List of tables

3 Identity Service Provider Requirements

3.1 Identity proofing concepts

Identity proofing concepts, descriptions and guidance is available in *TDIF 05A Role Guidance*.

The list of approved *Evidence of Identity (EoI) documents* that an *Identity Service Provider'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 are set out in Appendix A.

Descriptions of the *Identity Proofing Levels* are available in *TDIF: 05A Role Guidance*.

All Identity Proofing lifecycle management operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-12a). These requirements can be found in *TDIF 04 Functional Requirements*.

3.2 Identity Proofing

TDIF Req: IDP-03-02-01; **Updated**: Jun-21; **Applicability**: I
At a minimum, the *Applicant* *MUST* operate a TDIF accredited *Identity System* at *Identity Proofing level 1 Plus* as described in Table 1 below[1].

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.

[1] This does not prevent an IdP from supporting IP1. Rather, TDIF accreditation will not be supported for Applicants that can only meet IP1 requirements.

Table 1: Identity Proofing Levels

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Intended use:	For very low-risk transactions where no verification of identity is required, but the parties desire a continuing conversation	For low-risk transactions or services where fraud will have minor consequences for the service or *User*	For moderate-risk transactions or services where fraud will have moderate consequences for the service or *User*	For moderate to high-risk transactions or services where fraud will have moderate to high consequences for the service or *User*	For high-risk transactions or services where fraud will have high consequences for the service or *User*	For very high-risk transactions or services where major consequences arise from fraudulent verifications.
***Identity Proofing* objectives**[2]	Claimed identity meets: • Uniqueness	Claimed identity meets: • Uniqueness • Legitimacy • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control	Claimed identity meets: • Uniqueness • Legitimacy • Operation • Binding • Fraud Control
Uniqueness Objective						
***Identifier* chosen by the *Individual* is unique**	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
A check undertaken by the *IdP* to establish that the *Individual* is the sole claimant of the *Identity*[3]	-	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
Legitimacy Objective						
A check undertaken by the *IdP* that the *identity* is not that of a deceased person	-	*MAY*	*MAY*	*MAY*	*MUST*	*MUST*

[2] See *TDIF 05A Role Guidance* for full descriptions of each proofing objective.

[3] This *MAY* be done through checking internal organisation records for an *Identity* with the same *Attributes*.

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Binding Objective						
A check undertaken to confirm the link between the *individual* and the claimed *identity*[4]	-	-	-	*MUST*	*MUST*	*MUST*
The original, physical *EoI* documents to be provided in-person.	-	-	-	-	-	*MUST*
In person interview required to satisfy the *Binding Objective*	-	-	-	-	-	*MUST*
Fraud Control Objective						
Checks to be undertaken against information or records held within the *IdP*[5] to confirm the *identity* is not known to be used fraudulently.	-	*MUST*	*MUST*	*MUST*	*MUST*	*MUST*
Checks to be undertaken against information on known fraudulent identities from other *Authoritative Sources*[6]	-	*MAY*	*MAY*	*MAY*	*MAY*	*MAY*
Other Requirements						
***Personnel* performing *Identity Proofing* processes required to be provided with tools and training to detect fraudulent *Attributes* and *Identity Documents*[7]**	-	-	*MAY*	*MAY*	*MUST*	*MUST*
***NAATI* accredited translation of identity documents in languages other than English required?[8]**	-	-	*MAY*	*MAY*	*MUST*	*MUST*

[4] Verification of the link between the individual and the identity to occur through biometric verification in accordance with the requirements set out in Section 3.8.

[5] Such as checks against internal registers of known fraudulent identities or vulnerable identities

[6] Such as law enforcement or other government agencies.

[7] Such as recognition of document security features, particularly for foreign documents.

