 of *NIST* SP 800-63B.

4.5 Loss, theft, damage and unauthorised duplication

TDIF Req: CSP-04-05-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “loss, theft, damage and unauthorised duplication” as set out in Section 6.2 of *NIST* SP 800-63B.

4.6 Expiration

TDIF Req: CSP-04-06-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement “expiration” as set out in Section 6.3 of *NIST* SP 800-63B.

4.7 Revocation and termination

TDIF Req: CSP-04-07-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "revocation and termination" as set out in Section 6.4 of *NIST* SP 800-63B.

4.8 Session management

4.8.1 Session bindings

TDIF Req: CSP-04-08-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MAY* "start a session in response to an *authentication* event" as described in Section 7 of *NIST* SP 800-63B.

TDIF Req: CSP-04-08-02; **Updated**: Mar-20; **Applicability**: C

If the *Applicant* starts a session they *MUST* implement "session bindings" as set out in Section 7.1 of *NIST* SP 800-63B.

4.8.2 Browser cookies

TDIF Req: CSP-04-08-03; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MAY* implement "browser cookies" as set out in Section 7.1.1 of *NIST* SP 800-63B.

4.8.3 Access tokens

TDIF Req: CSP-04-08-04; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "*access tokens*" as set out in Section 7.1.2 of *NIST* SP 800-63B.

4.8.4 Device identification

TDIF Req: CSP-04-08-05; **Updated**: Mar-20; **Applicability**: C

The *Applicant* *MUST* implement "*device identification*" as set out in Section 7.1.3 of *NIST* SP 800-63B.

4.9 Reauthentication

TDIF Req: CSP-04-09-01; **Updated**: Mar-20; **Applicability**: C
The *Applicant MUST* implement “reauthentication” as set out in Section 7.2 of *NIST* SP 800-63B.

4.10 Credential Step-Up

The requirements in this section only apply to an *Applicant* if its identity system supports *Step-Up* of a *Credential* from one *Credential Level* to another. *Step-Up* is supported for all *Credential Levels*.

TDIF Req: CSP-04-10-01; **Updated**: Mar-20; **Applicability**: C

The *Applicant MUST* achieve all the requirements of the higher *Credential Level.*

TDIF Req: CSP-04-10-02; **Updated**: Mar-20; **Applicability**: C
The *Applicant MUST* ensure that an *Individual* can prove ownership of their existing *Identity* by authenticating with their *Credential* to their account prior to commencing the *Credential Step-Up* process.

5 Attribute Service Provider Requirements

5.1 Attribute Classes

TDIF Req: ASP-05-01-01; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MUST* support at least one *Attribute Class* as described in Table 6.

Table 6: *Attribute* Classes

Attribute Class	Description
Authorisation	An *Individual* gives a permission, delegation or privilege for someone to act on their behalf. (e.g. an *Individual* authorised to act on behalf of their children when applying for a government service).
Qualification	A statement of attainment by an education or training organization consistent with the *AQF*[8] (e.g. a bachelor's degree from an Australian university).
Entitlement	Meeting a set of conditions which enables a *Individual* to have a right to something (e.g. an *Individual* is a resident of an Australian state or territory aged over 60 years and not working more than a set number of hours per week is entitled to a Seniors Card).
Self-Asserted	Unverified *Attributes* provided by an *Individual* that can assist with service delivery, such as prefilling online forms. This *Attribute Class* can be used for 'Tell Us Once' services.
Platform	*Attributes* which uniquely identify platforms and ICT systems that connect into the *Australian Government's identity federation*. For example, MyGov.

TDIF Req: ASP-05-01-02; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MAY* directly connect to an *Identity Service Provider*.

TDIF Req: ASP-05-01-03; **Updated**: Mar-20; **Applicability**: A, I

Beyond the minimum dataset required to associate *Identity Attributes* with *Attributes* related to *Attribute Classes*, the *Applicant* *MUST NOT* store *Attributes* held by an *Identity Service Provider* and *Attribute Service Provider* together in the one repository.

[8] Australian Qualifications Framework. Further information is available at https://www.aqf.edu.au/

5.2 General requirements

TDIF Req: ASP-05-02-01; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MUST* either be an *Authoritative Source* for *Attributes* it issues or have approval from the *Authoritative Source* to manage *Attributes* on their behalf.

TDIF Req: ASP-05-02-01a; **Updated**: Mar-20; **Applicability**: A
Where the *Applicant* manages *Attributes* on behalf of an *Authoritative Source*, it *MUST* provide evidence of this arrangement to the *DTA*. Evidence of this arrangement will be requested by the *DTA* as part of initial accreditation and annually thereafter as part of the *Annual Assessment*.

