Australian Government
Digital Transformation Agency

Identity Proofing Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

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	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

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

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

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'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). 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 objective of identity proofing is to proof an individual's identity information to obtain a reusable digital identity. This document comprises two parts:

- Part 1: describes the TDIF Identity Proofing Requirements to be met by IdPs.
- Part 2: 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.

There are six identity proofing objectives: uniqueness, legitimacy, operation within the community, biometric binding, determining linkages between changed identity attributes and checks that an identity is not fraudulent. These objectives are met at different levels of assurance across the four Identity Proofing (IP) Levels. Increasing levels of assurance are achieved through the proofing of evidence of identity.

- At IP 1 anonymous or pseudonymous identity is supported and can occur using an online channel or in-person at an IdP's shopfront. Typically, IP1 transactions are information related. Contact details, not biographical information, are used to enrol with an IdP.

- At IP 2, an IdP collects biographical attributes and document identifiers, which it verifies with the relevant Authoritative Source. The biographical attributes and document identifiers of two identity documents, a Binding document and a Use in the Community (UitC) document verified with the Document Issuer.
- At IP 3 the IdP collects biographical information printed on or associated with a Commencement of Identity document, a Binding document and a UitC document which are verified at source with the Document Issuer. A biometric match between the source photograph on the Binding document and the document owner is conducted. Where a UitC document is not available, a social footprint check validated with Document Issuers may be conducted.
- At IP 4 all the requirements for IP 3 apply. IP3 processes are confirmed through an in-person interview and a police check of the individual is required.

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

These Identity Proofing Requirements are supported by the companion *Trust Framework: Authentication Credential Requirements* which sets out authentication credential management requirements. Together these TDIF documents enable an individual, should they choose to do so, to undergo a single identity verification process and manage a single authentication credential to enable them to access a range of digital services.

2 Part one: Identity proofing requirements

2.1 Identity proofing objectives

An identity proofing process tests the veracity of claims an individual makes regarding their identity. IdPs **MUST** undertake this process on the basis of evidence provided by the individual with a view to achieving the following objectives:

Table 1: identity proofing objectives

Objective	Description	How to/Example
Unique in context	Confirming that an individual can be distinguished from others in the intended context.	For all IP levels in this document, the IdP MUST ensure that there are no duplicate records and that documents issued to a single holder is not used by more than one identity.
Legitimate	Confirming with Authoritative Sources that the claimed identity has been legitimately created in Australia, either through birth or immigration.	For IP 3, IP 4 and step-up, the IdP verifies information on the individual's Commencement of Identity document or record using the DVS.
Operational	Verifying with authoritative or reliable sources that a claimed identity exists and has been in use in the Australian Community over time.	For IP 2 through IP 4 and step-up, the IdP to verifies information contained in the individual's Use in the Community identity documents using the DVS or another issuing body as approved by the Trust Framework Accreditation Authority or does a social footprint check using independent authoritative sources.
Bound	Anchoring an individual to a claimed identity through biometric matching to an authoritative source.	For IP 3, IP 4 and step-up, the IdP matches the person's facial image with the image held by the Authoritative Sources for Binding Documents (i.e. DFAT, DOHA or RTAs) using the FVS.

Objective	Description	How to/Example
Linked	Confirming that, where biographical attributes have changed, the new attributes relate to the same individual.	Where biographical identity attributes don't match e.g. due to change of name or date of birth, the IdP MUST ensure that the changed attribute is linked to the previous attribute through a Commencement of Identity agency-issued linking document using the DVS
Not Fraudulent	Confirming that a claimed identity is neither fraudulent nor fictitious.	The IdP checks whether the identity has been reported as stolen or appears on an internal list of known fraudulent identities and the Identity Exchange(s) conducts a check of its stolen and known fraudulent identities database.