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

Requirements	IP1	IP1 Plus	IP2	IP2 Plus	IP3	IP4
Attributes that MUST be verified with an Authoritative Source or checked against evidence:[9]	-	All names Date of Birth	All names Date of Birth	All names Date of Birth	All names Date of Birth	All names Date of Birth
Documents required for Verification	**IP1**	**IP1 Plus**	**IP2**	**IP2 Plus**	**IP3**	**IP4**
Verification of a *CoI document MUST* be undertaken?	-	-	Yes or *Photo ID* (see below)	Yes or *Photo ID* (see below)	Yes[10]	Yes[10]
Verification of a *Photo ID MUST* be undertaken?	-	Yes or UiTC (see below)[11]	Yes or CoI (see above)	Yes or CoI (see above)	Yes	Yes
Verification of a *UiTC document MUST* be undertaken*?*	-	-	Yes x1	Yes x1	Yes x1	Yes x2
Verification of a *Linking document MUST* be undertaken if *Attribute*s vary across *EoI* documents?	-	-	Yes	Yes	Yes	Yes
Verification of a *UiTC document MUST* be undertaken that can confirm name and date of birth required?	-	Yes or *Photo ID* (see above)[11]	-	-	-	-
Approved technical *Credential* bindings	CL1/CL2/CL3	CL1/CL2/CL3	CL2/CL3	CL2/CL3	CL2/CL3	CL3

[9] This requires all names and the date of birth of the *Individual* to be verified as part of the *Identity Proofing* process. It does not require every identity document to include these *attributes*.

[10] Australian Passports *MAY* be used for *CoI* and *Photo ID* for up to *IP3* proofing but *MUST NOT* be accepted as *CoI* for IP4 proofing.

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

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**: Jun-21; **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*)
- Any other processes or approaches supported by the IdP and consistent with requirement IDP-03-03-01b

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 6 (**Appendix A**) with the *Individual's Express 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[12]. *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 Attribute collection, verification and validation

TDIF Req: IDP-03-06-01; **Updated**: Jun-21; **Applicability**: I

The *Applicant* *MUST NOT* collect, verify or validate *Attributes* beyond those listed in Table 2 and Table 3[13][14].

TDIF Req: IDP-03-06-02; **Archived**: Jun-21

This requirement has been archived in version 1.7.

[12] An *IdP* can offer multiple proofing levels without offering *Identity Proofing Step-up*

[13] An *Applicant* must demonstrate to the *DTA* a need for its accredited *identity system* to collect, verify and validate *Attributes* beyond those listed in tables 2 and 3. An *Applicant's* accredited *identity system* must be separate from the Applicant's other business operations.

[14] Biometric attributes and verification are covered in section 3.8 Biometric Verification Requirements

Table 2: *Attribute* collection, *verification* and *validation*

Attribute collection, verification and validation
Identity Attributes (verified)
All verified names – family name(s), given name(s), surname(s), full name(s), previous name(s) as recorded on the *EoI document*
Verified date of birth as recorded on the *EoI document* [if collected]
Contact Attributes (validated)
Mobile phone number
Email address
EoI* document *Attributes (verified restricted Attributes)
EoI document type name
EoI document type code
EoI document issuer
EoI document identifier(s) (e.g. registration, document, licence, or card numbers)
EoI document issuer state
Other *EoI document Attributes* (i.e. other *Attributes* on the document verified by an *Authoritative Source*)
Verification method used for each *EoI document* (i.e. S, T, V)
Date and time the *EoI document* was verified
Identity System metadata
Date and time *Attributes* last updated (i.e. verified names and date of birth)
Date and time email address was last validated (if collected)
Date and time mobile phone number was last validated (if collected)
Date and time the *User* authenticated at the *Identity Service Provider*
Identity Proofing Level achieved
Date and time the *Digital Identity* was created
Digital Identity (*User Identifier*)

Table 3: *Assumed Self-asserted Attributes*

***Attributes* that may be collected and recorded**[15]
Preferred name(s)
Residential address
Postal address
Other address (e.g. second residential address)
Other phone number (e.g. landline)
Place of Birth
Titles (e.g. Dr. Mr, Ms)

[15] Assumed Self-asserted attributes in this table are limited and are considered separate from Assumed Self-asserted attributes that an Attribute Service Provider (ASP) may offer. See Section 5 of this document for a list of ASP requirements.

TDIF Req: IDP-03-06-03; **Archived**: Jun-21
This requirement has been archived in version 1.7.

TDIF Req: IDP-03-06-04; **Archived**: Jun-21
This requirement has been archived in version 1.7.

