

NATIONAL
IDENTITY
PROOFING
GUIDELINES



**National Identity
Proofing Guidelines**



IDENTITY SECURITY

ISBN: 978-1-925290-64-6 (print)
ISBN: 978-1-925290-65-3 (online)

© Commonwealth of Australia 2016

All material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

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 (www.itsanhonour.gov.au).

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Attorney-General's Department
3-5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au

Contents

Chapter 1 — Introduction

1.1	Background	1
1.2	Purpose	1
1.3	Who should use these Guidelines?	3
1.4	Scope	3
1.5	Conventions	4
1.6	Abbreviations and definitions	4
1.7	Implementation	5
1.8	Review of the Guidelines	5
1.9	Relationship to international standards	6

Chapter 2 — Overview of Identity Proofing

2.1	What is identity?	7
2.2	Identity proofing objectives	7
2.3	Levels of assurance	9

Chapter 3 — Choice of Level of Assurance

3.1	Undertaking a risk assessment	12
3.2	Reliance on known customers	13
3.3	Choosing a level of assurance	13
3.4	Privacy	14
3.5	Other considerations	14

Chapter 4 — Identity Proofing Objectives and Requirements at each Level of Assurance

4.1	Minimum Identity Proofing Requirements	15
-----	--	----

Chapter 5 — People unable to meet minimum identity proofing requirements	19
5.1 Exceptions processes to confirm a claimed identity	19
5.2 Verifying the identity of children	20
Chapter 6 — Assessing Applications	21
6.1 Recording identity proofing outcomes	21
6.2 Identifying fraudulent applications	21
Chapter 7 — Monitoring and Evaluation	23
7.1 Evaluation of identity proofing processes	23
Appendix A	24
Glossary	24
Appendix B	27
Suggested evidence types and weightings	27
Appendix C	30
Guidance on use of third party identity service providers	30

Chapter 1

Introduction

1.1 Background

- 1.1.1 Establishing confidence in a person's identity is a critical starting point for delivering a range of government services and benefits, as it is for many transactions conducted by the private sector and other non-government organisations.
- 1.1.2 Identity proofing has traditionally been conducted in 'face to face' settings. Our increasingly digital economy, in which more and more people are looking to transact online at times most convenient to them, creates a range of challenges to these traditional approaches. However it also presents a range of potential opportunities through the use of new and emerging technologies.
- 1.1.3 Australians rely heavily on documents produced by a range of government agencies to help verify their identities. Rather than a single identity card, the backbone of Australia's system of identities—our identity infrastructure—is provided by around 20 government agencies that manage over 50 million core identity documents. Australia's identity infrastructure is also supported by many businesses and non-government organisations that issue documents or other services used as evidence of identity, such as banks and universities.
- 1.1.4 Identity crime is amongst the most prevalent of all types of crime in Australia. Each year around 4-5 per cent of Australians (estimated at around 750,000 to 937,000 people) experience identity crime resulting in a financial loss. However the true extent of identity crime is likely to be unknown, as a considerable proportion of incidents go unreported. The Australian Crime Commission has rated identity crime as a key enabler of serious and organised crime, which in turn costs Australia around \$15 billion annually.
- 1.1.5 Identity proofing is an important part of efforts to prevent identity crime. It is also critical to promote the trust and confidence in identities, particularly online, which will be a key enabler of Australia's digital economy into the future.

