Australian Government
Digital Transformation Agency

# Identity Proofing Requirements

Trusted Digital Identity Framework
August 2018, version 1.07

dta

## Digital Transformation Agency

## Licence

## Use of the Coat of Arms

## Conventions

The key words "**MUST**", "**MUST NOT**", "**SHOULD**", "**SHOULD NOT**", and "**MAY**" in this document are to be interpreted as described in the current version of the *Trusted Digital Identity Framework: Overview and Glossary*.

## Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you have difficulties 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

The Trust Framework Accreditation Authority has reviewed and endorsed this document for release.

## 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 – 1.05 | Mar 2018 | AJH & GJF | Updates based on internal review and merged online and offline identity proofing requirements into the one document (including use of referee process and in-person Id proofing). |
| 1.06 | Mar 2018 | SJP | Converted to new template and updated based on internal review. |
| 1.07 | Aug 2018 | GJF | Updated based on stakeholder feedback. |

# Contents

# 1 Introduction

Establishing confidence in an individual'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 private sector and other non-government organisations. The objective of identity proofing is to verify an individual's identity information to obtain a reusable digital identity.

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 *TDIF: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives 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:

- Proofing requirements for individuals who may be unable to consent (children, incapacitated, etc) in order to have their identity verified by an IdP.
- Identity proofing non-person entities.
- End-to-end identity management processes such as identity refresh or identity retirement.

This document comprises four parts:

- Part 1: provides an introduction and context.
- Part 2: describes the TDIF identity proofing objectives, identity proofing levels, Evidence of Identity (EoI) categories and verification methods.
- Part 3: describes the TDIF Identity Proofing Requirements to be met by IdPs.
- Part 4: provides guidance on how to implement these requirements.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- 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 an individual. The assurance reflected by each level is derived from the veracity of the claims about an individual's identity, through the evidence provided, to meet some or all of the identity proofing objectives of:

- Context uniqueness.
- Legitimacy.
- Operation within the community.
- Binding between the individual and the evidence of identity.
- 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 and genuine.
- The claimed identity exists and accepted as operating in the real world.
- The claimed identity has been verified as being associated with, and bound to the individual supplying the identity evidence.
- 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 and likely risks to be considered are described in the *TDIF: Risk Management Requirements*.

These *TDIF: 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 an individual 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. The key differences between the TDIF IPs and NIPGs is also 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 an individual in the provision of their services.

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

- **Confirm uniqueness of the identity in the IdP context (Uniqueness Objective)** to ensure that digital identities 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 need to uniquely identify the individual in all contexts.[1]
- **Confirm the claimed identity is legitimate (Legitimacy Objective)** to ensure the identity has been genuinely created as well as confirming that there is continuity in an individual's identity attributes where there have been changes. Increased confidence in the legitimacy of an individual's identity is achieved through verifying Commencement of Identity (CoI) 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.
- **Confirm the operation of the identity in the community over time (Operation Objective)** to provide additional confidence that an individual'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 individual's identity has a history and reduces the risk that it is fraudulent.

[1] Uniqueness does not preclude the ability for a person to create multiple digital identities with the one IdP or to create multiple digital identities across multiple IdPs.

- **Confirm the binding between identity attributes and the individual claiming the identity (Binding Objective)** to provide confidence that the individual's identity confirmed through Legitimacy and Operation objectives is not only legitimate, but that the individual currently claiming the identity is its legitimate holder. This reduces the opportunity for identity fraud. The TDIF relies on facial binding to reduce this risk.
- **Confirm the identity is not known to be used fraudulently (Anti-fraud Objective)** 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) by combining or undertaking more extensive checks in relation to each objective so the higher (more confidence) identity proofing levels can be defined.

Table 1 below outlines for each of the respective identity proofing levels the applicable[2] identity proofing objectives, the EoI required and examples of relevant use.

[2] Unless a transitional arrangement is in effect. See 'Transitional Arrangements' (Section 4.6) for further details.

