Australian Government
Digital Transformation Agency

Identity Proofing Requirements

Trusted Digital Identity Framework
March 2018, version 1.06

CONSULTATION DRAFT

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Mar 2018
Commonwealth GovPass Design Authority	TBA

Change log

Version	Date	Author	Description of the changes
0.01-0.074	Aug 2016	SJP	Initial version and minor updates
0.075	Jan 2017	DA & AH	Changes how IP 2, IP 3 and step-up between IP 2 and IP 3 will be satisfied. Requires the use of the DVS to verify all identity attributes and requires individuals to verify their identity using Commencement of Identity, Linking and Use in the Community identity documents. Photos on Linking documents will be verified with the Document Issuer through the Government's Face Verification Service.
0.08	May 2017	PH & MC	Changes based on feedback from DIBP and DFAT, and internal stakeholder feedback. Glossary added. Identity verification process overview added. Evidence of Identity categories changed. Individuals required to verify their identity using: Commencement of Identity, Binding, Linking and Use in the Community. Definitions Section added. Section on biometric attributes and Validation requirements added. GPG 45 and NIST 800-63 A comparison conducted.
0.09	Jul 2017	PH	Document restructure - Document split into an introduction and 2 parts. Standard moved to part 1 of the document, guidance to meet the standard contained in part 2 of the document
0.10	Dec 2017	PH	Incorporated targeted and public consultation Feedback. FoD file check out of scope. Social footprint checks redefined. More options added to UitC document list. Recast as a requirements document.
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority.
1.01 – 1.04	Feb 2018	AJH	Updates based on internal review and merged online and offline identity proofing requirements into the one document.
1.05	Mar 2018	AJH & GJF	Updates based on internal feedback.
1.06	Mar 2018	SJP	Converted to new template and updated based on internal review.

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **MUST NOT** – means an absolute prohibition of this document.
- **SHOULD** – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.
- **SHOULD NOT** – means there may exist valid reasons when a particular item is acceptable, but the full implications need to be understood before implementing the item.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

Establishing confidence in a person's identity is a critical starting point for delivering a range of government digital services and benefits, as it is for many transactions conducted by the privacy sector and other non-government organisations. The objective of identity proofing is to verify a person's identity information to obtain a reusable digital identity.

Whilst many people will be able to establish a digital identity based on their existing documentation, for a number of valid reasons some individuals will require assistance, either online or in person, to prove their identity. These *Trust Framework: Identity Proofing Requirements* have been written to provide a broader range of options for people unable to successfully verify their identity in an exclusively digital channel. This may be due a lack of Evidence of Identity (EoI) or limitations in their digital access or literacy. This document enables people to have their identity information verified either face-to-face over a counter or through digital means.

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). This federation will be capable of providing trusted digital identities to Relying Parties in order for them to deliver online services and benefits to people. Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF), which contains the tools, rules and accreditation criteria to govern the identity federation. This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document sets out the identity proofing requirements to be met by agencies and organisations accredited as Identity Service Providers (IdPs) under the TDIF. The following items are out of scope but will be addressed in a later release of this document:

- Minimum age limitations for children and young people under the age of 15 who may have their identity verified by an IdP.

- Collection and use of non-facial biometrics for the purpose of supporting identity proofing processes.
- Identity proofing non-person entities.
- End-to-end identity management processes such as identity refresh or identity retirement.

This document comprises three parts:

- Part 1: describes the TDIF identity proofing objectives, identity proofing levels, EoI categories and EoI verification methods.
- Part 2: describes the TDIF Identity Proofing Requirements to be met by IdPs.
- Part 3: provides guidance on how to implement these requirements.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

1.1 Context

Within the TDIF there are four Identity Proofing (IP) levels of assurance (or confidence) defined for the identity proofing process, which are ranked from lowest to highest based on the consequence of incorrectly identifying a person. The assurance reflected by each level is derived from the veracity of the claims about a person's identity, through the evidence provided, to meet some or all of the identity proofing objectives of:

- Context uniqueness.
- Legitimacy.
- Binding between the person and the evidence of identity.
- Operation within the community.
- Confirmation that an identity is not known to be fraudulent.

As a result of these objectives being met at different levels of assurance across the four IPs the Relying Party can have a degree of confidence, depending of the IP achieved, that:

- The claimed identity has been resolved to a single, unique identity within the context of the cohort of people that the IdP serves.
- The supplied identity evidence has been confirmed as legitimately existing, correct, current and genuine.
- The claimed identity has been verified as being associated with, and bound to the person supplying the identity evidence.
- The claimed identity exists and accepted as operating in the real world.
- The claimed identity is not known to be fraudulent.

As the 'consumers' of digital identities, Relying Parties need to determine their required level of identity assurance based on an identity risk assessment. Guidance on how to perform an identity risk assessment is set out in the *Trust Framework: Risk Management Requirements*.

These *Trust Framework: Identity Proofing Requirements* are supported by a suite of companion documents within the TDIF, including the *Authentication Credential Requirements*, the *Protective Security Requirements*, the *Privacy Requirements* and the *Fraud Control Requirements*. Together this suite enables Relying Parties to obtain a level of confidence about the identity of a person who has requested a digital service.