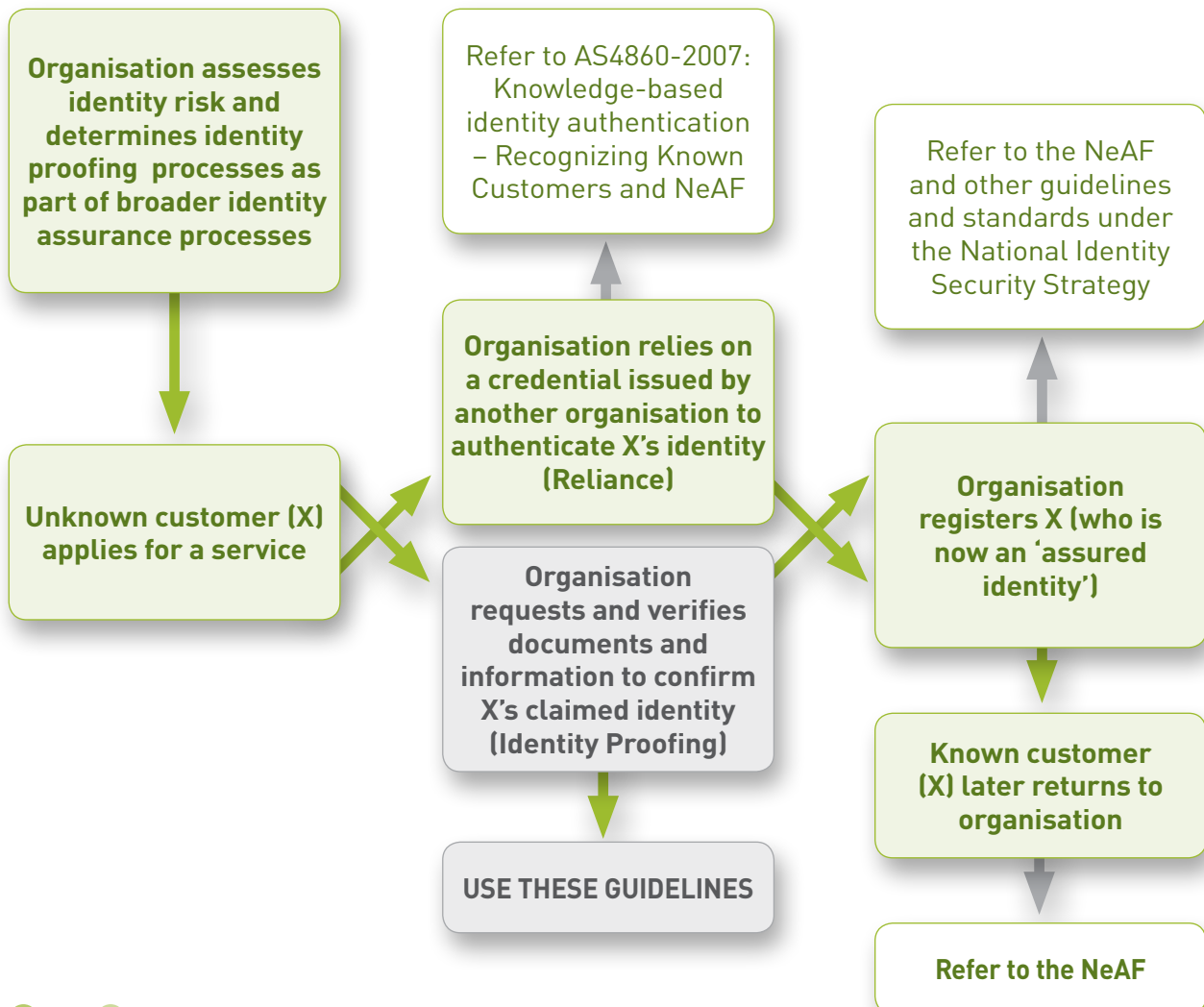
1.2 Purpose

- 1.2.1 The purpose of these Guidelines is to strengthen identity proofing processes and increase trust through a standardised and transparent national approach.
- 1.2.2 To fulfil this purpose, these Guidelines provide a set of recommended processes and requirements for identity proofing—the process by which organisations seek to verify a person's identity by collecting information about the person and confirming it with relevant authoritative sources.¹ Identity proofing is rarely done in absolute terms—rather to a specified or understood level of assurance.
- 1.2.3 The Guidelines replace the identity proofing elements of the 2007 Gold Standard Enrolment Framework (GSEF) developed under the National Identity Security Strategy. The GSEF has been incorporated into requirements and processes for the highest level of assurance contained within these Guidelines.

¹ Information would generally be collected directly from the individual concerned, but may be from another person who is authorised to act on their behalf, such as a legal guardian.

- 1.2.4 Identity proofing is an integral part of the broader identity assurance approach outlined in the National e-Authentication Framework (NeAF) and should be considered in the context of broader identity authentication and management processes. The three phases of an authentication process are:
1. **Enrolment phase:** application and initiation, identity proofing, record-keeping/recording and registration.
 2. **Credential management phase:** all processes relevant to the lifecycle management, such as creation, issuance of a credential, binding of an individual to a credential, activation, storage, revocation, renewal and/or replacement and record keeping.
 3. **Entity authentication phase:** consists of the entity's use of its credential to attest to its identity to a relying party.
- 1.2.5 Guidance on when to use these Guidelines as part of a broader identity assurance approach is illustrated in **Figure 1**.

Figure 1: Decision tree to inform appropriate use of these Guidelines



1.3 Who should use these Guidelines?

- 1.3.1. These Guidelines 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').²
- 1.3.2. The Guidelines may also be used by other government agencies which face identity-related risks in the performance of their functions or delivery of services, if considered necessary following a risk assessment and cost benefit analysis. Identity related risks are those risks associated with incorrectly identifying a person. The consequences of incorrectly identifying a person may include:
- **Fraud risks:** a person without entitlement receiving a financial payment or other non-financial benefit as a result of a transaction (e.g. payment of a benefit or grant)
 - **Security risk:** a person gaining unauthorised access to information, facilities, goods or services, particularly those of a sensitive nature
 - **Privacy risk:** a person gaining unauthorised access to someone else's personal information
 - **Downstream risks:** a person using an identity credential or record issued or created by one organisation to commit identity crime against other organisations.
- 1.3.3. Private sector or other non-government organisations that face similar identity related risks may also choose to use these Guidelines as a better practice reference.
- 1.3.4. These Guidelines should be used by agencies or organisations looking to design new identity proofing processes or strengthen existing processes, as part of broader fraud, security, privacy and authentication and identity management processes.

1.4 Scope

- 1.4.1. The Guidelines encourage greater transparency between the government agencies which form part of Australia's national identity infrastructure. They do this by providing a common framework for categorising and understanding various identity proofing processes. They also encourage reporting on implementation by key identity document and credential issuing agencies to enable other organisations to better judge how much trust they should place in identity proofing processes of other organisations.
- 1.4.2. These Guidelines are only suitable for the identification of people, not organisations or other types of entities. They are primarily designed for identity proofing at the point of initial enrolment³ with an organisation and do not address other, non-identity related aspects of background checking (e.g. criminal histories) or eligibility (e.g. criteria such as income, residency or citizenship status).

² Key identity documents and credentials include those commonly requested as evidence of identity, regardless of whether these documents and credentials were originally issued for identity related purposes.

³ Excluding birth registration processes.

- 1.4.3 These Guidelines do not supersede or replace any legislative requirements on government agencies or other organisations to verify identity (although organisations could use these Guidelines to help implement or satisfy specific legislative requirements). However, agencies are encouraged to reference these Guidelines when reviewing and updating legislative requirements to verify identity.

1.5 Conventions

- 1.5.1 These Guidelines adopt the following conventions:
- **SHALL** indicates something that is *required* in order to meet these Guidelines.
 - **SHOULD** indicates something that is *recommended* but not required in order to meet these Guidelines (i.e. an organisation should implement these recommendations unless it is unreasonable to do so or an alternative process is used which provides an equivalent level of assurance).
 - **MAY** indicates something that is *permitted* under these Guidelines, but is not required.
 - **SHOULD NOT** indicates something that is *not recommended* under these Guidelines, unless circumstances make other approaches unfeasible.
 - **SHALL NOT** indicates something that is not permitted in order to meet the Guidelines

1.6 Abbreviations and definitions

- 1.6.1 The following abbreviations are used throughout these Guidelines:
- | | |
|-------|---|
| DIBP | Australian Government Department of Immigration and Border Protection |
| DFAT | Australian Government Department of Foreign Affairs and Trade |
| DVS | Document Verification Service |
| LoA | Level of Assurance |
| NeAF | National e-Authentication Framework |
| NISCG | National Identity Security Coordination Group |
| RBDM | (Australian) Registry of Births Deaths and Marriages |
- 1.6.2 A glossary is included at **Appendix A** to provide definitions for technical terms used in these Guidelines.