**Table 1**: Identity proofing levels

| | IP 1 | IP2 | IP 3 | IP 4 |
|---|---|---|---|---|
| **Confidence** | **Low** | **Medium** | **High** | **Very High** |
| **Identity proofing objectives to be met** | Claimed identity meets:<br>• Uniqueness | Claimed identity meets:<br>• Uniqueness<br>• Legitimacy<br>• Operation<br>• Anti-Fraud | Claimed identity meets:<br>• Uniqueness<br>• Legitimacy<br>• Operation<br>• Binding<br>• Anti-Fraud | Claimed identity meets:<br>• Uniqueness<br>• Legitimacy<br>• Operation<br>• Binding<br>• Anti-Fraud |
| **EoI requirements** | NIL | 1 CoI, OR<br>1 Photo ID<br>+<br>1 UiTC, OR<br>3 documents each from different sources, OR<br>3 electronic data points from 1 source<br>+<br>Linking documents (where necessary) | 1 CoI<br>+<br>1 UiTC, OR<br>3 documents each from different sources, OR<br>3 electronic data points from 1 source<br>+<br>1 Photo ID, OR<br>1 Alternative Binding<br>+<br>Linking documents (where necessary) | 1 CoI<br>+<br>1 UiTC, OR<br>3 documents each from different sources, OR<br>3 electronic data points from 1 source<br>+<br>1 Photo ID AND Interview,<br>+<br>Linking documents (where necessary) |
| **Intended use** | For transactions where no verification is required, but the parties desire a continuing conversation (eg. post in a discussion forum) | For low risk or services where fraud will have minor consequences (eg. provision utility services) | For moderate risk or services where fraud will have moderate consequences (eg. access to common government services, or undertaking financial transactions). | For high risk or services where major consequences arise from fraudulent verifications. (eg. for secure access or 'trusted'/ 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 an individual and, as such, it relies heavily on the identity evidence presented. This evidence may be physical or digital/electronic credentials[3] 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 an individual's identity falls into five fundamental categories:

- **Commencement of Identity (CoI)** is a government issued document:
    - Which anchors an individual's identity and provides evidence of its establishment or creation in Australia.
    - Which is the product of high integrity business processes which create and issue the 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 individual claiming the identity.
    - Where the biometric image of the individual 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[4], or by the visual inspection of a trained operator.
- **Use in the Community (UitC)** is a verifiable document issued by a reliable source which:

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

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

    - 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, or court, 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 authoritative sources (eg. DVS).
- **Alternative Binding (Identity Attestation)** is:
    - An attestation by a verified referee who has either a provable relationship with the individual claiming an identity or has a professional status such that they can reliably attest to the identity of the individual.
    - Endorsement of an image of the individual, 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 individual 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 an individual'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 issuer's revocation processes (e.g. a stolen passport may still pass technical verification).
- **Visual Verification** – the act of a trained operator[5] 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 individual.
- **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.

[5] TDIF Fraud Control Requirements provides further guidance.

## 2.5 Identity attributes

Within the identity federation an identity is roughly equivalent to a persona, verified or self-asserted, that an individual 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 an individual within a given context.

The *TDIF: Attribute Profile* details the attribute sets used within the TDIF. Of particular importance for this document is the 'core identity attributes[6]', which includes:

- Given name(s)
- Family Name
- Date of Birth (DoB)

[6] NB. These must be collected and verified at IP2 and above

# 3 Identity Service Provider requirements

## 3.1 General requirements

The IdP **MUST**:

- Verify an individual's EoI to an authoritative source where it is possible.
- As applicable[7], record the following identity attributes:
  - The core identity attributes provided for the Legitimacy Objective.
  - All variations of the core identity attributes provided on EoI documents.
  - For each Identity Proofing Objective, the EoI used[8] (as per Annex B) and:
    - The EoI issuer.
    - The name(s) recorded on the EoI.
    - DoB if recorded on the EoI.
    - Date of Issue/Expiry.
    - Identifier(s) recorded on the EoI.
    - The verification method used for that EoI (S, T, V).
    - Date and time the EoI was verified.
  - The individual's asserted contact attributes[9], which may include address, phone and email, etc (as provided or used in the claims).
  - The individual's asserted preferred name(s).
  - Identity proofing level achieved.
  - Date and time the identity was proofed.
  - Credential details/type and individual's unique IdP identifier allocated.
- Where the individual's core identity attributes are not consistent between presented EoI (once naming and DoB conventions are considered), verify the attributes collected via a Linking document and record the EoI attributes as per above.
- For each verification event (eg. create, update, etc), record the EoI used in the process, as per above, and the outcome/results.
- Validate at least 1 of the claimed contact details.