This document aligns with and builds on several national and international approaches that define levels of identity proofing. This includes the:

- Council of Australian Government's (COAG) National Identity Proofing Guidelines (NIPG), and
- National Institute of Standards and Technology (NIST) Special Publication (SP) Digital Identity Guidelines (800-63 series).

The mappings between TDIF IPs and other identity proofing approaches is listed in Annex A.

2 Identity proofing concepts

2.1 Identity proofing objectives

Not all Relying Parties or transactions within the identity federation will require the same level of confidence in the digital identity. As such, Relying Parties will require varying levels of confidence (accepted risk) in the digital identity based on the consequence of incorrectly identifying a person in the provision of their services.

To achieve this IdPs undertake an identity proofing process that tests the veracity of claims, i.e. EoI, a person makes regarding their identity with a view to achieving some or all of the following objectives.

1. **Confirm uniqueness of the identity in the intended context** to ensure that people can be distinguished from one another and that the right service is delivered to the right person. This reduces risks such as doubling up on service provision, however, whilst it may be unique in the context of the online transaction it does not necessarily need to uniquely identify the person in all contexts.

2. **Confirm the claimed identity is legitimate** to ensure the identity has been genuinely created as well as confirming that there is continuity in a person's identity attributes where there have been changes. Increased confidence in the legitimacy of a person's identity is achieved through verifying Commencement of Identity EoI with authoritative sources and verifying Linking Documents where name or date of birth details differ between pieces of EoI. This reduces risks such as the registration of imposters or non-genuine identities.

3. **Confirm the binding between identity attributes and the person claiming the identity** to provide a high level of confidence that the person's identity confirmed through objectives 1 and 2 is not only legitimate, but that the person currently claiming the identity is its legitimate holder. This reduces the opportunity for identity fraud. The Trust Framework relies on facial binding to reduce this risk.

4. **Confirm the operation of the identity in the community over time** to provide additional confidence that a person's identity is legitimate in that it is being used in the community (including online where appropriate). Requiring a pattern of use over a period of time implies that the person's identity has a history and reduces the risk that it is fraudulent.

5. **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. These checks, either internally or with external sources, such as law enforcement agencies or comparing personal attributes against the Fact of Death file decrease the risk of a fraudulent identity within the identity federation.

2.2 Identity proofing levels

As mentioned in Section 1 above, the TDIF utilises four identity proofing levels, ranging from level 1 (low, self-asserted) through to level 4 (very high, in-person verified).

Table 1 below outlines for each of the respective identity proofing levels the applicable Identity proofing objectives, the EoI required and examples of relevant use.

Table 1: identity proofing levels

	IP 1	IP2	IP 3	IP 4
Confidence	**Low**	**Medium**	**High**	**Very High**
Identity proofing objectives	Claimed identity is: unique in context	Claimed identity: is unique in context, is supported by evidence, is known to be operating in the community, and is known not to be fraudulent.	Claimed identity: is unique in context, exists as a legitimate identity, is bound to the person (ie. supported by a biometric match), is confirmed to be operating in the community, and is not known to be fraudulent.	Claimed identity: is unique in context, exists as a legitimate identity, is strongly bound to the person (ie. supported by a biometric match), is confirmed to be operating in the community, and is not known to be fraudulent.
EoI requirements	NIL	1 CoI, OR 1 Photo ID + 1 UiTC, OR 3 documents each from different sources, OR 3 electronic data	1 CoI + 1 Photo ID, OR 1 Alternative Binding + 1 UiTC, OR 3 documents each from different	1 CoI + 1 Photo ID, + 2 UiTC, OR 3 document each from different sources, OR

	IP 1	IP2	IP 3	IP 4
		points from 1 source + Linking documents (where necessary)	sources, OR 3 electronic data points from 1 source + Linking documents (where necessary)	3 electronic data points from 1 source + Linking documents (where necessary)
Intended use	For low risk or low value transactions where no verification is required, but the parties desire a continuing conversation (eg. post in a discussion forum)	For moderate risk or moderate value services where fraud will have moderate consequences (eg. provision utility services)	For major risk or major value services with a high risk of serious consequences from fraud (eg. provision of common government services such as issuing licences, access cards, or undertaking financial exchanges).	For services where extreme consequences arise from fraudulent verifications. (eg. provision of trusted government credentials, such as passports, secure access, etc, or to proof 'trusted' roles such as privileged positions)
Comments	Pseudonymity is supported, but not anonymity	Facial-matching is not required	Facial matching is required	Facial matching and In-person interview required

2.3 Evidence of identity

Identity Proofing is the process by which an IdP collects, validates, and verifies information about a person and, as such, it relies heavily on the identity evidence presented. This evidence may be physical or digital/electronic credentials[2] and can have widely varying strength in relation to authoritative source and credential security. In addition, there may be different identity attributes contained within the evidence, including identity attributes (full name and date of birth), document identifiers and contact information (e.g address, phone number).