1.7 Implementation

- 1.7.1 The identity proofing requirements outlined within these Guidelines are designed to be applied on the basis of a risk assessment that takes into account identity risks to the organisation itself, other organisations and individuals. The risk assessment should also consider risks to Australia's broader national identity system in the case of issuance of identity documents or credentials.
- 1.7.2 These Guidelines can be implemented over time as agencies refine and update identity management policies, business processes, service delivery and information technology systems.
- 1.7.3 Some key identity documents, such as driver licences, are issued by each state and territory. There would be benefit in the relevant agencies in each jurisdiction collaborating nationally to undertake a risk assessment process and determining identity proofing requirements for issuance of these documents. This would help promote national consistency and avoid potential gaps that could be exploited by criminals.
- 1.7.4 Identity proofing can occur where a person is unknown to an organisation or where the organisation wishes to re-assess the person's claimed identity at a later point of time. Decisions on whether and how to implement these Guidelines to 'known customers' **SHOULD** be made by organisations on a risk management basis.
- Organisations **SHOULD** use the processes specified in these Guidelines to assess the identity of their existing customers if the original identity proofing processes are deemed insufficient based on a risk assessment and other management strategies have not been able to reduce the risk.
 - An organisation **MAY** also use the processes specified in these Guidelines to assess the identity of their existing customers on a periodic basis (for instance to check that a change of name has not been recorded through re-verification of a birth certificate with the issuing authority).

1.8 Review of the Guidelines

- 1.8.1 Given the rapidly evolving nature of techniques and tools available to assess identity, especially online, these Guidelines are designed to be reviewed on a yearly basis.

1.9 Relationship to international standards

1.9.1 These Guidelines have been designed to align with a range of existing international standards and guidelines, as outlined in **Table 1**. This is not meant to imply there is direct correlation between the identity assurance levels in these Guidelines and those in the international equivalents. Rather, these Australian Guidelines generally meet or exceed the identity proofing requirements contained in other comparable documents.

Table 1: Comparison of Australian and international identity proofing frameworks

Identity proofing framework	Level of assurance			
	1 - Low	2 - Medium	3 - High	4 - Very high
Australian National Identity Proofing Guidelines (these Guidelines)				
National e-Authentication Framework (2009)	1 - Low	2 - Medium	3 - High	4 - Very high
ISO/IEC 29115:2013 Information technology – Security techniques – Entity Authentication Assurance Framework	1 - Low	2 - Medium	3 - High	4 - Very high
United States Electronic Authentication Guidelines NIST Special Publication 800-63-2 (2013)	Level 1	Level 2	Level 3	Level 4
United Kingdom Good Practice Guide Identity Proofing and Verification of an Individual GPG No.45 Issue No. 2.2 (2013)	Level 1	Level 2	Level 3	Level 4
New Zealand Evidence of Identity Standard Version 2.0 (2009)	Low	Moderate	High	
Canadian Standard on Identity and Credential Assurance (2013)	Level 1	Level 2	Level 3	Level 4

Chapter 2

Overview of Identity Proofing

2.1 What is identity?


- 2.1.1 A person's identity is not a fixed concept; it is highly dependent on context. It is some combination of characteristics or attributes that allow a person to be uniquely distinguished from others within a specific context.
- 2.1.2 A person's identity in Australia (for the purposes of these Guidelines) is generally considered to be established at birth with the creation of a RBDM birth record that details unique information about an individual—such as name, date and place of birth. For people not born in Australia, their identity in Australia is generally established from personal details recorded on DIBP Australian immigration documents or records.
- 2.1.3 Australian citizens and permanent residents retain the right, enshrined in Australian privacy legislation, to act anonymously or pseudonymously when interacting with governments or businesses, unless: i) an organisation is required or authorised under Australian law to request identification; or ii) it is otherwise impracticable to deal with individuals who have not identified themselves.⁴

2.2 Identity proofing objectives

- 2.2.1 The veracity of claims about a person's identity is established through evidence provided to meet some or all of the following five identity proofing objectives (depending on confidence in the claimed identity required):
1. **Confirm uniqueness of the identity in the intended context** to ensure that individuals can be distinguished from one another and that the right service is delivered to the right individual. This would include a check that another person has not previously claimed ownership of the identity (i.e. there is a sole claimant), for example by checking the organisation's database for identity records with the same attributes.
 2. **Confirm the claimed identity is legitimate** to ensure the identity has not been fraudulently created (i.e. the identity is that of a real person) through evidence of commencement of identity in Australia. Where greater confidence in the claimed identity is required, this objective may also include a check that an identity has not been recorded as deceased (e.g. through the Fact of Death file).⁵

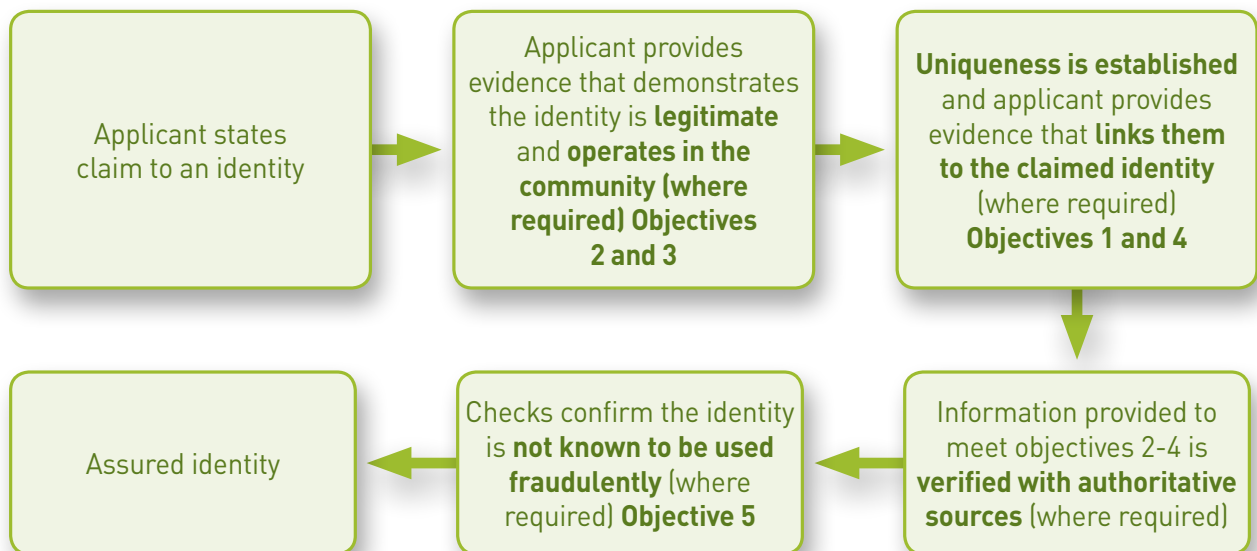
⁴ Note identity proofing would not preclude issuance of an identity credential, document or service in a preferred name (once a person's identity has been confirmed).