TDIF Req: ASP-05-02-02; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MUST* ensure every *Attribute* it issues or manages is uniquely identifiable.

TDIF Req: ASP-05-02-03; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MUST* manage and provide up-to-date, relevant and accurate *Attributes*.

TDIF Req: ASP-05-02-04; **Updated**: Mar-20; **Applicability**: A
If the *Applicant* is an *Authoritative Source* for an *Attribute*, the *Applicant* *MUST* verify all requests to update relevant *Attributes* prior to making changes.

TDIF Req: ASP-05-02-05; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MUST* take reasonable measures to prevent the continued use of an *Attribute* (e.g. suspension, deactivation) when requested to do so by an authorised *Individual* or *Authoritative Source*.

TDIF Req: ASP-05-02-05a; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MUST* confirm the legitimacy of the request from an authorised *Individual* or *Authoritative Source* in accordance with ASP-05-02-05, prior to actioning the request.

TDIF Req: ASP-05-02-06; **Updated**: Mar-20; **Applicability**: A
The *Applicant* *MAY* support issuing or linking multiple *Attributes* and *Attribute Classes* to a *Person*.

TDIF Req: ASP-05-02-06a; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MAY* support issuing or linking multiple *Attributes* relating to the same entity to a *Person*.

TDIF Req: ASP-05-02-06b; **Updated**: Mar-20; **Applicability**: A

The *Applicant* *MAY* support issuing or linking multiple *People* to the same *Attribute*.

Appendix A : Evidence types and verification methods

This Appendix sets out the *EoI document* types and the verification methods that an *Applicant* may support to confirm a claimed *Identity* is *legitimate* (*Legitimacy Objective*), confirm the operation of the *Identity* in the Australian community over time (*Operation Objective*), and confirm the link between the *Individual* and the *Identity* being claimed (*Binding Objective*).

Table 7 lists the *EoI document* types and the verification methods that an *Applicant* may support. *EoI document* types and verification methods may need to change in the future as *Applicants* update *Identity Proofing* processes, security practices and the methods of provision.

Table 7: Evidence types and verification methods

Type of Evidence	Notes	Verification method
Legitimacy Objective - confirm the claimed *Identity* is legitimate		
Commencement of Identity documents		
Australian birth certificate[9]	Issued by an Australian State or Territory Government Register of Births, Deaths and Marriages.	Source Visual
Australian Passport	Issued in the *individual's* name or former name, within 3 years of the expiry date.	Source Technical Visual
Australian citizenship certificate	Issued in the *individual's* name or former name. If their name appears on their parents' certificate, they can use that.	Source Visual
Foreign Passport	A current passport issued by another country, with a valid entry stamp or visa.	Source Technical Visual

[9] Although an Australia Passport in not evidence of *Commencement of Identity* in Australia, it can be used as proxy at *IP 2, IP 2 Plus* and *IP 3,* but not for *IP 4*. Use of the Australian Passport to provide evidence of *Commencement of Identity* should be considered on a risk management basis. Australian Passports are generally valid for 10 years and so will not always reflect changes of name. By contrast, many *RBDMs* are now updating birth records where a change of name has occurred and issuing a new certificate. This would mean that old birth records in the previous name could not be electronically verified.

Type of Evidence	Notes	Verification method
DFAT issued Certificate of Identity	Issued in the *individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual
DFAT issued Document of Identity	Issued in the *individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual
Immicard	A card issued in the *individual's* name or former name by the Department of Home Affairs.	Source Visual
Aboriginal and/or Torres Strait Islander descent records	This includes proof of Aboriginal and/or Torres Strait Islander heritage	Visual
Linking documents		
Australian marriage certificate	Issued by an Australian State or Territory Government	Source Visual
Change of Name Certificate	Legal change of name or deed poll certificate.	Source Visual
Australian divorce papers	In your name or former name. For example, a Decree Nisi or Decree Absolute.	Visual
Commonwealth victims certificate	Issued by a magistrate in Issued by an Australian State or Territory Government.	Visual
Australian birth certificate	Issued by a State or Territory Government Register of Births, Deaths and Marriages.	Visual
Operation Objective – confirm the operation of the *Identity* in the Australian community over time		
Use in the Community documents		
DHS Concession card	Issued by Services Australia.	Source Visual
Medicare Card	Issued by Services Australia.	Source Visual
Student ID card	A current student ID card issued by an Australian secondary school, TAFE, university or Registered Training Organisation which includes the *Individual's* name and may also include their photo.	Visual
Bank or financial institution card, passbook, statement	Issued by a bank, credit union or building society. Card statements or passbooks must cover at least 6 months of financial	Source Visual