The evidence and information sources used within the TDIF for the enrolment and proofing of a person's identity falls into five fundamental categories:

- **Commencement of Identity (CoI)** is a government issued document:

[2] Commonly referred to as documents, however, they may not be paper based

- Which anchors a person'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 document and manage it throughout its lifecycle.
- With identity attributes contained in or printed on the document able to be securely verified through authoritative sources (eg. Document or Facial Verification Service (DVS/FVS).

- **Photo ID** is a document:
  - Which allows binding between the presented identity attributes and the person claiming the identity.
  - Where the biometric image of the person is securely contained in or printed on the 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 document are able to be securely verified through authoritative sources.
  - Where the image of the holder contained in or printed on the document can be either verified through the FVS, or through a secure technical means from the securely stored image[3], or by the visual inspection of a trained operator.
- **Use in the Community (UitC)** is a verifiable document issued by a reliable source which:
  - Includes identity attributes (in particular the name) either contained in or printed on the document, or within a repository that provides reasonable confidence that they cannot be modified after the fact.
  - Can be used to confirm the activity of the identity in the community over time.
  - Has identity attributes which may be verified through authoritative sources or community footprint checks.
- **Linking document** is a government issued document:
  - Which provides a link demonstrating the continuity of the claimed identity where identity details (i.e. name, date of birth) have changed. e.g. change of name certificate, marriage certificate, or in some cases a birth certificate.
  - With attributes contained in or printed on the document that can be verified through the DVS.

[3] For example: contained in a secure Integrated Circuit Chip (ICC) on a passport

- **Alternative Binding (Identity Attestation)** is:
  - An attestation by a verified referee who has either a provable relationship with the person claiming an identity or has a professional status such that they can reliably attest to the identity of the person.
  - Endorsement of an image of the person, providing the required linkage between the identity and their biometric image.
  - An alternative to presenting a Photo ID document by addressing the issue of requiring a linkage between the person claiming an identity and their presented identity data sources in the absence of an existing facial document (such as photo ID).

Annex B contains a list of evidence that is approved for use within the TDIF against each of the categories listed above. Evidence not listed in Annex B may not be used without the explicit permission of the Trust Framework Accreditation Authority. Whilst at present this evidence is predominantly physical credential/document sources in the future digital/electronic sources may become more prevalent and these may be added by the Trust Framework Accreditation Authority to the approved EoI listed.

2.4 Verification methods

Within the identity proofing process the actions associated with checking the veracity of the claims about a person's identity is heavily dependent on EoI document verification. Whilst verifying identity credentials depends upon their format (physical or electronic), they can be checked using various methods which all have respective strengths and weaknesses. As such these requirements have defined four verification methods that are used within the identity proofing process.

The four methods of verification in order of preference are:

- **Source Verification** - the act of verifying physical or electronic EoI directly with the issuing body (or their representative, e.g. via the DVS or FVS services). 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 mechanism bound to a secure chip or appended to it (eg. via Public Key Technology). Technical verification is generally very accurate, but is dependent of the issuers revocation processes (e.g. a stolen passport may still pass technical verification).
- **Visual Verification** - the act of a trained operator visually confirming, either electronically or in-person, that the evidence presented, with any security features, appears to be valid and unaltered, and/or making a facial comparison check. Generally this 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 person.
- **Community Footprint Check (CFC) –** is a check associated with UiTC documents that provides historical evidence of the identity operating in the community over time. This check can review either physical documents or non-documentary identity data held in a repository, accessible by an IdP, that provides a degree of confidence that it cannot be modified after the fact.

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

2.5 Identity attributes

Within the identity federation an identity is roughly equivalent to a persona, verified or self-asserted, that a person may choose to be known by. Associated with any identity is virtually an unlimited set of possible claimed values (attributes) that are characteristics of that identity. This can include attributes such as a full name, preferred name, date of birth, gender, title, location of birth, citizenship, address, phone number, email address, occupation, etc. In addition, different types of evidence of identity may contain different identity attributes contained within the evidence. These may also contain identifiers, attributes that can provide linkage to a specific identity such as passport number, drivers licence, customer reference number, etc. When combined these attributes uniquely describe a person within a given context.

307 The *Trust Framework: Attribute Profile* details the attribute sets used within the TDIF.

308 Of particular importance for this document is the ‘core attribute set’, which includes:

309 • Given name(s)

310 • Family Name

311 • Date of Birth (DOB)

3 Identity Service Provider Requirements

3.1 General requirements

The IdP **MUST**:

- Verify a person's EoI to an authoritative source where it is possible.
- As applicable, record the core attribute set that have been provided by the person.
- Record all variations of the core attribute set provided on EoI documents.
- Where the person's core attribute set are not consistent between presented EoI (once naming and DOB conventions are considered), verify the attributes collected via a Linking document and record the Linking document's type (and identifier if applicable).
- As applicable, record the following identity attributes:
    - The person's asserted contact attributes, which may include address, phone and email, etc (as provided or used in the claims).
    - The person's asserted preferred name(s).
    - EoI identifiers used in the process.
    - Identity proofing level achieved.
    - Date identity proofed.
    - Credential details/type and person's unique IdP identifier allocated.
- Record the EoI used in the ID proofing process and their applicable identifier(s).
- For each verified attribute, record the verification sources used in the process, the outcome/results and date undertaken.
- Validate at least 1 of the claimed contact details.
- Ensure that where an identity verification or validation process is unsuccessful, the following is undertaken:
    - The issue is recorded, in the IdP's system.
    - Advise the person of the outcome and provide them with guidance, based on the reason for the error, to resolve the issue.
    - Advise the person of alternative methods to complete the proofing process.
    - Where the ID proofing process cannot be completed during the current transaction and is mediated by the Identity Exchange, inform the Identity Exchange that the proofing process has ceased.