[7] NB. At IP1 a claimant can be pseudonymous. In addition, some EoI may not contain all nominated attributes (eg. DoB, Identifier, Date Issued/Expired, etc)

[8] Where the document is verifiable at source, e.g. using DVS/FVS, the IdP SHOULD record the data items that are required to be sent to the source for that document type

[9] NB. Where contact attributes are used to manage credentials they SHOULD be verified.

- Ensure that, where visual verification is undertaken, that original EoI documents are used.
- Comply with the *TDIF: Privacy Requirements* for the collection and use of biometrics.
- Ensure that where an identity verification or validation process is unsuccessful, the following is undertaken:
  - The issue, including the reason it failed, is recorded in the IdP's system.
  - Advise the individual of the outcome and provide them with guidance, based on the reason for the error, to resolve the issue.
  - Advise the individual 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[10].
- On a monthly basis re-verify the individual's identity attributes are not known to be fraudulent by confirming the individual's identity is not recorded on the Fact of Death File or listed in the IdPs list of known fraudulent identities.
- Ensure that the individual successfully completes all mandated assurance activities for the relevant IP level prior to bestowing them an identity at that level.
- Ensure attributes are only provided to RPs with the consent of the individual[11].
- Ensure that evidence used for UiTC verification activities has 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 an individual can easily move their identity, at level, to a different accredited IdP at any time.
- Ensure that an individual can securely view and manage their identity (changes to their information is to be configuration controlled).
- Ensure that if verified attributes are changed that they are re-verified.
- 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

[10] Unless a transitional arrangement is in effect. See 'Transitional Arrangements' (Section 4.6) for further details.

[11] Consent **MUST** be collected from the individual before the attributes are disclosed to a Relying Party. Depending on the transmission path, consent **MAY** be collected by an intermediary on behalf of the IdP (e.g. an Identity Exchange). If no intermediary is used then consent **MUST** be collected by the IdP prior to disclosure.

algorithmic matching to documents (such as passports) that make clean, high quality digital images available.

- Ensure that if an authentication credential is lost, the individual is able to disable or remove it from their identity.
- Issue to proofed individuals accredited credentials[12] as per the Permissible Combinations of Credential Level and Identity Proofing Level[13]:

| | | **Authentication Credential Level** | | |
|---|---|---|---|---|
| | | **CL1** | **CL2** | **CL3** |
| **Required Identity Proofing Level** | **IP1** | Allowed | Allowed | Allowed |
| | **IP2** | NO | Allowed | Allowed |
| | **IP3** | NO | Allowed | Allowed |
| | **IP4** | NO | NO | Allowed |

- Where it asserts attributes to RPs, be able to provide both the IP and CL attributes that were used in the authentication of the individual (refer to TDIF Attribute Profile).
- When facial images are source or technically verified use presentation attack detection (PAD) technologies (e.g. secure image capture and liveness detection measures), to ensure that the entity being proofed is a real person.
- Ensure that Visual Verification is not used for visually matching the individual to the Photo ID if either source or technical verification of the document is feasible[14].
- Where Visual Verification method is used for visually matching the individual to the Photo ID, ensure that operators are trained, and competent, in facial identification testing to improve the accuracy of matching the individual's face with the biometric image of the Photo ID document. (See the *TDIF: Fraud Control Requirements* for further information).
- 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.

[12] In accordance with the *TDIF: Authentication Credential Requirements*

[13] NB. The credential may be provided directly by the IdP or via a third-party Credential Provider.

[14] For IP4 activities, an adjudication process for occasions where Source and/or Technical verification fails is to be proposed that will be assessed by the Accreditation Authority.