2.2 Identity proofing levels

2.2.1 Identity Proofing Level 1 (IP 1)

The following criteria **MUST** be met in order to satisfy IP 1:

- The pseudonymous identity is unique in context.
- Contact details such as email address and mobile phone number are self-asserted by the individual and validated by an IdP.
- Where attributes are stored, an IdP **MUST** establish there are no other records with the same pseudonymous identity and that the email address is not associated with any other active records.

2.2.2 Identity Proofing Level 2 (IP 2)

The following criteria **MUST** be met in order to satisfy IP 2:

- Identity is unique in context and known to be operating within the community.
- Identity is not recorded on a list of known fraudulent identities.
- Attributes are verified with Authoritative Sources, and Identity attributes associated with all other sources are validated at source for:
    - **ONE Binding** Document taken from Table 3 below, verified with an Authoritative Source.

- **ONE Use in the Community** document validated at source or a **Social Footprint** check as described in the *Evidence of Identity: Social Footprint check* section of this Standard.
- If different names appear on the documents (once naming conventions are considered) then a **Linking** document **MUST** be used to verify the link between the former name and the current name.
- Pseudonymous identities are not supported.
- Note: the documents and credentials are each in the same name(s) when accounting for various naming conventions used across Government issued identity documents. For example, '*Joe H Bloggs'* on one document may be considered the same as '*Joe Henry Bloggs'* on another document.

- IdP performs sole claimant check to establish there are no other records with the same set of attributes.
- Contact details such as email address or mobile phone number are self-asserted by the individual and validated by the IdP.

2.2.3 Identity Proofing Level 3 (IP 3)

The following criteria **MUST** be met in order to satisfy IP 3:

- Identity is unique in context, it exists legitimately, is accepted and operating in the community and is strongly bound to an individual.
- Identity is not recorded on a list of known fraudulent identities.
- Attributes are verified with Authoritative Sources, and Identity attributes associated with all other sources are validated at source for:
  - **ONE Binding** Document taken from Table 3 below, verified with an Authoritative Source.
  - **ONE Commencement of Identity** document taken from Table 3 below, verified with an Authoritative Source.
  - Note: the documents and credentials are each in the same name(s) when accounting for various naming conventions used across Government issued identity documents,
  - **ONE Use in the Community** document validated at source or a **Social Footprint** check as described in the *Evidence of Identity: Social Footprint check* section of this document.

    - Note: If different names appear on the documents (once naming conventions are considered) then a **Linking** document **MUST** be used to verify the link between the former name and the current name.
    - Pseudonymous identities are not supported.
- Real-time matching of the individual's facial image (including liveness detection and presentation attack mitigation) with the image held by the Binding Document Issuer to bind the individual to their identity information. This **MUST** be done using the FVS or through equivalent biometric matching to the information contained on the NFC chip.
- Binding between the individual and the facial image only occurs after the individual's identity attributes have been successfully verified at source with the Document Issuer.
- Anonymous and pseudonymous identities are not supported.
- Sole claimant check by the IdP to establish that it holds no other records with the same set of identity attributes.
- Contact details such as email address or mobile phone number are self-asserted by the individual and validated by the IdP.

2.2.4 Identity Proofing Step-up (IP 2 to IP 3 only)

Step-up identity proofing occurs when an individual has satisfied IP 2 and now requires their digital identity to be verified to IP 3. An individual will be required to undergo a full IP3 identity proofing if they cannot meet the criteria below.

The following criteria **MUST** be met in order to satisfy IP2 to IP3 Step-up:

- **ONE Commencement of Identity** document taken from Table 3 below, verified with an Authoritative Source.
- Note: the documents and credentials are each in the same name(s) when accounting for various naming conventions used across Government issued identity documents.
- If different names appear on the documents (once naming conventions are considered) then a **Linking** document **MUST** be used to verify the link between the former name and the current name.
- Real-time matching of the individual's facial image (including liveness detection and presentation attack mitigation) with the image held by the Binding Document

Issuer to bind the individual to their identity information. This **MUST** be done using the FVS or through equivalent biometric matching to the information contained on the NFC chip.

- Binding between the individual and the facial image only occurs after the individual's identity attributes have been successfully verified at source with the Document Issuer.