- Ensure that EoI is not used for more than one ID Proofing objective.
- Comply with DVS/FVS standards if DVS/FVS is used for Source Verification.
- On a monthly basis re-verify the person's identity attributes are not known to be fraudulent by confirming the person's identity is not recorded on the Fact of Death File or listed in the IdPs list of known fraudulent identities.
- Ensure that the person successfully completes all mandated assurance activities for the relevant IP level prior to bestowing them an identity at that level.
- Only provide attributes to RPs with the consent of the person.
- Ensure that evidence used for UiTC verification activities are less than a year one and have not expired.
- Ensure that any IdP-assigned identifier allocated to the identity is permanent and not re-allocated to any other (future) identity.
- Ensure that a person can easily move their identity, at level, to a different accredited IdP at any time.
- Ensure that a person can securely view and manage their identity (changes to their information is to be configuration controlled).
- If using algorithmic matching, be able to show that the algorithmic matching software is of sufficient quality to reliably match real world photo identity documents showing normal wear and of normal age, or restrict the use of the algorithmic matching to documents (such as passports) that make clean, high quality digital images available.
- Ensure that if an authentication credential is lost, the person is able to disable or remove it from their identity.
- Ensure that if an authentication credential is lost, the person is able to disable or remove it from their identity.

The IdP **SHOULD**:

- Never lock out a Subscriber from their identity.
- If a person loses control of their identity account to a malicious third party they can reclaim their identity without sharing any secrets with the IdP. For example, the IdP should be able to restore the identity on the IdP to a point earlier in time if the person has provided sufficient proof that they are the true owner of the account.

- Include identity proofing processes for victims of identity crime to validate their identity (potentially by using the Commonwealth Victims Certificate or other appropriate evidence) and be reallocated an authentication credential.

3.2 Identity Proofing Level 1 (IP1)

Identity Proofing Level 1 provides low confidence in the accuracy or legitimacy of a claimed identity and is intended for transactions where no verification is required, but the parties desire a continuing conversation (eg provision of common general service such as obtain store card or personalise a user experience, or establish a discussion forum). It should be noted that within the TDIF at IP1 pseudonymity is possible, but not anonymity.

The IdP **MUST** address Identity Proofing Objective 1 by ensuring the person's identity is unique in context.

3.3 Identity Proofing Level 2 (IP2)

Identity Proofing Level 2 provides medium confidence in the claimed identity and is intended for moderate risk, moderate value services where fraud will have moderate consequences (eg. provision of utility services). It should be noted that at IP2 there is no requirement for facial binding to the claimed identity and that neither anonymous nor pseudonymous identities are supported.

The IdP **MUST** address Identity Proofing Objective 1 by ensuring the person's identity is unique in context.

The IdP **MUST** address Identity Proofing Objective 2 by ensuring the person's identity attributes are EITHER:

- Source verified using a CoI or Photo ID document OR
- Technically verified from a Photo ID document, OR
- Visually verified against a CoI or Photo ID document.

The IdP **MUST** address Identity Proofing Objective 4 by verifying the person's name as being used in the community by EITHER:

- Source verification of one UiTC document, OR
- A CPC by EITHER:
  - A paper–based visual check of 3 documents each from a different source, OR
  - An electronic check of at least, 3 distinct data points (ie. transactions).

The IdP **MUST** address Identity Proofing Objective 5 by ensuring the person's identity is not known to be fraudulent by confirming it is not listed in the IdPs list of known fraudulent identities or recorded on the Fact of Death File.

3.4 Identity Proofing Level 3 (IP3)

Identity Proofing Level 3 provides high confidence in the claimed identity and is intended for services with a major risk of serious consequences from fraud (eg. provision of common government services such as issuing licences, access cards, or undertaking financial exchanges). It should be noted that facial binding to the person's claimed identity is required.

The IdP **MUST** address Identity Proofing Objective 1 by ensuring the person's identity is unique in context.

The IdP **MUST** address Identity Proofing Objective 2 by ensuring the person's identity attributes are:

- Source verified using a CoI document, AND EITHER
  - Source verified using a Photo ID document, OR
  - Technically verified from a Photo ID document, OR
  - Visually verified against a CoI or Photo ID document.

The IdP **MUST** address Identity Proofing Objective 3 by binding the person's facial image using their core attribute set which were verified from the Photo ID document, by EITHER:

- Source verification, OR
- Technical verification, OR
- Visual verification, OR
- An Alternative binding process, in which the referee:

- Has been identity proofed to IP3, AND
- Uses either a physical ('wet') signature, or a CL3 credential or approved digital signature to endorse their attestation, AND
- Has proven, via a verified document, a relationship to the person, OR
- Is an authorised to witness a Statutory Declaration under Commonwealth law.