Type of Evidence	Notes	Verification method
	transactions and be in the *Individual's* name. The *Individual's* signature must be on the card and their current address on the statement or passbook. Documents from foreign banks or institutions are not accepted.	
Education certificate or certified academic transcript.	Issued by an Australian secondary school, TAFE, university or Registered Training Organisation which includes the *Individual's* name or former name.	Source Visual
Mortgage papers	For an Australian property in the name of the *Individual* or their former name. These need to be legally drawn.	Visual
Veterans Affairs card	A current card issued in the *Individual's* name.	Visual
Tenancy agreement or lease	A current formal agreement or lease in the *Individual's* name showing their address.	Visual
Motor vehicle registration	Current registration papers with the *Individual's* name, address and proof of payment.	Source Visual
Rates notice	A paid rates notice issued in the *Individual's* name with their address that is less than 12 months old.	Visual
Electoral enrolment	Proof of electoral enrolment in the *Individual's* name and showing their current address.	Source Visual
Postal Records	A history of at least 6 months of postal deliveries.	Source Visual
Telephone Records	Records showing 6 months of phone usage.	Source Visual
Any document listed in another category	If not used elsewhere.	Source Technical Visual
Utility account	Issued in the *Individual's* name, with their address, that is less than 6 months old.	Visual
Superannuation statement	Issued in the *Individual's* name, with their address, that is less than 6 months old.	Visual
Seniors card	Issued in the *Individual's* name.	Visual
Land titles office records	Issued in the *Individual's* name.	Visual
Insurance renewal	Current insurance renewal for house and contents, vehicle, boat, or similar insurance in	Source Visual

Type of Evidence	Notes	Verification method
	the *Individual's* name held for over 12 months.	
Binding Objective – confirm the link between the *Identity* and the *Individual* claiming the *Identity*		
Photo ID documents		
Australian Passport	Issued in the *Individual's* name or former name, within 3 years of the expiry date.	Source Technical Visual
Australian State or Territory issued Drivers licence includes a digital Drivers licence)	A current licence issued by an Australian State or Territory Government in the *Individual's* name with their photo. For digital Drivers licence the security features must be tested to ensure authenticity.	Source Technical Visual
Foreign passport	A current passport issued by another country, with a valid entry stamp or visa.	Source Technical Visual
Foreign military ID card	An identification card issued in the name of an *Individual's* by a foreign government showing a picture of the *Individual* and identifying the *Individual* as a current member of the defence forces of that government	Visual
Titre de Voyage/ *DFAT* issued UN Travel documents	Issued in the *Individual's* name or former name by the Department of Foreign Affairs and Trade.	Source Visual
Australian citizenship certificate	Issued in the *Individual's* name or former name by the Department of Foreign Affairs and Trade.[10]	Source
Indigenous Community Card[11]	*EoI* used to provide confirmation of identity for Aboriginal or Torres Strait Islanders who have not provided other *Identity Documents*.	Visual
Shooter or firearm licence	A current card issued in the *Individual's* name and includes their photo.	Visual
Aviation Security Identity Card	A current card issued in the *Individual's* name and includes their photo.	Visual

[10] NB. Citizenship certificate may not have an actual photo embedded, but an associated photo is stored in the source environment.

[11] The *IDP* must satisfy itself that the quality of the card and card issuance process is sufficient to support its use as a Ph*oto ID document*.

Type of Evidence	Notes	Verification method
Maritime Security Identity Card	A current card issued in the *Individual's* name and includes their photo.	Visual
Australian Government issued photo ID card (employee ID)	A Photo ID card issued by the Commonwealth, or an Australian State or Territory Government issued in the *Individual's* name and includes their photo. The card may include a validity period.	Visual
Australian Department of Defence Highly Trusted Token	A current card issued in the *Individual's* name and includes their photo.	Technical Visual
Defence Force identity card	Issued by the Australian Defence Force and shows the *Individual's* name and photo.	Visual
Police identity card	A current card issued in the *Individual's* name and includes their photo.	Visual
Australian State or Territory issued trade (work or business) licence	A current card issued in the *Individual's* name and includes their photo (e.g. trade licences, real estate agents, security agents etc.)	Visual
Tangentyere Community ID card	A current card issued in the *Individual's* name and includes their photo.	Visual
Proof-of-Age card[12]	Issued by an Australian State or Territory Government in the *Individual's* name and includes their photo.	Visual
Australia Post Keypass	A current card issued in the *Individual's* name and includes their photo.	Source Visual
Working with children/Vulnerable card	A current card issued in the *Individual's* name and includes their photo.	Source Visual

[12] NB. State names vary but they have the same fundamental intent e.g. NSW/WA Photo Card, ACT Proof of Identity, Qld Adult Proof of Age, TAS Personal Information, NT Evidence of Age, VIC/SA Proof of Age.