⁵ Note there may be legitimate reasons for registering a person who has died, such as for tax liability reasons.

- 
3. **Confirm the operation of the identity in the community over time** to provide additional confidence that an identity is legitimate in that it is being used in the community (including online where appropriate). Even where a person is able to obtain genuine identity documents in a fictitious name, it will be harder to provide evidence that the identity has been active in the community, particularly over an extended period of time and if evidence reflects the breadth of a person's life, such as:
 - Citizen: evidence that demonstrates the person's life as a citizen and any support or services they are provided by government
 - Money: evidence that demonstrates the person's financial and working life, and
 - Living: evidence that demonstrates where they live and what they consume.
 4. **Confirm the linkage between the identity and the person claiming the identity** to provide confidence that the identity confirmed through objectives 2 and 3 is not only legitimate, but that the person claiming the identity is its legitimate holder. This has traditionally been done by comparing a person's face against a photograph, although there is an increasing range of technologies that can provide alternative methods, such as comparison of a biometric captured at enrolment against a biometric previously captured by a trusted organisation.
 5. **Confirm the identity is not known to be used fraudulently** to provide additional confidence that a fraudulent (either fictitious or stolen) identity is not being used. This could be through checks against internal registers of known fraudulent identities or against 'dummy records' recorded in the system. Where possible, this could include checks against information provided by external sources, such as law enforcement agencies.

2.2.2 The role of each objective in the identity proofing process is outlined in Figure 2.

Figure 2: Overview of the identity proofing process



2.3 Levels of assurance

2.2.3 These Guidelines recognise that it will not always be necessary or appropriate to confirm a person's identity with a high degree of confidence, particularly for transactions or services that are low value or involve low levels of risk. These Guidelines therefore adopt a risk-based approach to identity proofing using varying Levels of Assurance (LoA) that can be applied commensurate with the level of risk involved in any particular context as outlined in Table 2.

2.2.4 The purpose of tiered levels of assurance is to help organisations (i.e. relying parties) understand how much trust they can place in documents and credentials issued by other organisations (noting that issuing organisations are also relying parties due to the interrelated nature of Australia's identity system).

2.2.5 These Guidelines specify two methods of processing:

- **Remote** refers to any interaction that happens where there is no in-person interaction, such as submission of an application and provision of evidence via mail, online, videoconferencing or over the phone.
- **Local** refers to a method of processing applications where an in-person interaction occurs and original evidence is physically sighted.

Table 2: Levels of assurance in a person’s claimed identity

Level of Assurance	Description	Aim	Controls	Method of processing
1 – Low	<p>Little confidence in the accuracy or legitimacy of a claimed identity.</p> <p>Appropriate for transactions with minimal consequences to the organisation or community from registration of a fraudulent identity.</p> <p>Examples may include commercial email providers which require assurance that an imposter has not gained unauthorised access to an account, although the account itself could be created using a pseudonym.</p>	Identity is unique within the context	Self-claimed or self-asserted identity (pseudonymity is possible, but not anonymity)	Local or remote
2 – Medium ('Bronze standard')	<p>Some confidence in the claimed identity.</p> <p>Appropriate for transactions with some consequences associated with registration of fraudulent identities, such as access to a service by an ineligible person and/or some minor consequences to the community from registration of a fraudulent identity.</p> <p>Examples may include provision of some low value/risk services, such as registration for a library card or rental of goods.</p>	Identity is unique within the context, identity is recognised by authoritative sources and identity is used in other contexts	Evidence of identity through use of identity information or documents from authoritative sources	Local or remote
3 – High ('Silver standard')	<p>High confidence in the claimed identity.</p> <p>Appropriate for transactions with serious consequences associated with fraudulent registration, such as allowing access to sensitive information, systems or people, including those of organisations other than that which undertook the initial identity proofing.</p> <p>Examples include issuance of documents and credentials used as secondary evidence of identity in the community (see Appendix B).</p>	Identity is unique within the context, the identity is recognised by authoritative sources, identity information is verified with authoritative sources, identity is used in other contexts and the person is linked to the identity	Evidence of identity through use of identity information or documents from authoritative sources + information or documents verified with an authoritative source	Local or remote

Level of Assurance	Description	Aim	Controls	Method of processing
4 – Very high ('Gold standard')	<p>Very high confidence in the claimed identity.</p> <p>Appropriate for transactions with very serious consequences associated with fraudulent registration to the organisation and/or significant consequences to the community from registering a fraudulent identity, such as from issuance of a document commonly used as evidence of identity.</p> <p>Examples include issuance of government documents used as primary evidence of identity in the community e.g. the Australian Passport.</p> <p>(The majority of requirements at this level align with the former GSEF)</p>	<p>Identity is unique within the context, identity is recognised by authoritative sources, identity information is verified, identity is used in other contexts and the person is linked to the identity</p>	<p>Evidence of identity through use of identity information or documents from authoritative sources + information or documents verified with an authoritative source + individual witnessed in-person</p>	<p>Local only</p>

2.2.6 LoA 4 retains the requirement for a local, in-person interaction as part of the identity proofing process. This provides greater opportunities for examining the integrity of original identity documents provided as evidence of identity and establishing a linkage between a person and their claimed identity. However developments in biometrics, mobile and other technology are continually improving the integrity of online or remote processes for identity proofing. AGD will continue to monitor these developments to determine whether in future this could offer government agencies with a viable alternative method for remote identity proofing with an equivalent 'gold standard' level of assurance. Should this become the case, these Guidelines may be updated accordingly, having regard to their alignment with relevant international standards.