The IdP **MUST** address Identity Proofing Objective 4 by verifying the person's name as being used in the community by EITHER:

- Source verification of one UiTC document, OR
- A CPC by EITHER:
  - A paper–based visual check of 3 documents each from a different source. One must date less than 1 year prior, one must date between 1 and 3 years prior and one must date over 3 years prior to the time of proofing, OR
  - An electronic check of at least, 3 distinct data points (ie. transactions). One must date less than 1 year prior, one must date between 1 and 3 years prior and one must date over 3 years prior to the time of proofing.

The IdP **MUST** address Identity Proofing Objective 5 by ensuring the person's identity is not known to be fraudulent by confirming it is not listed in the IdPs list of known fraudulent identities or recorded on the Fact of Death File.

The IdP **MUST** also:

- Use secure image capture and liveness detection measures, to ensure that the entity presenting is a real person, as part of the image capture and face verification process when face images are source or technically verified.
- Ensure that Visual Verification is not used for visually matching the person to the Photo ID if either source or technical verification of the document is feasible.
- Comply with the *Trust Framework: Privacy Requirements* for the collection and use of biometrics.
- Where visual verification method is used for visually matching the person to the Photo ID, ensure that operators are able to match the person's face with the biometric image of the Photo ID document with reasonable accuracy.

- Where both visual verification of document details and facial matching is performed, ensure they are able to demonstrate reasonable processes and security controls are in place to preserve the integrity of the process.

Where both visual verification of document details and facial matching is performed, the IdP **SHOULD** ensure a manual, in-person inspection of the physical security features of the document.

3.5 Identity Proofing Level 4 (IP4)

Identity Proofing Level 4 provides very high confidence in the claimed identity is intended for services where extreme consequences arise from fraudulent verifications. (eg. provision of trusted government credentials such as passports, secure access, etc, or to proof 'trusted' roles such as privileged positions). It should be noted that both facial binding to the person's claimed identity and an in-person interview are required.

The IdP **MUST** address Identity Proofing Objective 1 by ensuring the person's identity is unique in context.

The IdP **MUST** address Identity Proofing Objective 2 by ensuring the person's identity attributes are:

- Source verified using a CoI document, AND EITHER
    - Source verified using a Photo ID document, OR
    - Technically verified from a Photo ID document.

The IdP **MUST** address Identity Proofing Objective 3 by binding the person's facial image using their identity attributes which were verified from the Photo ID document, by:

- Visual verification at an in-person interview, AND EITHER
    - Source verification, OR
    - Technical verification.

The IdP **MUST** address Identity Proofing Objective 4 by verifying the person's name as being used in the community by EITHER:

- Source verification of two UiTC documents, OR
- A CPC by EITHER:
  - A paper–based visual check of 3 documents each from a different source. One must date less than 1 year prior, one must date between 3 and 5 years prior and one must date over 5 years prior to the time of proofing, OR
  - An electronic check of at least, 3 distinct data points (ie. transactions). One must date less than 1 year prior, one must date between 3 and 5 years prior and one must date over 5 years prior to the time of proofing.

The IdP **MUST** address Identity Proofing Objective 5 by ensuring the person's identity is not known to be fraudulent by confirming it is not listed in the IdPs list of known fraudulent identities or recorded on the Fact of Death File.

The IdP **MUST** also:

- Use secure image capture and liveness detection measures, to ensure that the entity presenting is a real person, as part of the image capture and face verification process when face images are source or technically verified.
- Ensure that Visual Verification method is not used for visually matching the person to the Photo ID if either Source or Technical verification of the document is feasible.
- Comply with the *Trust Framework: Privacy Requirements* for the collection and use of biometrics.
- Where Visual Verification method is used for visually matching the person to their Photo ID, ensure that operators are able to match the person's face with the biometric image of the Photo ID document with reasonable accuracy.
- Where both visual verification of document details and facial matching is performed, ensure they are able to demonstrate reasonable processes and security controls are in place to preserve the integrity of the process.
- Ensure that EoI used by the person to support their claimed identity:
  - Is presented by the person as part of an in-person interview with the IdP (prior to completion of the proofing).
  - Are original documents (electronic footprint check excepted).
  - Is visually verified as part of that interview.

Where both visual verification of document details and facial matching is performed, the IdP **SHOULD** ensure a manual, in-person inspection of the physical security features of the document.

3.6 "Step-Up" between IP levels

The IdP **MUST**:

- Ensure that the Step-Up identity proofing process achieves all the requirements of the higher proofing level.
- Ensure that a person can prove ownership of their existing identity by authenticating to the same authentication level as the existing proofing level prior to commencing the process (eg. an IP2 identity can only commence the process if its owner (i.e. the person) can authenticate to the appropriate Authentication Credential Level).
- Use Source Verification to re-verify any applicable CoI or Photo ID document that has been previously presented.
- Re-validate that the claimed identity is not known to be fraudulent by verifying it is not listed in the IdPs list of known fraudulent identities or recorded on the Fact of Death File.