2.2.5 Identity Proofing Level 4 (IP 4)

The following criteria **MUST** be met in order to satisfy IP 4

- All requirements for IP 3.
- The individual brings their supporting documentation to an in-person interview with the IdP.
- A police and background check.

2.2.6 Summary of identity proofing requirements

Table 2: summary of identity proofing requirements

Requirement	IP1	IP2	Step up to IP3	IP3	IP4
Documents		1 x Binding 1 x UitC or SFC	1 x CoI 1 x Binding	1 x CoI 1 x Binding 1 x UitC or SFC	
Anonymous or pseudonymous identities	x				
Identity is unique in context	x	x		x	x
Identity exists legitimately		x		x	x
Operating in the community		x		x	x
Bound to an individual			x	x	x

Requirement	IP1	IP2	Step up to IP3	IP3	IP4
Document verification		x	x	x	x
Biometric verification			x	x	x
Sole Claimant check		x		x	x
Contact Details	self-asserted validated by IdP				
In person check					x

2.3 Evidence of Identity

The documents that **MAY** be used for the enrolment and proofing of digital identities fall into four categories:

- A **Commencement of Identity** (CoI) document is a government issued document:
  - which anchors an identity and provides evidence of its establishment or creation in Australia.
  - Is the product of high integrity business processes which create and issue the document and manage it throughout its lifecycle.
  - With attributes contained in or printed on the document able to be verified through the DVS.
  - Which is listed as a Commencement of Identity document in *Table 3: Evidence of Identity* below (indicated with an 'x').
- A **Binding** document is a government issued document:
  - With attributes printed on the document able to be verified through the DVS.
  - Where the photo of the individual printed on the document or stored in the Document Issuer database can be verified (in real time using liveness detection) through the FVS or where the image contained on the NFC chip can be matched biometrically to the document owner (in real time using liveness detection).

- The document is listed as a **Binding** document in *Table 3: Evidence of Identity* below (indicated with an 'x').

- **A Linking** document is a government issued document:
  - Which provides a link between two names resulting from a name change. e.g. change of name certificate, marriage certificate, or in some cases a birth certificate.
  - With attributes printed on the document that can be verified through the DVS.
  - The document is listed as a **Linking** document in *Table 3: Evidence of Identity* below (indicated with an 'x').
- A **Use in the Community** (UitC) is a government issued document or a document issued by a reliable and independent source.
- A **Social Footprint** check (SFC) is used to confirm whether an identity has been operating in the community over time. For this check, a minimum of three distinct data points evidencing a history of transactions over a minimum five-year period **MUST** be validated. These data points may be from a common transaction history or a number of independent sources, however all such sources should be reliable and there should be reasonable confidence that they cannot be modified after the fact. Examples of such data sources include tax records, health records, postal records, telephone records, and banking and other financial records. Such evidence should provide evidence of activity over time (e.g. an account transaction, not just the creation of an account). A SFC **MUST NOT** include access to an individual's social media accounts or information.

All evidence of identity **MUST** be verified at source. All facial images must be bound to evidence of identity documents through biometric matching for IP3 and above.

Note: Documents can only be used once in the identity proofing process. E.g. a Driver Licence that is used as a **Binding** document can't also be used as a **Use in the Community document**. However, where a document is identified as both a **CoI** and a **Binding** document in Table 3, it **MAY** be used as both, provided that: the **CoI** issuing agency holds a biometric quality facial photograph which is under 10 years old that is linked to the **CoI** document.