- Establish and maintain an Identity Service Provider Operations Manual, which at a minimum includes the following information:
  - Roles and responsibilities of IdP and associated staff (i.e. IdP operators).
  - Processes, procedures and workflows used to support the IdP's identity management functions (i.e. access control, storage, backup, archive and retrieval, disaster recovery, business continuity and records management)
  - Procedures and workflows used to register, verify, authenticate and validate the identity of a person who interacts with the IdP.
  - Procedures used which describe how IdP operators manage a cyber security incident[15]
  - Processes, procedures and workflows used to support system logging and the types of events captured.
  - Details of all interactions between the IdP and a CSP.
- Ensure that all information included in the Identity Service Provider Operations Manual is consistent with information included in the IdPs protective security documentation.

The IdP **SHOULD**:

- Not lock out an individual from their identity without their express permission or strong suspicion of fraud.
- Ensure a secure account recovery process is implemented so that if an individual loses control of their identity account to a third party they are able to reclaim it. For example, the IdP should be able to restore the identity on the IdP to a point earlier in time if the individual 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[16] or other appropriate evidence) and be registered.
- Where both visual verification of document details and facial matching is performed ensure a manual, in-person inspection of the physical security features of the document.

[15] 'Cyber security incident' is defined in the *TDIF: Overview and Glossary*.

[16] Refer to https://www.homeaffairs.gov.au/about/crime/identity-security/victims-of-commonwealth-crime

## 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 Uniqueness Objective by ensuring the individual'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 Uniqueness Objective by ensuring the individual's identity is unique in context.

The IdP **MUST** address Identity Proofing Legitimacy Objective by ensuring all the individual's core 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 Operation Objective by verifying the individual's name as being used in the community by EITHER:

- Source verification of one UiTC document, OR
- A CFC 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 Anti-Fraud Objective by ensuring the individual's identity is not known to be fraudulent by confirming it is not listed in the IdPs list of known fraudulent identities or 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 individual's claimed identity is required.

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

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

- Source verified using a CoI[17] 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 Operation Objective by verifying the individual's name as being used in the community by EITHER:

- Source verification of one UiTC document, OR
- A CFC 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

[17] Unless a transitional arrangement is in effect. See 'Transitional Arrangements' (Section 4.6) for further details.

    - 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 Binding Objective by binding the individual's facial image, presented during the proofing process, and their core identity attributes, which were verified to achieve the Legitimacy Objective, 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 EITHER
    - Has proven, via a verified document, a relationship to the individual, OR
    - Is authorised to witness a Statutory Declaration under law.

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

## 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 individual's claimed identity and an in-person interview are required.

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

The IdP **MUST** address Identity Proofing Legitimacy Objective by ensuring the individual'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 Operation Objective by verifying the individual's name as being used in the community by EITHER:

- Source verification of one UiTC document, OR
- A CFC 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 Binding Objective by binding the individual's facial image, presented during the proofing process, and their core identity attributes, which were verified to achieve the Legitimacy Objective, by:

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

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

The IdP **MUST** also:

- Ensure that EoI used by the individual to support their claimed identity:
  - Is presented by the individual 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.

## 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 an individual can prove ownership of their existing identity by authenticating with their credential to their account 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 **MAY** choose to step-up an individual to a higher proofing level without repeating checks that have already been undertaken at the lower proofing levels where the requirements have been met. For example, an individual 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 could 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. 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 individual's name has been verified. A CFC is used as an alternative option when the person does not provide evidence that can be verified via an approved UiTC document.

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 an individual'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 a CFC verifies that the individual's 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 may be sufficient, although other attributes (such as a phone number or email address, or EoI identifiers) may also need to be used.

Each of the respective IP 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 date 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 date 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 (identity attestation)

An Alternative binding, is an attestation by a verified referee who has either a provable relationship with the individual, 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 individual's verified identity attributes to their facial image at IP3[18].

There is no stipulation on the form or format of an attestation[19], rather it depends on what the IdP can process, either electronic or physical. However, within it the referee documents:

- The individual's core identity attributes (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 individual that is being proofed.

[18] Alternative Binding cannot be used at IP4

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

- That they have sighted the individual at an in-person interview.
- Their (referee) name, contact details, including as applicable their identifier.
- Acknowledgement of the penalties for making false declarations[20].
- Formally signs the attestation, either physically or digitally.