The IdP **SHOULD NOT** Step-Up an identity that has not been used within the previous 13 months.

The IdP **MAY** choose to step-up a person to a higher proofing level without repeating checks that have already been undertaken at the lower proofing levels. For example, a person with an IP2 identity based on an online, source verified check of a driver's licence (Photo ID document, but with no facial check) and a Medicare card (UitC), will need to present a CoI document, and would need to re-present their driver's licence (Photo ID document) to have their face bound to the identity. In addition to visually verifying the facial image, the IdP will need to be satisfied that the Photo ID document is the same as was presented previously, or re-check the details of the Photo ID document and also conduct a fraudulent identity check if it hasn't been performed within the last month. The Medicare card however would not need to be re-presented.

4 Identity proofing guidance

4.1 Community footprint check

A CFC is a check associated with UiTC documents that provide historical evidence of the identity operating in the community over time and, as per all UiTC verification activities, can only be undertaken after the person's name has been verified. A CFC is used as an alternative option when the person does not provide evidence that can be verified at an electronic authoritative source.

The CFC can either be undertaken as a Visual verification of physical credentials or an electronic (on-line) check of non-documentary identity data held in a repository that provides reasonable confidence that it cannot be modified after the fact and is accessible by the IdP. Examples of electronic data sources include tax records, health records, postal records, telephone records, and credit references or banking and other financial records. A CFC does not include checking a person's social media activity.

During the IdPs accreditation activities, the Trust Framework Accreditation Authority will review and endorse any proposed electronic repository that an IdP plans to utilise for CFC activities. As such, it should be noted that different IdPs may have access to different approved repositories.

Regardless of whether the evidence is physical or electronic an CFC verifies that person's verified name can be reasonably matched to the provided evidence or the data held in the repository. To do this it will be necessary to use other key biographical details obtained in the identity proofing process to ensure the accuracy of the verification activities. A combination of Name and Date of Birth or address is usually sufficient, although other attributes (such as a phone number or email address, or identifiers) may also need to be used.

Each of the respective levels has different requirements for proofing the verified name is being used in the community over time. In essence, the higher the level being proofed the longer the period that the evidence supporting the identity needs to be verified as operating in the community in order to provide the required additional confidence. These periods range from:

- At IP 1 – not applicable.
- At IP2 – no stipulation.
- At IP3:
  - 1 must date less than one year prior AND
  - 1 must data between one and three years prior, AND
  - 1 must date over three years prior to the time of proofing.
- At IP4:
  - 1 must date less than one year prior AND
  - 1 must data between three and five years prior AND
  - 1 must date over five years prior to the time of proofing.

An electronic CFC tests data points in the applicable repositories data (i.e. transactions or interactions) in order to validate a history of transactions supporting a claimed identity (eg. the use of a credit card, not just the issuance of the card). These data points may be from a common transaction history or a number of independent sources depending on the proofing level sought.

4.2 Alternative binding

An Alternate Binding, is an attestation by a verified referee who has either a provable relationship with the person, or has a professional status such that they can reliably attest to the identity of the person. An Alternative Binding is only used as an alternative to providing a Photo ID document for binding the person's verified identity attributes to their facial image at IP3[4].

There is no stipulation on the form or format of an attestation[5], rather it depends on what the IdP can process, either electronic or physical. However, within it the referee documents:

- The person's core attribute set (including identifiers and basis of attesting details, eg. provable relationship or professional status, as applicable) that enables them to attest to the fact that these attributes are bound to the person that is being proofed.

[4] Alternative Binding cannot be used at IP4

[5] It is expected to be similar in form to that of a Statutory Declaration

- That they have sighted the person at an in-person interview.
- Their (referee) name, contact details, including as applicable their identifier.
- Acknowledgement of the penalties for making a false declarations[6].
- Formally signs the attestation, either physically or digitally.

If digitally signed an accredited Public Key Infrastructure (eg. Gatekeeper) should be used. If an electronic form is used the referee has to use a CL3 credential to prove their identity to the IdP as part of submitting the form.

If the referee is claiming a provable relationship to the person, documentation proving the relationship is appended to the attestation. This documentation may include approved CoI or Linking documents, approved Powers of Attorney, or guardianship, or similar documentation demonstrating family or community relationship in excess of 3 years. This relationship may be proven via documentary evidence (eg. a marriage or birth certificate confirmed through source verification) or by other reliable means if available.

If the referee is making the attestation on the basis of professional status, they must provide or have provided evidence of that professional status, and there must be reasonable cause to believe that they have retained their professional status. Professional status includes the list of authorised witnesses to statutory declarations as defined by Commonwealth law and tribal elders designated by the Department of Human Services.

4.3 Recording, verifying and matching identity attributes

Guidance for the recording of names is provided in the AGD Improving the integrity of identity data: Recording of a name to establish identity; Better Practice Guidelines for Commonwealth Agencies – June 2011.

Guidance for improving the integrity of identity data to enable data matching is provided in the AGD Improving the Integrity of Identity Data; Data Matching: Better Practice Guidelines 2009.