Chapter 3

Choice of Level of Assurance

3.1 Undertaking a risk assessment

- 3.1.1 The design and implementation of identity proofing processes **SHALL** be informed by an assessment of the identity-related risks associated with the transaction or service. This would normally be conducted as a component of broader authentication and management processes.⁶ The risk assessment **SHOULD** also consider the privacy impacts of collection and use of personal information (see 3.4 for further information). The risk assessment **SHALL** follow a methodology consistent with the Australian/New Zealand Standard *AS/NZ ISO 31000-2009 Risk Management – Principles and Guidelines*. Detailed guidance on assessing identity-related risks is available in the National e-Authentication Framework.⁷
- 3.1.2 A risk assessment **SHALL** be undertaken for each different type of service or identity document or credential issued by an organisation (i.e. an organisation that issues two different types of identity documents would need to consider the risks associated with issuance of each document separately). Alternatively, where an organisation has already established that two types of identity documents are equivalent for identity purposes (such as a driver licence and proof of age card) a single risk assessment **MAY** be undertaken.
- 3.1.3 Risk assessments **SHOULD** consider the impacts to the organisation itself as well as the risks associated with the misuse of any resulting identity document in the broader community, where appropriate (for many services there will be no risks to the broader community). This includes the impacts on:
- individuals (e.g. an entitled person has difficulty accessing a government service because their identity has been used previously by another to claim the service or have other financial, psychological or legal difficulties associated with recovering their stolen identity)
 - government agencies (e.g. incorrect attribution of identity results in significant losses for an agency)
 - non-government organisations (e.g. fraudulently obtained genuine identity documents are used to commit fraud against other businesses)
 - the broader Australian identity system (e.g. if issuance of a credential, document or service could be used, in combination with other evidence types, to fraudulently obtain higher integrity identity documents or credentials).
- 3.1.4 Detailed assessment of broader identity risks would normally only be required for organisations that issue documents that are commonly relied upon as evidence of identity (e.g. driver licences, passports, Medicare cards) or organisations in industries that are known to be targeted by criminals. These assessments **SHOULD** include processes for consulting with relevant law enforcement and other organisations that may rely upon these documents to better understand use of the documents in the community and the risks associated with fraudulently obtained genuine documents.

⁶ Note risk assessments are intended to inform the design of identity proofing processes. They are *not* required for individual transactions or for individual people.

⁷ Available at www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management/national-e-authentication-framework/

- 3.1.5 State and territory government agencies **SHOULD** consider undertaking coordinated national risk assessments with relevant agencies in other jurisdictions. This is particularly relevant for issuance of driver licences, and documents issued by RBDMs.
- 3.1.6 The risk assessment **SHOULD** also consider non-identity proofing risk mitigation strategies. For example, some identity risk could be mitigated via supporting identity management and/or fraud detection processes (such as internal data cleansing, data matching against other organisation records or data analysis to detect suspicious transactions). These mitigation strategies may provide a more cost effective option to counter identity fraud than rigorous upfront identity proofing processes.
- 3.1.7 Organisations **SHALL** review and refine their risk assessment strategies on an on-going basis in light of their experience with continuing or emerging identity related risks and vulnerabilities.

3.2 Reliance on known customers

- 3.2.1 During the risk assessment, organisations **SHOULD** consider whether they may be able to rely upon the identity proofing processes of other organisations to create a new identity record. If an organisation relies on authentication of a credential issued by another organisation these Guidelines should not be used. Instead, the organisation should refer to *AS4860-2007: Knowledge-based identity authentication – Recognizing Known Customers* and the NeAF. 'Known customers' are people whose identity has previously been verified by another trusted organisation and issued with a credential.⁸ Where the person already possesses recognised credentials issued by another trusted organisation at or above the desired LoA, authentication of these credentials **MAY** be accepted as a substitute, in whole or in part, for identity proofing where formal recognition arrangements are in place.

3.3 Choosing a level of assurance

- 3.3.1 Services or transactions that involve little or no inherent identity risk will not normally require identity proofing processes. Services that have a higher level of identity risk will require an identity proofing process, where these risks are not acceptable or cannot be mitigated more effectively via other means (such as mechanisms to detect fraudulent transactions).
- 3.3.2 The choice of the level of assurance required for any identity proofing process (and broader authentication and management processes) is a function of the risk ratings, taking into account the impact of any other non-identity proofing mitigations (such as backend management mitigations). Choice of assurance level **SHOULD** be based on the residual risks following consideration of the impact of other risk mitigation strategies.

⁸ Note known customers can also refer to customers whose identity has previously been verified by the organisations itself.

- 3.3.3 The choice of assurance level **SHOULD** also be balanced against the costs associated with implementing identity proofing processes that are overly rigorous. Such processes can include a greater financial and time impost on both organisations and people.
- 3.3.4 Organisations **SHALL** therefore make a decision about the level of residual identity-related risk they are willing to bear, based on available resources and other considerations (such as cost/benefit of implementation of identity proofing processes and privacy considerations).

3.4 Privacy

- 3.4.1 Stronger identity proofing processes will often, though not necessarily, require collection of greater amounts of personal information (the best designed identity proofing processes minimise the amount of personal information collected). Collecting more personal information than is reasonably necessary can adversely impact on privacy and breach privacy legislation. This can also increase the potential consequences from any theft, loss or compromise of the personal information collected and retained as a result of the identity proofing process.
- 3.4.2 An identity-related risk assessment **SHALL** include consideration of the appropriate amount of information to collect, and privacy implications from collecting and storing personal information for identity proofing purposes. Organisations **SHALL** ensure handling of personal information as part of the identity proofing process align with relevant Commonwealth or state and territory privacy legislation, such as provisions regarding collection, consent, access to information, disclosure and retention.
- 3.4.3 Identity risk assessments **MAY** therefore be coordinated with a privacy impact assessment, where appropriate. Privacy impact assessments 'tell the story' of a project from a privacy perspective and helps manage privacy impacts. Like an identity risk assessment, the specific details of a privacy impact assessment will be dependent on the context in which it is being conducted. In broad terms, a robust privacy impact assessment⁹ describes how personal information flows, is used and stored. In an identity proofing process, it analyses the possible impacts on individuals' privacy, and identifies and recommends options for managing, minimising or eradicating impacts.