Table 3: evidence of identity documents

Government issued document	Commencement of Identity	Binding (photo ID)	Linking	Use in the Community
Australian Birth Certificate	x		x	
Australian Passport		x		
Australian electronic visa record supported by a foreign passport	x	x		
ImmiCard	x	x		
Australian Citizenship Certificate, including any of the following: Citizenship by Descent Extract from Register of Births (Citizenship by Descent) Certificate of Naturalisation Certificate of Registration Certificate of Australian Citizenship Declaratory Certificate of Citizenship Evidentiary Certificate	x			
Australian Change of Name Certificate			x	x
Australian State or Territory issued Driver Licence (including Learner's Permits or Learner Licences)		x		x
Australian Marriage Certificate			x	x
Medicare Card				x
DFAT-issued Convention Travel Document (Titre de Voyage)		x		
DFAT-issued Certificate of Identity		x		x

2.4 Identity attributes

For the purposes of this document, an IdP **MUST** verify the following attributes if they are associated with documents from Authoritative Sources using the DVS. An IdP **MUST** validate the following attributes if they are associated with documents issued by other Document Issuers.

Once a document has been validated or verified, the following attributes **MUST** be stored by an IdP as part of IP 2, Step-up, IP 3 and IP 4 identity proofing:

- **Full name** (Given name/s and family name) as printed or otherwise incorporated in or on every document that is verified.
    - If different names appear on the documents, a historical connection between the names **MUST** be confirmed using a linking document. The IdP **MUST** collect all name changes as it becomes aware of them and each name change **MUST** be verified through the DVS.
    - If more than one individual is listed on a certificate e.g. a marriage certificate, the attributes of both individuals **MUST** be verified.
- **Date of Birth** as displayed on, or linked to documents being verified. If identity documents display different dates of birth, the IdP **SHOULD** record all dates of birth as listed on verified identity documents.
- **Document identifiers** as displayed on the document (e.g. type of document, Issuing authority, birth certificate number, passport number, document date of issue etc).
- **Contact details** such as an email address and mobile phone number **MUST** be collected and validated to establish a link between the individual and the device they are using to perform the identity proofing check.
    - The email address is to be validated through an email confirmation method.
    - The mobile phone number is to be validated through a one-time PIN, QR code or SMS confirmation method.

For the purposes of this document, the following attributes **MUST** be collected and verified by an IdP as part of Step-up, IP 3 and IP 4 identity proofing, but **MUST NOT** be stored:

- **Biometric data** such as a facial image, as used in an Australian passport, or an Immicard or visa.

- Once collected and verified, biometric data **MUST** be immediately and permanently deleted by the IdP.

For the purposes of this Standard, the following additional attributes **MAY** be collected:

- Residential address
- Mailing address

3 Part two: Guidance

3.1 Recording and verifying identity attributes

3.1.1 Recording names: variations, multiple names and verified evidence

Names are rarely unique and there are many possible variations on any single name. Further complexity is introduced when foreign names are transliterated or otherwise anglicised.

For IP 2 through IP 4 and step up identity proofing:

- Identity documents **MAY** be considered to be in the same name(s) when accounting for various naming conventions used across Government issued identity documents and credentials. For example, 'Joe H Bloggs' on one document **MAY** be considered the same as 'Joe Henry Bloggs' on another document. More detail on naming conventions can be found in: AGD's *Improving the integrity of identity data: recording of a name to establish identity - Better Practice Guidelines for Commonwealth Agencies*.
- For some cultural groups an individual may only have one name. This **MUST NOT** preclude completion of the identity proofing process.
- Aliases or preferred names **MAY** also be requested from individuals; however, they are considered unverified identity attributes. An alias or preferred name **MAY** be used by an IdP to offer a personalised service to the individual, however they **MUST NOT** be asserted as a verified attribute to Relying Party services.
- If identity documents are in different names (once naming conventions are considered), a link between the names **MUST** be established. Subject to naming conventions, if different names appear on the documents, a historical connection between the names must be confirmed. The IdP **MUST** collect all name changes as they become aware of them and the name change **MUST** be verified through the DVS.
    - Identity proofing **MUST** cease if the historical connection between the two verified names cannot be established and the individual **MUST** be redirected to an offline channel to complete the process.