3.7 Attribute disclosure

TDIF Req: IDP-03-07-01; **Updated**: Jun-21; **Applicability**: I
In accordance with PRIV-03-09-05, the *Applicant* *MUST* limit this disclosure to *Attributes* listed in Table 2.

TDIF Req: IDP-03-07-01a; **Archived**: Jun-21
This requirement has been archived in version 1.7.

TDIF Req: IDP-03-07-02; **Updated**: Jun-21; **Applicability**: I
In accordance with PRIV-03-09-01, the *Applicant* *MUST* limit this disclosure to the following *Attributes*:

- Identity *Attribute*s (verified) listed in Table 2.
- Contact *Attribute*s (validated) listed in Table 2.
- *Identity System* metadata listed in Table 2.
- *Assumed Self-asserted Attributes* listed in Table 3.

TDIF Req: IDP-03-07-03; **Updated**: Jun-21; **Applicability**: I
The *Applicant* *MUST* seek permission from the *DTA* to disclose *Attributes* beyond those listed in IDP-03-07-02.

TDIF Req: IDP-03-07-03a; **Updated**: Jun-21; **Applicability**: I
The *Applicant* *MUST NOT* disclose *Attributes* beyond those listed in IDP-03-07-02 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**: Jun-21; **Applicability**: I
The minimum number of subjects for the testing *MUST* be at least the same as described in current published version of the FIDO Biometric Requirements[16].

[16] This number is 245 as of the publication date of the *TDIF 05 Role Requirements Release 4 V1.7*.

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-03-08-17a; **Updated**: Jun-21; **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 the International Civil Aviation Organization (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:

TDIF Req: CSP-04-03-03h; **Updated**: Jun-21; **Applicability**: C
The *PAD* decision *MAY* be made either locally on the *Individual's* device or by the *Applicant*.

TDIF Req: CSP-04-03-03i; **Updated**: Jun-21; **Applicability**: C
The biometric system *MUST* allow no more than 5 consecutive failed *Authentication* attempts or 10 consecutive failed attempts.

TDIF Req: CSP-04-03-03j; **Updated**: Jun-21; **Applicability**: C
Once the limit of consecutive failed attempts has been reached, the biometric system *MUST* either:

- Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt (e.g. 1 minute before the following failed attempt, 2 minutes before the second following attempt), or
- Disable the biometric *User Authentication* and offer another factor (e.g. a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

TDIF Req: CSP-04-03-03k; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* make a determination of sensor and endpoint performance, integrity, and authenticity. Acceptable methods for making this determination include, but are not limited to:

- *Authentication* of the sensor or endpoint
- Certification by an approved accreditation authority
- Runtime interrogation of signed metadata (e.g. *Attestation*).

TDIF Req: CSP-04-03-03l; **Updated**: Jun-21; **Applicability**: C
If supported, biometric comparison that is performed centrally *MUST* implement the following requirements:

- Use of the biometric as an *Authentication factor MUST* be limited to one or more specific devices that are identified using approved cryptography (i.e. *AACAs and AACPs*)
- Since the biometric has not yet unlocked the main *Authentication Key*, a separate *Key MUST* be used for identifying the device
- Biometric revocation, referred to as 'biometric template protection' in *ISO/IEC 24745*, *MUST* be implemented

- All transmission of biometrics *MUST* be over the *Authenticated Protected Channel*.

TDIF Req: CSP-04-03-03m; **Updated**: Jun-21; **Applicability**: C
Biometric Samples collected in the *Authentication* process *MAY* be used to train comparison algorithms or — with *User Express Consent* — for other research purposes.

TDIF Req: CSP-04-03-03n; **Updated**: Jun-21; **Applicability**: C
Biometric Samples and any biometric data derived from the *Biometric Sample* such as a probe produced through signal processing *MUST* be zeroised immediately after any training or research data has been derived.

4.3.4 Credential Attestation

TDIF Req: CSP-04-03-04; **Updated**: Jun-21; **Applicability**: C
If *Credential Attestation* is supported, the *Applicant* *MUST* implement the following requirements for the operation of *Credential Attestation*.