3.5 Other considerations

- 3.5.1 Misuse of identity information is a key enabler of a range of fraudulent activities. The identity risk assessment **SHOULD** be undertaken within the context of the broader authentication, identity management, fraud, information security and risk management processes of the enrolling organisation.¹⁰
- 3.5.2 A monitoring and evaluation plan **SHOULD** be developed as part of the design phase before an identity proofing process becomes operational.

⁹ Further information on undertaking a privacy impact assessment is available in the Office of the Australian Information Commissioner *Guide to undertaking privacy impact assessments* (May 2014)

¹⁰ Further information on security risk management, including information security, can be found at www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Security-risk-management.aspx

Chapter 4

Identity Proofing Objectives and Requirements at each Level of Assurance

4.1 Minimum Identity Proofing Requirements

- 4.1.1 **Table 3** outlines the *minimum* identity proofing requirements to satisfy the identity proofing objectives for each Level of Assurance. Additional identity proofing processes, including those not described in these Guidelines, **MAY** also be used *in addition* to these the minimum requirements, where necessary to mitigate identity risks identified during the risk assessment phase. A summary of how the requirements apply at each LoA is included at **Appendix B**.
- 4.1.2 The identity proofing requirements rely on evidence from authoritative sources, such as government issued documents as well as evidence of a person's digital footprint. A list of suggested evidence types and suggested weightings (PRIMARY or SECONDARY) is included at **Appendix B**. Only documents or other evidence types that remain valid **SHALL** be accepted.¹¹
- 4.1.3 All LoAs only include processes designed to substantiate a person's claim to an identity. While these may be undertaken in combination with other background checks to determine a person's criminal history, eligibility or suitability, these checks are beyond the scope of these Guidelines.
- 4.1.4 In fulfilling some or all of the identity proofing requirements organisations **MAY** choose to engage third party identity service providers. For instance, some commercial organisations offer services that use a person's 'online social footprint' as evidence of their identity. Further information on use of third party providers is included in **Appendix C**.
- 4.1.5 In some cases a single document will address multiple identity proofing requirements. For example an ImmiCard could potentially meet objectives 2, 3 and 4. To avoid a single point of failure (i.e. compromise of a single piece of evidence), organisations **SHOULD NOT** rely on a single piece of evidence to satisfy multiple objectives unless a person can demonstrate legitimate reasons for not being able to provide documents or other information to meet the preferred evidentiary requirements. However, a PRIMARY identity document **MAY** be used to support both objectives 2 and 3 (see **Appendix B**).
- 4.1.6 Identity proofing **SHALL** be by the organisation itself or by a third party contracted to carry out the process. Applicants **SHOULD** be provided with secure channels (e.g. registered mail or secure online channels) to provide personal information and documents and be encouraged to use them.
- 4.1.7 Internal fraud controls **SHOULD** be implemented for personnel involved in identity proofing processes (particularly at higher LoAs), such as employment screening, information processing controls, physical access to sensitive assets, segregation of high risk duties and access restrictions and accountability for resources and records.

¹¹ A valid document is one that has an expiry date which has not yet passed or where the expiry date has passed but the document is otherwise treated by the issuing agency as being valid for evidence of identity verification. For example, Australian passports can be verified through the Document Verification Service (DVS) for up to two years following their expiry date, so they would still be considered valid for identity checking purposes. Likewise, expired ImmiCards are still able to be verified through the DVS (as the expiry date is for administrative purposes).

Table 3: Minimum Identity Proofing Requirements

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Objective 1. Confirm uniqueness in the intended context			
Identifier chosen by the individual is unique	Checks that the person is the sole claimant of the identity SHOULD be undertaken except where this is prevented for privacy or security reasons. This MAY ¹² be through: <ul style="list-style-type: none"> checking internal organisation records for identities with the same biographical attributes¹³ matching the person against all other organisation records using biometric recognition. 		

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Objective 2. Confirm the claimed identity is legitimate			
Nil	Nil	<i>Commencement of Identity</i> ¹⁴ Evidence SHALL ¹⁵ be provided via verification of one of the following options: <ol style="list-style-type: none"> Australian Birth Certificate or authorised record of birth¹⁶ Australian Passport¹⁷ OR Immigration record or document: <ul style="list-style-type: none"> Australian Citizenship Certificate Australian visa (supported by a foreign passport, which is needed for verification) OR ImmiCard <i>Deceased identity</i> A check that the identity is not that of a deceased person SHOULD be undertaken.	<i>Commencement of Identity</i> As per Level 3 requirements, with the addition that an Australian Passport SHALL NOT be accepted as evidence of commencement of identity. Documents SHALL be provided at an in-person interaction (in the case of Australian visas the foreign passport SHALL be produced as most Australian visas are electronic). <i>Deceased identity</i> As per Level 3 requirements.

¹² Other methods of checking that a person is the sole claimant **MAY** be used that are not listed in the Guidelines.

¹³ Depending on the number of attributes chosen (i.e. if name only is used or in rare cases name + DOB), there may be statistical twins (i.e. people with the same attributes). Therefore detection of a record with the same attributes would not necessarily be cause to deny an applicant, but would warrant further investigation or checks (e.g. checking other attributes such as place of birth).

¹⁴ Where a change of name has occurred evidence must be provided [see guidance under 'Other Requirements' in **Table 3**].

¹⁵ If commencement of identity in Australia has not been established then the foreign passport can be accepted as a proxy of commencement of identity.

¹⁶ A higher level of confidence that a birth certificate has not been cancelled (due to death or change of name) will be achieved if the birth certificate is verified with the issuing authority and if a recent birth certificate is requested and sighted (e.g. a birth certificate less than 10 years old).

¹⁷ Although an Australian Passport is not evidence of commencement of identity in Australia, it can be used as proxy at lower levels of assurance. Use of the Australian Passport to provide evidence of commencement of identity should be considered on a risk management basis. Passports are generally valid for 10 years and so will not always reflect changes of name. By contrast, many RBDMs are now updating birth records where a change of name has occurred and issuing a new certificate. This would mean that old birth certificates in the previous name could not be electronically verified.