An accredited Public Key Infrastructure (e.g. Gatekeeper) should be used if information is digitally signed. 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 individual, 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. 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 law and tribal elders designated by the Department of Human Services.

## 4.3 Recording, verifying and matching identity attributes

The individual's name is as recorded on the EoI used to meet the Legitimacy Objective.

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*.

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

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*.

## 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 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 *TDIF: 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 individual 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[21].
- Validating a physical address through the physical delivery of a one-time code or similar mechanism (e.g. QR code).

[21] NB. Such validation should consider the risk that the device or delivery mechanism has been tampered with (e.g. redirect, SMishing, SIM swap, call forwarding) and include appropriate mitigations

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

## 4.6 Transitional arrangements

It's likely to take several months (if not years) before the benefits of the identity federation are fully realised. During the initial establishment of the identity federation from time to time, the Trust Framework Accreditation Authority may authorise temporary and alternative measures that can be implemented by IdPs. These measures, or transitional arrangements, may conflict with existing TDIF requirements. These measures may, for example, 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 a potential fraud risk. These measures are used to overcome a limitation within the identity federation and are enacted for a specific time. IdPs can choose whether or not to implement a transitional arrangement or follow the TDIF requirements as specified.

Transitional arrangements may be cancelled by the Trust Framework Accreditation Authority at any time once they've been enacted or extended beyond their original validity period if they are still needed. Relevant TDIF requirements need to be met once transitional arrangements are no longer in effect.

### 4.6.1 Transitional arrangements currently in effect

From 1 August 2018 through 30 December 2018, an Australian Passport **MAY** be used as a COI document. This change will not impact the current IP 2 requirements but will impact the current IP 3 and IP 4 requirements.

For IP 3:

- To satisfy the Identity Proofing Legitimacy Objective, the Australian Passport (interim CoI document) **MUST** be source verified AND an alternative Photo ID document **MUST** be either source verified, technically verified or visually verified.

- The Australian Passport **MAY** also be used to satisfy the Identity Proofing Binding Objective as currently defined in section 3.4.

- All other IP 3 requirements remain the same and **MUST** be met.

For IP 4:

- To satisfy the Identity Proofing Legitimacy Objective, the Australian Passport (interim CoI document) **MUST** be source verified AND an alternative Photo ID document **MUST** be either source verified or technically verified.

- The Australian Passport **MAY** also be used to satisfy the Identity Proofing Binding Objective as currently defined in section 3.5.

- All other IP 4 requirements remain the same and **MUST** be met.

### 4.6.2 Transitional arrangements no longer in effect

n/a

# 5 References

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

1. Attorney-General's Department, 2011, '*Improving the integrity of identity data: recording of a name to establish identity – better practice guidelines for Commonwealth Agencies'*, Australian Government. https://www.homeaffairs.gov.au/crime/Documents/recording-name-establish-identity.pdf

2. Attorney-General's Department, 2016, '*National Identity Proofing Guidelines (NIPGs)*, Australian Government. https://www.homeaffairs.gov.au/about/crime/identity-security/guidelines-and-standards

3. Department of Internal Affairs, 2009, '*Evidence of Identity Standard'*, New Zealand Government. https://www.dia.govt.nz/Resource-material-Evidence-of-Identity-Standard-Index

4. Digital Transformation Agency, 2009, '*National e-Authentication Framework'*, Australian Government. https://www.dta.gov.au/standard/design-guides/authentication-frameworks/national-e-authentication-framework/

5. 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/

6. 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

7. 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-individual

# 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 3:** relationship between this document and other IdP standards and guidelines

| TDIF Identity Proofing Requirements | | IP 1 | IP 2 | IP 3 | IP 4 |
|---|---|---|---|---|---|
| Digital ID and Authentication Council of Canada (DIACC) | | IAL 1 | IAL 2 | IAL 3 | IAL 4 |
| ISO/IEC 29115:2013 – Information technology – security techniques – entity authentication assurance framework | | LOA 1 | LOA 2 | LOA 3 | LOA 4 |
| ISO/IEC TS 29003 – Information technology – security techniques – identity proofing | | LOA 1 | LOA 2 | LOA 3 | LOA 4 |
| National e-Authentication Framework | LOA 0 | LOA 1 | LOA 2 | LOA 3 | LOA 4 |
| National Identity Proofing Guidelines | | 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 |
| New Zealand Government Evident of Identity Standard | | Low | Moderate | Moderate | High |
| 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 | |