TDIF Req: CSP-04-03-04a; **Updated**: Jun-21; **Applicability**: C
Information conveyed by *Credential Attestation* *MAY* include, but is not limited to:

- The provenance (e.g. manufacturer or supplier certification), health, and integrity of the *Credential* and endpoint
- Security features of the *Credential*
- Security and performance characteristics of biometric sensor(s)
- Sensor modality.

TDIF Req: CSP-04-03-04b; **Updated**: Jun-21; **Applicability**: C
If this *Attestation* is signed, it *MUST* be signed using a digital signature that provides at least the minimum-security strength specified in the latest version of the *ISM*.

TDIF Req: CSP-04-03-04c; **Updated**: Jun-21; **Applicability**: C
Attestation information *MAY* be used as part of an *Applicant's* risk-based *Authentication* decision.

4.3.5 *CSP-impersonation Resistance*

As per Table 4, *CSP-impersonation Resistance* is required at CL3.

TDIF Req: CSP-04-03-05; **Updated**: Jun-21; **Applicability**: C
Where the *Applicant* supports *CL3,* it *MUST* implement the following *CSP-impersonation Resistance* requirements. These requirements do not need to be implemented for CL1 or CL2.

TDIF Req: CSP-04-03-05a; **Updated**: Jun-21; **Applicability**: C
A *CSP-impersonation* resistant *Authentication Protocol MUST* establish an *Authenticated Protected Channel* with the *Applicant*.

TDIF Req: CSP-04-03-05b; **Updated**: Jun-21; **Applicability**: C
A *CSP-impersonation resistant Authentication Protocol MUST* strongly and irreversibly bind a channel identifier that was negotiated in establishing the *Authenticated Protected Channel* to the *Authentication* output (e.g. by signing the two values together using a *Private Key* controlled by the claimant for which the *Public Key* is known to the *Applicant)*.

TDIF Req: CSP-04-03-05c; **Updated**: Jun-21; **Applicability**: C
The *Applicant MUST* validate the signature or other information used to prove *CSP-impersonation Resistance*. This prevents an *impostor CSP Attacker*, even one that has obtained a certificate representing the actual *CSP*, from replaying that *Authentication* on a different *Authenticated Protected Channel*.

TDIF Req: CSP-04-03-05d; **Updated**: Jun-21; **Applicability**: C
AACAs MUST be used to establish *CSP-impersonation Resistance* where it is required.

TDIF Req: CSP-04-03-05e; **Updated**: Jun-21; **Applicability**: C
*Key*s used for this purpose *MUST* provide at least the minimum-security strength specified in the latest edition of the *ISM*.

TDIF Req: CSP-04-03-05f; **Updated**: Jun-21; **Applicability**: C

Credentials that involve the manual entry of an *Authentication* output, such as *out-of-band* and *OTP Credentials*, MUST NOT be considered *CSP-impersonation resistant* because the manual entry does not bind the *Authentication* output to the specific *Session* being authenticated.

4.3.6 IdP-CSP communications

TDIF Req: CSP-04-03-06; **Updated**: Jun-21; **Applicability**: C, I

In situations where the *IdP* and *CSP* are separate entities, communication MUST occur through a mutually authenticated secure channel (such as a client-authenticated *TLS* connection) using approved cryptography (i.e. *AACAs* and *AACPs*).

4.3.7 *CSP-compromise Resistance*

As per Table 4, *CSP-compromise Resistance* is required at *CL3*.

TDIF Req: CSP-04-03-07; **Updated**: Jun-21; **Applicability**: C

Where the *Applicant* supports *CL3,* it MUST implement the following *CSP-compromise Resistance* requirements. These requirements do not need to be implemented for *CL1* or *CL2.*

TDIF Req: CSP-04-03-07a; **Updated**: Jun-21; **Applicability**: C

To be considered *CSP-compromise* resistant, *Public Key*s stored by the *Applicant* MUST be associated with the use of *approved cryptographic algorithms* (i.e. *AACAs*).

TDIF Req: CSP-04-03-07b; **Updated**: Jun-21; **Applicability**: C

*Key*s MUST provide at least the minimum-security strength specified in the latest version of the *ISM*.

4.3.8 Replay resistance

As per Table 4, *replay resistance* is required at *CL2* and *CL3*.