CHAPTER 4

IDENTITY PROOFING OBJECTIVES AND REQUIREMENTS AT EACH LEVEL OF ASSURANCE

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Objective 3. Confirm the operation of the identity in the community over time¹⁸			
Nil	Evidence of the identity operating in the community through verification of a person's social footprint SHALL be provided (refer Appendix B). This SHOULD include: <ul style="list-style-type: none"> One PRIMARY type of evidence AND one SECONDARY type of evidence. 	As per Level 2 requirements, although this evidence SHALL be verified with an authoritative source (e.g. issuing authority), where possible.	As per Level 3 requirements, except that original physical evidence SHALL also be provided at an in-person interaction. ¹⁹

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Objective 4. Confirm the linkage between the identity and the person claiming the identity			
Nil	No additional requirements. Evidence provided to meet objective 3 will provide a low level of confidence in the linkage between the identity and the person. ²⁰	Evidence SHALL be provided of a linkage between the person and the claimed identity. This MAY be through: <ul style="list-style-type: none"> Manual/visual comparison of a person's face against a photograph on a PRIMARY²¹ piece of evidence (either remotely²² or in-person) OR Verification of a biometric template collected at registration (either remotely or in-person) against a biometric template held by an authoritative source²³ OR Knowledge based authentication (if questions are derived from multiple authoritative sources, do not use publically available information²⁴, are randomised and a time limit is set for answering the questions or other equivalent practices are used). 	As per Level 3 requirements, except that a visual comparison of a person's face against a photograph on a PRIMARY evidence type SHALL occur as part of an in-person interaction.

18 Although evidence of identity operating in the Australian community is encouraged where possible, in many cases (particularly for verification of foreign nationals) this will not be possible and foreign evidence types will be required.

19 Where digital evidence of identity operating in the community is used, it should be verified by an authoritative source to an equivalent level of assurance.

20 Someone who has access to personal information and identity documents about an individual is likely to be the owner. However, this only provides a low level of assurance in the linkage because family and close friends could be expected to have access to the same evidence.

21 See **Appendix B** for further information on weightings of evidence types.

22 For example, via a high definition video.

23 Note biometric signatures **MAY** be used (i.e. comparison of biometric templates), but manual (i.e. visual) comparison of signatures **SHALL NOT** be used.

24 For example organisations could draw questions from records held by government agencies, such as education records, historical address information, purchases of houses, registration of cars. Non-government organisations may also be able to provide authoritative sources of information (see **Appendix B**).

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Objective 5. Confirm the identity is not known to be used fraudulently			
Nil	Nil	<p>Checks SHOULD be undertaken against information or records held within the organisation, such as checks against internal registers of known fraudulent identities or vulnerable identities (where available).²⁵</p> <p>Checks MAY also be undertaken against information on known fraudulent identities from other authoritative sources, such as law enforcement or other government agencies.</p> <p>An identity flagged as potentially fraudulent does not mean a person will automatically be denied access to a service. Instead it suggests that the organisation needs to take further steps to confirm the person's identity. The organisation SHOULD take further steps to confirm the person's identity, such as enquiries with law enforcement or other organisations, provision of extra identity information, a detailed interview with the person or provision of trusted referee reports.</p>	

Level of Assurance			
Level 1 (Low)	Level 2 (Medium)	Level 3 (High)	Level 4 (Very High)
Other requirements			
Nil	<p>If the person's name differs between pieces of evidence, a RBDM-issued change of name certificate, marriage certificate or amended commencement of identity document (e.g. Australian Citizenship Certificate) SHALL be provided to provide a link between the two names.²⁶</p> <p>The following attributes SHALL be verified with an authoritative source or checked against evidence²⁷:</p> <ul style="list-style-type: none"> • First name • Middle name/s • Surname • Date of Birth 	<p>As per Level 2 requirements AND the following attributes SHALL be verified with an authoritative source:²⁸</p> <ul style="list-style-type: none"> • First name • Middle name/s • Surname • Date of Birth <p>Documents in languages other than English SHOULD be accompanied by a NAATI²⁹ accredited translation.</p>	<p>As per Level 3 requirements AND only original physical documents SHALL be accepted.</p> <p>The following attributes MAY also be confirmed:</p> <ul style="list-style-type: none"> • Place of Birth • Signature³⁰ • Residential address

25 Internal records of fraudulent and vulnerable identities **MAY** take the form of separate registers or could be 'dummy records' in the system.

26 This evidence is required even when the difference could be explained by an error e.g. Anne recorded as Anna to ensure all records of the same person can be linked.

27 Attributes would generally (although not necessarily) be verified through when evidence provided to support objectives 2, 3 and 4 is verified.

28 Attributes would generally (although not necessarily) be verified through when evidence provided to support objectives 2, 3 and 4 is verified.

29 National Accreditation Authority for Translators and Interpreters. Further information is available at http://www.naati.com.au/home_page.html

30 Note manual/visual comparison of a signature against a signature previously provided to an authoritative source is not a biometric check and not sufficient evidence to provide a link between a person and an identity.

Chapter 5

People unable to meet minimum identity proofing requirements

5.1 Exceptions processes to confirm a claimed identity

- 5.1.1 Although the majority of people should be able to meet the requirements of these Guidelines, in some cases people may face genuine difficulty in providing the necessary evidence to identify themselves to the required level of assurance. Each organisation **MAY** develop alternative identity proofing processes for these 'exceptions cases' (if appropriate) informed by a risk assessment and **SHOULD** review these processes regularly.
- 5.1.2 Exceptional cases are those where a person does not possess, and is unable to obtain, the necessary information or evidence of identity. This **MAY** (but does not necessarily always) include: people whose birth was not registered; people who are homeless; undocumented arrivals to Australia; people living in remote areas; people who are transgender or intersex; people effected by natural disasters; people with limited access to identity documents, for example because they were raised in institutional or foster care; people with limited participation in society; and young people or those over 18 who are yet to establish a 'social footprint' in the community.
- 5.1.3 Alternative identity proofing processes that organisations **MAY** consider for these exceptions cases³¹ include (note different combinations of these processes may be appropriate depending on the individual circumstances).
1. Acceptance of alternative types of evidence of identity (such as multiple types of SECONDARY evidence types where normally a PRIMARY evidence type would be required).
 2. Verification of the person's claimed identity with a trusted referee whose identity has been (or is being) verified to an equal or greater level of assurance.
 3. Verification of a person's claimed identity with reputable organisations or bodies known to them (for example, Aboriginal and Torres Strait Islander organisations may hold, or be able to verify, the identity of clients where no prior government record exists).
 4. A detailed interview with the person about their life story to assess the consistency and legitimacy of their claims.
 5. Alternative methods of providing information or documents (such as provision of certified copies by trusted third parties instead of attending an in-person interaction where a person can demonstrate they live in a very remote area).
 6. Providing support for individuals to obtain evidence (such as assisting a person to register their birth with an RBDM).