- The connection between the names **MUST** be supported by a Linking document as per Table 3: Evidence of Identity.
- If identity proofing occurs using identity documents in different names, the IdP **MUST** record the name listed on the most recent RBDM or DOHA issued certificate - i.e. latest issued Change of Name, Marriage Certificate, visa or Citizenship Certificate etc. E.g. After a marriage between Joe A and Jane B, the following variations on family name **MUST** be accepted by the IdP: "Joe A", "Joe B", "Joe A-B" or "Joe B-A".

3.1.2 Recording Dates of Birth

Discrepancies in date of birth on identity documents may occur when:

- A person is not aware of their exact date of birth.
- A person, born in a country using a different calendar, has their date of birth incorrectly converted to a date in the Gregorian Calendar.
- A data entry error occurs because the date format used in a foreign document differs from the Australian date format.
- Different approaches have been used by Australian Government agencies to assigning or recording date of birth.

If identity proofing occurs using identity documents with different dates of birth, the IdP **MUST** record all dates of birth as they are recorded on verified documents. The authoritative date of birth should be the date of birth recorded on the most recent Commencement of Identity document

3.1.3 Verifying or validating biographical attributes and document identifiers

IdPs **MUST** verify attributes associated with Authoritative Sources using the DVS and validate attributes associated with other documents with the Document Issuer.

Where an identity verification or validation process is unsuccessful, the IdP **MUST** advise the individual and provide them with guidance based on the reason for the error e.g. if document information has been entered incorrectly, the IdP **MUST** advise the individual to check the information they have entered.

The IdP **MUST** set the number of acceptable unsuccessful verification or validation attempts based on the individual agency risk mitigation processes of Document Issuers.

Where the IdP identifies that an identity verification or validation cannot be successfully completed, they **MUST**:

- Record the issue in their internal system.
- Inform the individual that the digital identity proofing process has ceased and that they will be transitioned to an offline channel to complete the process.
- Where the enrolment request came through the exchange, inform the Identity Exchange that the digital identity proofing process has ceased.
    - The Identity Exchange **SHOULD** advise the Relying Party service of the issue.
    - The IdP should guide the individual to an offline channel (telephony, shopfront) to complete the identity proofing process.

3.2 Verifying Biometric Data

3.2.1 Collecting and verifying facial images

Facial images are collected by the IdP to match with biometric data held by Binding Document Issuers.

The IdP **MUST**:

- Comply with FVS requirements for facial image collection to ensure that biometric data matches are enabled.
- Where a solution using image on the NFC chip, ensure that the technology, match quality and thresholds are at a minimum equal to those used for FVS biometric matching.
- Encrypt facial images upon collection using Australian Signals Directorate Approved Cryptographic Algorithms.
- Use liveness detection checks when collecting facial images to ensure that the entity presenting is a real person.

- Guard against presentation attacks when facial images are collected, to ensure that the person presenting is the legitimate owner of the Binding Document being checked.
- Immediately delete collected facial images once binding has occurred.

The IdP **MUST NOT:**

- Store verified facial images or biometric data collected and matched.

3.2.2 Self-Asserted Attributes

The IdP **MUST** validate email addresses and telephone numbers through an email confirmation method for email addresses and through a one-time PIN, QR code or SMS confirmation method for mobile phones.