TDIF Req: CSP-04-03-08; **Updated**: Jun-21; **Applicability**: C
Where the *Applicant* supports *CL2* or *CL3,* it *MUST* implement at least one of the following *Credentials*:

- *OTP Devices*
- *Out-of-band Devices*
- Cryptographic-based *Credentials*
- *Look-up Secrets*.

4.3.9 *Authentication* intent

As per Table 4, *Authentication* intent is required at *CL 3*.

TDIF Req: CSP-04-03-09; **Updated**: Jun-21; **Applicability**: C
Where the *Applicant* supports *CL 3* it *MUST* implement the following *Authentication* intent requirements. These requirements do not need to be implemented for *CL 1* or *CL 2.*

TDIF Req: CSP-04-03-09a; **Updated**: Jun-21; **Applicability**: C
Authentication intent *MUST* be established by the *Credential* itself.

TDIF Req: CSP-04-03-09b; **Updated**: Jun-21; **Applicability**: C
Authentication intent *MAY* be established in several ways, including:

- *Authentication* processes that require the *Individual's* intervention (e.g. an *Individual* entering an *Authentication* output from an *OTP* device).
- Cryptographic devices that require *User* action (e.g. pushing a button or reinsertion) for each *Authentication* or re-authentication operation.

4.3.10 Restricted *Credentials*

TDIF Req: CSP-04-03-10; **Updated**: Jun-21; **Applicability**: C
If, at any time, the *Applicant* determines that a *Credential* is resulting in an unacceptable risk to any party, then they *MUST* prevent continued use of that *Credential*. Such *Credentials* are referred to as *Restricted Credentials*.

TDIF Req: CSP-04-03-11; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* supports the use of a Restricted *Credential*, it *MUST*:

1. Offer *Individuals* at least one alternate *Credential* that is not restricted and can be used to authenticate at the required *CL*
2. Provide meaningful notice to *Individuals* regarding the security risks of the *Restricted Credential* and availability of alternative(s) that are not restricted
3. Address any additional risk to *Individuals* in its *security Risk Assessment*
4. Develop a migration plan for the possibility that the *Restricted Credential* is no longer acceptable at some point in the future.

4.4 *Credential* lifecycle management

4.4.1 *Credential* binding

TDIF Req: CSP-04-04-01; **Updated**: Jun-21; **Applicability**: C

A *Credential* MUST be bound to an *Individual's* account by either:

- Issuance by the *Applicant* as part of enrolment; or
- Associating a *User*-provided *Credential* that is acceptable to the *Applicant*.

TDIF Req: CSP-04-04-01a; **Updated**: Jun-21; **Applicability**: C

Throughout the *Digital Identity* lifecycle, the *Applicant* MUST maintain a record of all *Credentials* that are or have been associated with each *Digital Identity* account.

TDIF Req: CSP-04-04-01b; **Updated**: Jun-21; **Applicability**: C

The *Applicant* MUST maintain the information required for *Throttling Authentication* attempts when required.

TDIF Req: CSP-04-04-01c; **Updated**: Jun-21; **Applicability**: C

The *Applicant* MUST also verify the *Credential* type of a *User*-provided *Credential* (e.g. *Single-factor Cryptographic Device* vs. *Multi-factor Cryptographic Device*) so the *Applicant* can determine compliance with requirements at each CL.

TDIF Req: CSP-04-04-01d; **Updated**: Jun-21; **Applicability**: C

The record created by the *Applicant* MUST contain the date and time the *Credential* was bound to the account.

TDIF Req: CSP-04-04-01e; **Updated**: Jun-21; **Applicability**: C
The record *MUST* include information about the source of the binding (e.g. IP address, device identifier) of any device associated with the enrolment.

TDIF Req: CSP-04-04-01f; **Updated**: Jun-21; **Applicability**: C
The record *MUST* also contain information about the source of unsuccessful *Authentications* attempted with the *Credential*.

TDIF Req: CSP-04-04-01g; **Updated**: Jun-21; **Applicability**: C
When any new *Credential* is bound to an *Individual's* account, the *Applicant MUST* ensure that the binding protocol and the protocol for provisioning the associated *Key*(s) are done at a level of security commensurate with the *CL* at which the *Credential* will be used.