## Key differences between TDIF IPs and NIPGs

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 accreditation requirements for IdPs to meet.
- Does not include an exemption policy.
- Supports transitional arrangements.
- Only allows the use of COI documents that can be checked using the Document Verification Service to be used for identity verification purposes.
- Requires a biometric binding process to link an individual to their identity attributes.
- Allows the use of an Australian Visa as either a CoI or Binding document where biometric data is available.

# Annex B: Approved Evidence of Identity

Unless a transitional arrangement is in effect[22], the following lists documents and validation options currently approved for use within the TDIF for the purpose of Identity Proofing. This list may be modified from time to time as required (ie. as new sources become available, or are agreed). 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 the Community document), the same particular document may not be used for more than one ID Proofing objective. Thus, for example, 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.

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

In all cases, regardless of verification method, the IdP must be satisfied that a particular identity source can be reasonably and 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, approved CFC repositories, etc.).

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

[22] See 'Transitional Arrangements' (Section 4.6) for further details.

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

Table 4: approved CoI documents

| **Category type:** Commencement of Identity | **Notes:** Shows identity creation within Australia | **Checks** |
|---|---|---|
| Australian issued Birth Certificate | NB. For the interim an Australian Passport may be utilised as a COI document at IP3 | S, (V[23]) |
| Australian issued Citizenship Certificate | Refer to https://www.dvs.gov.au/Pages/default.aspx | S, (V[23]) |
| Travel Visa (supported by foreign Passport) | Note the DVS uses the passport details to check for a current Australian Visa – 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 |

Table 5: approved Photo ID documents

| **Category type:** Photo ID document | **Notes:** A secure document with a clear photo of the individual | **Checks** |
|---|---|---|
| Australian Passport | | S, T, V |
| Australian State/Territory issued Drivers Licence | | S, V |
| Immicard | Note FVS utilises the photo attached to the record that the Immicard is linked to | S, T, V |
| Foreign Passport | Note FVS utilises the photo attached to the Visa record that the passport is linked to | T, V |
| Titre de Voyage/ DFAT issued UN Travel documents | | S, V |
| Australian issued Citizenship Certificate | Only if issued within the last ten years[24] | S |

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

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

| **Category type:** Photo ID document | **Notes:** A secure document with a clear photo of the individual | **Checks** |
|---|---|---|
| Indigenous Community Card[25] | Use this EoI to provide confirmation of identity for Aboriginal or Torres Strait Islanders who have not provided other identity documents | V |
| Proof-of-Age card[26] | State issued and KeyPass | V |
| Shooting/Firearms Licence | | V |
| Working with children/Vulnerable card | | V |
| Aviation Security ID | | V |
| Maritime Security ID | | V |
| Australian Defence Highly Trusted Token | | T, V |
| Police Force Officer ID | | V |
| PrisonerID | (where these include a photo) | V |
| Alternate Binding Record | See 'Alternate Binding' section for details | n/a |

## Table 6: 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 |
| Any document listed in COI or Photo ID document categories | If not used elsewhere | S, T or V |

[25] 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.

[26] NB. State names vary but they have the same fundamental intent eg. 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

Table 7: 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 |
| 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, T or V |
| 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 |

Table 8: approved Linking documents

| **Category type:** Linking document | **Notes:** Shows or supports a name change | **Checks** |
|---|---|---|
| Marriage Certificate | | S, V |
| Birth Certificate | Where history of name changes are listed | S, V |
| Change of Name Certificate | | S, V |
| Decree Nisi/Decree Absolute divorce papers | | V |
| Deed poll papers (change-of-name) | | V |
| Commonwealth (ID) Victims Certificate | | V |