3.3 Transitional Arrangements

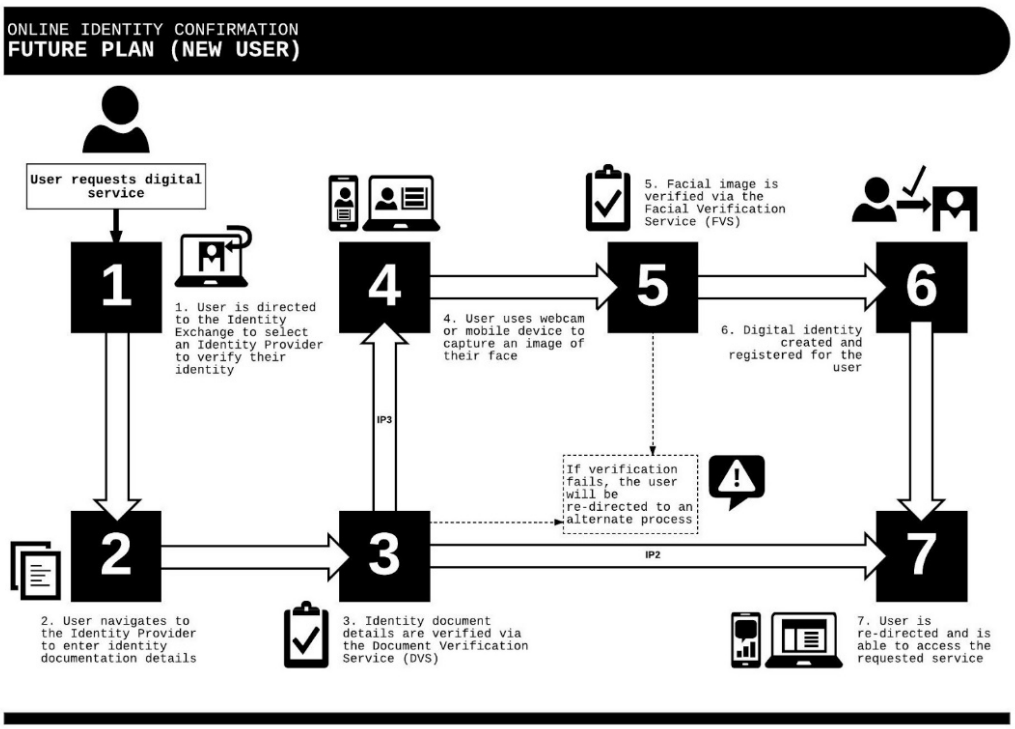
The Trust Framework Accreditation Authority may authorise alternate processes while government services such as the Facial Verification Service are being finalised.

3.4 Digital Identity Proofing Process

3.4.1 Overview

This document establishes four IdP levels, each of which provides Relying Parties with an increasing level of assurance that an individual is who they claim to be. Level 1 is the lowest IP level, Level 4 is the highest. Increasing levels of assurance will be achieved through the verification of data through Authoritative Sources. An indicative overview of the identity proofing process for IP2-IP4 can be found below at figure 1.

Figure 1: indicative overview of the identity proofing process



3.4.2 Identity proofing - future plan (new user)

Step 1. User is directed to an Identity Exchange to select an IdP to verify their identity.
Step 2. User navigates to the IdP to enter identity documentation details.
Step 3. Identity document details are verified via the Document Verification Service (DVS).
Step 4. User uses webcam or mobile device to capture an image of their face.
Step 5. Facial image is verified via the Facial Verification Service (FVS) or using NFC chip data.
Step 6. Digital identity created and registered for the user.
Step 7. User is redirected and is able to access the requested service.

If verification fails at either Step 3 or Step 5, the user will be re-directed to an offline channel process.

4 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. Pan-canadian Trust Framework – Identity Establishment Conformance Criteria, Canadian Government Digital Id And Authentication Council Of Canada, August 2016
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 this document and other identity standards

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 5: relationship between this document and other IdP standards and guidelines

TDIF	NIPGs	NeAF	NIST SP 800-63	GPG-45	RSDOPS	NLZ EoIS	Canada DIACC	ISO 29003	ISO 29115
n/a	n/a	LOA 0	n/a	n/a	Level 0	Nil	n/a	n/a	n/a
IP 1	LOA 1	LOA 1	IAL 1	Level 1	Level 1	Low	IAL 1	LOA 1	LOA 1
IP 2	LOA 2	LOA 2	IAL 1	Level 2	Level 2	Moderate	IAL 2	LOA 2	LOA 2
IP 3	LOA 3	LOA 3	IAL 2	Level 3	Level 3	Moderate	IAL 3	LOA 3	LOA 3
IP 4	LOA 4	LOA 4	IAL 3	Level 4	n/a	High	IAL 4	LOA 4	LOA 4

4.1 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.
- Requires use of Document Verification Service to check that a document with certain attributes has been issued.

- 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.