4.4.2 Binding at enrolment

TDIF Req: CSP-04-04-02; **Updated**: Jun-21; **Applicability**: C
For remote transactions where enrolment and binding cannot be completed in a single electronic transaction (i.e. within a single protected *Session*), the following requirements *MUST* be met to ensure that the same party acts as the *Individual* throughout the process:

- The *Individual MUST* identify themselves in each new binding transaction by presenting a temporary secret which was either established during a prior transaction or sent to the *Individual's* mobile phone number or email address.
- Long-term *Authentication* secrets *MUST* only be issued to the *Individual* within a protected *Session*.

TDIF Req: CSP-04-04-02a; **Updated**: Jun-21; **Applicability**: C
For in-person transactions where enrolment and binding cannot be completed in a single physical encounter (i.e. within a single protected *Session*), the following requirements *MUST* be met to ensure that the same party acts as the *Individual* throughout the process:

- The *Individual MUST* identify themselves in-person by either using a secret as described in CSP-04-04-02, or through use of a biometric that was recorded during the *identity proofing* process.
- Temporary secrets *MUST NOT* be reused

- If the *Applicant* issues long-term *Authentication* secrets during a physical transaction, then they *MUST* be loaded locally onto a physical device that is issued in-person to the *individual* or delivered in a manner that confirms the *individual's* email address or mobile phone number.

4.4.3 Binding additional *Credentials*

TDIF Req: CSP-04-04-03; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* supports the *Binding* of additional *Credentials* to an *Individual's* account, then it *MUST* implement the following requirements when *Binding* additional *Credentials* to an *individual's* account.

TDIF Req: CSP-04-04-03a; **Updated**: Jun-21; **Applicability**: C
Before *Binding* an additional *Credential* to an *Individual's* account, the *Applicant* *MUST* first require the *Individual* to authenticate at the *CL* (or a higher *CL*) at which the new *Credential* will be used.

TDIF Req: CSP-04-04-03b; **Updated**: Jun-21; **Applicability**: C
When a *Credential* is added, the *Applicant* *MAY* send a notification to the *Individual* via a mechanism that is independent of the transaction *Binding* the new *Credential* (e.g. email to an address previously associated with the *Individual*).

TDIF Req: CSP-04-04-03c; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* limit the number of *Credentials* that may be bound in this manner.

TDIF Req: CSP-04-04-04; **Updated**: Jun-21; **Applicability**: C
Before *Binding* a new *Credential* to an account, the *Applicant* *MUST* require the *Individual* to authenticate with a *Credential* of at least *CL1*.

TDIF Req: CSP-04-04-04a; **Updated**: Jun-21; **Applicability**: C
When a *Credential* is added, the *Applicant* *MAY* send a notification to the *Individual* via a mechanism that is independent of the transaction *Binding* the new *Credential* (e.g. email to an address previously associated with the *Individual*).

TDIF Req: CSP-04-04-05; **Archived**: Jun-21
This requirement has been archived in version 1.7.

4.4.4 Binding to a User-provided Credential

TDIF Req: CSP-04-04-06; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY*, where practical, accommodate the use of a *User*-provided *Credential* to relieve the burden to the *User* of managing a large number of *Credentials*.

4.4.5 Renewal

TDIF Req: CSP-04-04-07; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* bind an updated *Credential* a reasonable amount of time before an existing *Credential's* expiration.

TDIF Req: CSP-04-04-08; **Updated**: Jun-21; **Applicability**: C
Following successful use of the new *Credential*, the *Applicant* *MAY* revoke the *Credential* that it is replacing.

4.5 Loss, theft, damage and unauthorised duplication

TDIF Req: CSP-04-05-01; **Updated**: Jun-21; **Applicability**: C
The suspension, revocation or destruction of a compromised *Credential* *MUST* occur as promptly as practical following the detection or report of loss, theft, damage or unauthorised duplication of a *Credential*.

TDIF Req: CSP-04-05-02; **Updated**: Jun-21; **Applicability**: C
To facilitate secure reporting of the loss, theft or damage to a *Credential*, the *Applicant* *MAY* provide the *Individual* with a method of authenticating to the *Applicant* using a backup or alternate *Credential*.