[6] These should be as per those contained in a Statutory Declaration

4.4 Collecting and verifying facial images

Facial images are collected by the IdP to match with biometric data held by Photo ID document issuers using the FVS, or by algorithmic matching, or visually by a trained Assisted Digital Operator.

In order to match the facial image with the FVS the IdP will need to connect to and comply with the FVS standards and applicable formal arrangement in relation to the data sharing arrangements. This service is provided by the Department of Home Affairs and all queries in relation to the FVS should be addressed to them.

If using visual matching by operators or during in-person interviews, the IdP operators need to be trained and competent to perform facial identity verification. The T*rust Framework: Fraud Control Requirements* provides guidance in relation to training requirements and suitable training options. It is important that processes are established that are sufficiently robust to allow operators to reject poor matches and worn, faded, aged or identifiably fraudulent images.

4.5 Self-asserted attributes

Where contact information, such as email address or telephone number, is self-asserted, it is recommended that the IdP check that the attribute is under the control of the person by:

- Validating the email address through an email confirmation method.
- Validating the phone number through a one-time PIN, QR code, App or SMS confirmation method.
- Validating a physical address through the physical delivery of a one-time code or similar mechanism (e.g. QR code).

If the IdP already has an established relationship with the person and they are confident that the self-asserted details are correct then they could use their existing data.

4.6 Transitional arrangements

The Trust Framework and identity federation will take several months before their benefits are fully realised. During this period the Trust Accreditation Authority may authorise alternate approaches. This may include a temporary increase of additional forms of acceptable identity evidence, or approval of lower security documents (such as student ID cards), or possibly additional controls to mitigate the potential fraud risk. Where an IdP is unable to access a required authoritative source they are to discuss the options with the Trust Framework Accreditation Authority and seek confirmation for any proposed transitional arrangements prior to utilising them in their identity proofing activities.

5 References

The following information sources have been used in developing this document.

1. Attorney-General's Department, 2012, 'Improving the integrity of identity data: recording of a name to establish identity - better practice guidelines for Commonwealth Agencies', Australian Government. https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/recording-a-name-to-establish-an-identity.pdf
2. Attorney-General's Department, 2016, 'National Identity Proofing Guidelines (NIPGs), Australian Government. https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.PDF
3. Bradner, S. 1997, 'Key words for use in RFCs to Indicate Requirements Level' (Requests for Comment 2119), Internet Engineering Task Force, Switzerland. https://tools.ietf.org/html/rfc2119
4. Department of Internal Affairs, 2009, 'Evidence of Identity Standard', New Zealand Government. https://www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index
5. Digital Transformation Agency, 2009, 'National e-Authentication Framework', Australian Government. https://www.dta.gov.au/standard/design-guides/authentication-frameworks/national-e-authentication-framework/
6. National Institute of Standards and Technology, 2017, 'Digital Identity Guidelines (NIST SP 800-63)', Government of the United States. https://pages.nist.gov/800-63-3/
7. Canadian Government Digital Id And Authentication Council Of Canada, August 2016, 'Pan-canadian Trust Framework – Identity Establishment Conformance Criteria', Canadian Government Digital Id And Authentication Council Of Canada
8. United Kingdom Cabinet Office, 2012, 'Good Practice Guide -Requirements for secure delivery of online public services (GPG 43)', United Kingdom Cabinet Office.https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services
9. United Kingdom Cabinet Office, 2014, 'Good Practice Guide - Identity proofing and verification of an individual (GPG 45)', United Kingdom Cabinet Office. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individu

Annex A: relationship between TDIF IPs and other identity proofing approaches

This document is intended to align with national and international standards and guidelines that define levels of identity proofing. The table below provides a snapshot of mappings to various national and international identity proofing standards and guidelines. This is not meant to imply that there is a direct correlation between the IPs in this document and the levels in those standards. It is considered that the IP criteria in this document fulfils the criteria as described in those standards.

Table 2: relationship between this document and other IdP standards and guidelines

TDIF Identity Proofing Requirements		**IP 1**	**IP 2**	**IP 3**	**IP 4**
National Identity Proofing Guidelines		LOA 1	LOA 2	LOA 3	LOA 4
National e-Authentication Framework	LOA 0	LOA 1	LOA 2	LOA 3	LOA 4
National Institute of Standards and Technology Special Publication 800-63 (Digital Identity Guidelines)		IAL 1	IAL 1	IAL 2	IAL 3
United Kingdom Cabinet Office Good Practice Guide (GPG 45) – Validating and verifying the identity of an individual		Level 1	Level 2	Level 3	Level 4
United Kingdom Cabinet Office Good Practice Guide (GPG 43) – Requirements for secure delivery of online public services	Level 0	Level 1	Level 2	Level 3	
New Zealand Government Evident of Identity Standard		Low	Moderate	Moderate	High
Digital ID and Authentication Council of Canada (DIACC)		IAL 1	IAL 2	IAL 3	IAL 4
ISO/IEC TS 29003 – Information technology – security techniques – identity proofing		LOA 1	LOA 2	LOA 3	LOA 4
ISO/IEC 29115:2013 – Information technology – security techniques – entity authentication assurance framework		LOA 1	LOA 2	LOA 3	LOA 4

Australian Government standards

National Identity Proofing Guidelines

The NIPGs are designed for use primarily by those Commonwealth and state and territory government agencies which issue documents and credentials that are most commonly used as evidence of a person's identity (identity documents). This document aligns with the NIPGs. Noting this, there are some key differences between the two documents which are listed below. This document:

- Sets standards with no exemption policy.
- Only allows the use of documents that can be checked using the Document Verification Service to be used for identity verification purposes.
- Requires a biometric binding process to link a person to their identity attributes.
- Allows the use of an Australian visa as both a CoI and Binding document where biometric data is available.