TDIF Req: CSP-04-05-03; **Updated**: Jun-21; **Applicability**: C
If the *Applicant* implements CSP-04-05-02, then the backup *Credential* *MUST* be either a *Memorised Secret* or a physical *Credential*.

TDIF Req: CSP-04-05-04; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MAY* choose to *validate* a *User*'s contact details (i.e. email, mobile phone number) and *MUST* suspend a *Credential* reported to have been compromised.

4.11 Certification Authorities

TDIF Req: CSP-04-11-01; **Updated**: Jun-21; **Applicability**: C
If *Certification Authorities* are supported, then the *Applicant* *MUST* implement all of the following requirements to operate as a *Certification Authority*.

TDIF Req: CSP-04-11-02; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* ensure all:

a. *Certification Practice Statements (CPS)* and *Certificate Policies (CP)* conform to Request for Comment (RFC) 3647
b. *Digital Certificates* conform to the (RFC) 5280 format
c. *Certificate Revocation Lists (CRLs*) conform to the X.509 version 2 profile as described in RFC 5280
d. Online Certificate Status Protocol (OCSP) responses conform to RFC 6960.

TDIF Req: CSP-04-11-03; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* ensure the *Root Certification Authority* (CA) *Private Key* is not used to digitally sign *Digital Certificates,* except in the following cases:

- Self-signed *Digital Certificates* to represent the *Root CA* itself.
- *Digital Certificates* for *Subordinate CAs* and *Cross Certificates*.
- *Digital Certificates* for infrastructure purposes (for example, administrative role certificates and *OCSP Digital Certificates*).
- *Digital Certificates* issued solely for the purpose of testing software with *Digital Certificates* issued by the *Root CA*.

TDIF Req: CSP-04-11-04; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* implement a process to allow *Individuals* to request revocation of their *Digital Certificate.*

TDIF Req: CSP-04-11-04a; **Updated**: Jun-21; **Applicability**: C
The *Applicant* *MUST* implement revocation procedures for the following situations:

- The *Individual* notifies the *Applicant* that a *Digital Certificate* request was not authorised by them.
- The *Applicant* obtains evidence that a *Digital Certificate*'s *Private Key* suffered a *Key* compromise or no longer complies with the requirements outlined in the *Certificate Policy*.

5 Attribute Service Provider Requirements

All *Attribute* lifecycle management operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-12a). These requirements can be found in *TDIF 04 Functional 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 5: 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*[19] (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).
Assumed 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

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

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.

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*.

6 Identity Exchange Requirements

All Identity Exchange operations must be informed by the *Applicant's Fraud Control Plan* (FRAUD-02-02-01), *Privacy Policy* (PRIV-03-02-03) and *System Security Plan* (PROT-04-01-12a). These requirements can be found in *TDIF 04 Functional Requirements*.

6.1 *Audit Log*ging Requirements

TDIF Req: IDX-06-01-01**; Updated:** Jun-21**; Applicability:** X
The *Applicant* ***MUST*** generate a unique audit Id for an *Authentication Request* from a *Relying Party* to be used as the unique interaction identifier for the interaction.

TDIF Req: IDX-06-01-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* ***MUST*** log all related interactions between *Relying Parties* and *Identity Service Providers* using this unique audit id (this includes *Attribute Service Providers* acting as *Relying Parties*).

6.2 Consent Management

TDIF Req: IDX-06-02-01; **Updated:** Jun-21; **Applicability:** X
In accordance with PRIV-03-09-03, the *Applicant* ***MUST*** maintain the following information as part of its *Audit Logs*:

- Timestamp
- Duration of *Consent*. (including any time limit on the consent)
- *Relying Party*. (i.e. The *Relying Party* that requested to receive the *Attribute*s)
- The *Identifier* that identifies the *User* at the *Relying Party* authorised to receive the *Attribute*s
- *Identity Service Provider/Attribute Service Provider* from which the *Attribute*s were sourced
- The link to the *Identity* at the source of the *Attribute*s
- Name of any *Attribute* or *Attribute* set authorised
- *Consent* decision. This may be "grant", "deny", or "ongoing"

6.3 *Single Sign On*/Single *Logout*

Single Sign On is an optional feature that an *Applicant* may implement in their system.

TDIF Req: IDX-06-03-01; **Updated**: Jun-21; **Applicability**: X
If *Single Sign On* is supported, then the *Applicant* *MUST* implement the following requirements to operate *Single Sign On*.

TDIF Req: IDX-06-03-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* support the ability for a *Relying Party* to request that a *User* authenticates regardless of whether a pre-existing *Session* exists.

TDIF Req: IDX-06-03-02a**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MUST* implement a *single Logout* mechanism according to the *Federation Protocol* that it supports.

TDIF Req: IDX-06-03-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MAY* securely cache *Attributes* from an *Identity Service Provider* for the duration of an authenticated *Session* to support *Single Sign On*.

TDIF Req: IDX-06-03-03a**; Updated:** Jun-21**; Applicability:** X
If the *Applicant* securely caches *Attribute*s as per IDX-06-03-03, these *Attribute*s *MUST NOT* be accessible to the *Applicant's Personnel*.

TDIF Req: IDX-06-03-04**; Updated:** Jun-21**; Applicability:** X
The *Applicant* *MAY* restrict the expiration period for an *Authentication Session* to manage security risks.

6.4 User Dashboard

A *User Dashboard* is a way for an *Individual* to view their *Consumer History* and manage their *Express Consent*. A *User Dashboard is* an optional feature that an *Applicant* may implement in their system.

TDIF Req: IDX-06-04-01; **Updated:** Jun-21**; Applicability:** X
If a *User Dashboard* is supported, then the *Applicant* *MUST* implement the following requirements for the operation of a *User Dashboard.*

TDIF Req: IDX-06-04-02**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MUST display to the *Individual* their *Consumer History* and enable the *Individual* to view the *Express Consent* they have provided to share *Attributes* with a *Relying Party* or any third party.

TDIF Req: IDX-06-04-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MUST NOT store *Attributes* of the *Individual* beyond the *Individual's* presence at the *User Dashboard*.

6.5 IdP Selection

The *Applicant may* provide a method for an *Individual* to select an *Identity Service Provider* from a list of *Identity Service Providers* that are integrated with the *Identity Exchange* when accessing a *Relying Party*. This is known as *IdP Selection.*

TDIF Req: IDX-06-05-01; **Updated**: Jun-21; **Applicability**: X
If *IdP Selection* is supported, then the *Applicant* MUST implement the following requirements for the operation of *IdP Selection.*

TDIF Req: IDX-06-05-02; **Updated**: Jun-21; **Applicability**: X
The list of *Identity Service Providers* presented by the *Applicant* to the *User* MUST be capable of meeting the *Credential Level* and *Identity Proofing Level* requested in the *Authentication Request*.

TDIF Req: IDX-06-05-03**; Updated:** Jun-21**; Applicability:** X
The *Applicant* MAY provide a mechanism for an *Individual's* selection of an *Identity Service Provider* to be remembered so the *Individual* does not have to select an *Identity Service Provider* (again) when accessing a *Relying Party*.

TDIF Req: IDX-06-05-03a**; Updated:** Jun-21**; Applicability:** X
Express Consent MUST be obtained from the *Individual* prior to offering the mechanism described in IDX-06-05-03.

TDIF Req: IDX-06-05-03b**; Updated:** Jun-21**; Applicability:** X
The *Individual* MUST have the ability to opt out of using the mechanism described in IDX-06-05-03.

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 6 lists the *EoI document* types and the verification methods that an *Applicant* may support. A description of the verification methods is available in *TDIF 05A Role Guidance*. *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 6: 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	Issued by an Australian State or Territory Government Register of Births, Deaths and Marriages.	Source Visual
Australian Passport[20]	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

[20] 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.	Source Visual
Operation Objective – confirm the operation of the *Identity* in the Australian community over time		
Use in the Community documents		
Concession and Health Care Cards	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 transactions and be in the *Individual's* name.	Source Visual

Type of Evidence	Notes	Verification method
	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 the *Photo ID* 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	Source Visual

Type of Evidence	Notes	Verification method
	in 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 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 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 Home Affairs.[21]	Source
Indigenous Community Card[22]	*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
Maritime Security Identity Card	A current card issued in the *Individual's* name and includes their photo.	Visual

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

[22] 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
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[23]	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

[23] 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.