Annex B: Approved Identity Sources

The following lists documents and sources currently approved for use within the Trust Framework for the purpose of Identity Proofing. This list may be modified from time to time as new sources become available, or existing sources are found to be unreliable. Production IdPs will be notified of such changes as required.

Note that while documents may be used for multiple purposes (e.g. a Photo ID document or a Linking document may also be used as a Use in Community document), the same particular document may not be used more than once for any given category. Thus, an Immicard can be used as either Commencement, Photo ID or Use in Community, but may only be used for one of these purposes during an identity proofing check.

A common example is the use of a passport and a driver's licence, where one can be used as Photo ID (usually the passport) while the other is used for Use in Community.

In all cases, regardless of verification method, the IdP must be satisfied that a particular identity source can be reasonably securely verified. This may mean rejecting a source if, for example, it is known that the 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).

Abbreviations

S – Source Verifiable – can be checked via an electronic source (DVS, FVS etc.).

T – Technically Verifiable – can be checked using intrinsic technical features (ePassport).

V – Visually Verifiable – has security features enabling checking by a human operator**.**

748 **Table 3:** approved CoI documents

Category type: Commencement of Identity	**Notes:** Shows identity creation within Australia	**Checks**
Australian issued Birth Certificate		S, (V[7])
Australian issued Citizenship Certificate		S, (V[8])
International Passport (Visa)	Note that the Visa is the component that can be checked with DVS - there is a subtle difference between the Visa (commencement) and the passport (UiC, Photo ID), although they both associate to the same document	S
DFAT issued Certificate of Identity	DFAT issued Certificate of Identity	S
DFAT issued UN Travel documents	DFAT issued UN Travel documents	S

749 **Table 4:** approved Photo ID documents

Category type: Photo ID document	**Notes:** A secure document with a clear photo of the person	**Checks**
Australian issued Drivers Licence		S, V
Australian Passport		S, V, T
Immicard		S, V
International Passport	(see visa note under commencement)	V, T
Titre de Voyage		S, V
Citizenship Certificate	Only if it has a photo within ten years	S, V
Indigenous Community Card[9]		
Proof-of-Age card	State approved	V
Shooting/Firearms Licence		V

[7] Commencement documents **MUST** be checked to source. IdPs **MAY** conduct visual checks as an additional security measure.

[8] As per the footnote above.

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

Category type: Photo ID document	**Notes:** A secure document with a clear photo of the person	**Checks**
Working with children/Vulnerable card		V
Aviation Security ID		V
Maritime Security ID		V
Australian Defence Highly Trusted Token		V, T
Police Force Officer ID		V
Prison release certificate	(where these include a photo)	V
Alternate Binding Record	See 'Alternate Binding' section for details	n/a

750 **Table 5:** approved UitC documents

Category type: Use in the Community	**Notes:** Shows the use of an identity within the community	**Checks**
DHS Concession card	Refer to https://www.humanservices.gov.au/individuals/subjects/concession-and-health-care-cards	S, V
Medicare		S, V
Citizenship Certificate	Citizenship by Descent Certificate of Naturalisation Certificate of Registration Certificate of Australian Citizenship Declaratory Certificate of Citizenship Evidentiary Certificate Extract from Register of Births (Citizenship by Descent)	S, V

751 **Table 6:** community footprint checks

Category type: Community Footprint Check	**Notes:** Shows the use of an identity within the community over time	**Checks**
Bank or Financial institution card, passbook, statement		S, V

Category type: Community Footprint Check	**Notes:** Shows the use of an identity within the community over time	**Checks**
Credit Card		S, V
Education Certificate		V
Certified academic transcript from an Australian University		S, V
Mortgage Papers		V
Veterans Affairs card		V
Tenancy Agreement		V
Motor Vehicle Registration		V
Rates Notice		V
Any document listed in other category	If not used elsewhere	S, V or T
Electoral Roll		S
Banking or other Financial Records	A history of financial transactions	S
Tax Records	A history of taxation payments	S
Health Records	A history of usage of health services	S
Postal Records	A history of postal deliveries	S
Telephone Records	A history of phone usage	S

752 **Table 7:** approved Linking documents

Category type: Linking document	**Notes:** Shows or supports a name change	**Checks**
Marriage Certificate		S, V
Change of Name Certificate		S, V
Foreign Passport		S, V

Category type: Linking document	**Notes:** Shows or supports a name change	**Checks**
Decree Nisi/Decree Absolute divorce papers		V
Deed poll papers (change-of-name)		V
Commonwealth (ID) Victims Certificate		V

753