³¹ This is not an exhaustive list of options. It is the responsibility of each organisation to consider, on a risk basis, appropriate alternative processes

- 5.1.4 Identity proofing requirements for exceptions cases **SHOULD** include robust processes to confirm identity. This is not to disadvantage those people who may be unable to meet the standard requirements. Importantly, it is to prevent these exceptions processes from being exploited through criminals targeting people who may have identities that are more vulnerable to misuse.

5.2 Verifying the identity of children

- 5.2.1 In seeking to verify the identities of children organisations **SHOULD** use the general requirements wherever possible. In cases where this is not possible, organisations **SHOULD**:
1. verify the identity of the child's parent/s or legal guardian to the required LoA, and
 2. establish a documentary link between the child and their parent or legal guardians, such as through provision of the child's birth certificate.
- 5.2.2 Organisations which are using exceptions processes to confirm a child's identity at LoA 4 **MAY** request a range of additional evidence to indicate the child's use of the identity in the community (e.g. documents produced through the child's engagement with the health and education sectors).

Chapter 6

Assessing Applications

6.1 Recording identity proofing outcomes

- 6.1.1 A record of the outcomes of individual identity proofing processes **SHOULD** be captured in a corporate records system, maintained according to relevant privacy legislation for as long as required then securely disposed of or de-identified.
- 6.1.2 If a person has failed to meet the identity proofing requirements a record **SHOULD** be created (e.g. either as a dummy record or in an internal register) with the reason for this outcome. This can assist in the future identification of fraudulent applications.
- 6.1.3 Identity records associated with unsuccessful identity proofing processes **SHOULD** be flagged in the electronic records system (to prevent future registration) using one or more of the following categories:
- **Non-legitimate:** claimed identity does not appear to exist (i.e. no commencement of identity record and no reasonable reason for lack of documentation).
 - **Deceased:** owner of the claimed identity is deceased.
 - **Anomalous:** social footprint is either unavailable or too inconsistent with that reasonably expected of the claimed identity.
 - **Non-linkage:** applicant does not appear to be the legitimate owner of the identity (i.e. linkage between the claimant and the identity could not be established).
 - **Suspected Fraudulent:** identity evidence is either: revoked; reported lost or stolen; or otherwise suspected of being fraudulent (e.g. suspected counterfeit document).
 - **Fraudulent:** identity evidence is known to be fraudulent (e.g. based on report from law enforcement agency).

6.2 Identifying fraudulent applications

- 6.2.1 When conducting each individual identity proofing process (i.e. for individual applications), assessing officers **SHOULD** adopt a risk-based approach and consider:
- the subject's history with the organisation (e.g. have they previously applied and were declined the service because of identity reasons)
 - genuine difficulties meeting requirements (e.g. are language barriers a reason for inconsistencies?)
 - the results of any counter-fraud check (e.g. an alert may be recorded for a person who is vulnerable to identity theft or has been a victim of identity theft)
 - type and level of fraud known/suspected to occur within a particular group of applicants
 - type and level of fraud known/suspected to occur with respect to particular types of evidence, and
 - internal consistency between information and documents provided.

- 6.2.2 If discrepancies are found in the identity information provided by a person, an organisation might have cause to suspect that claims of identity made are not genuine. In these situations, the organisation **SHOULD**:
- require additional supporting information (e.g. an additional identity document, trusted referees report or an additional process such as an interview), or
 - apply some of the requirements for a higher assurance level to the individual case to resolve those discrepancies, or
 - undertake alternative processes, such as a more detailed interview.
- 6.2.3 Organisations **SHOULD** provide staff (including employees and contractors) involved in identity proofing processes with training³² and tools³³ to detect fraudulent applications, such as recognition of document security features, particularly for foreign documents, at higher Levels of Assurance. This **MAY** include information about any groups of applicants or types of documents that have been identified as more likely to be fraudulent and thus should be treated with additional caution.
- 6.2.4 Ideally, agencies **SHOULD** have a separate investigations unit or team. This would include officers trained in fraud detection and with authority to undertake investigations.³⁴ Further investigations could include conducting in-depth interviews with people about their life history to detect inconsistencies that could indicate fraud. It could also involve interviewing people and organisations associated with the subject.
- 6.2.5 Suspected cases of fraud **SHALL** be referred to police or other relevant law enforcement agency following completion of an internal investigation (where appropriate).
- 6.2.6 Organisations **MAY** develop policies and procedures to inform individuals (where practical) when they become aware that a person has been a victim of identity theft and support the individual to recover their identity (such as through referral to relevant services).³⁵
- 6.2.7 Unless it is unlawful to do so or alternative advice is received from law enforcement agencies, government agencies **SHOULD NOT** return any documents that are suspected to be fraudulent until the individual's identity has been fully established. Loss of this evidence could significantly jeopardise any action an agency **MAY** wish to take against a fraudulent applicant.
- 6.2.8 A detailed interview by an investigator trained in fraud detection **MAY** provide a useful way of investigating a case where fraud is suspected. It can be a useful tool to detect inconsistencies that may indicate inaccurate information has been provided. This may be particularly useful where information has been provided by someone who cannot meet the usual identity proofing requirements as well as an additional check for suspicious applications.

32 Training in fraud investigation and detection is available through the Attorney-General's Department Protective Security Training Centre or through a variety of providers listed at www.myskills.gov.au

33 Tools could include the International 1.0 Checking Guide or free systems like the Netherlands Police Agency's Electronic Reference Database of Travel Documents (Edison TD) and Document Information System for Civil Status (DISCS) systems to help identify fraudulent documents. These two systems have pictures of genuine identity documents (travel documents in EdisonTD and other types of identity documents in DISCS) and include a description of the document's security features.

34 The Australian Government Investigations Standards specifies minimum training standards for investigations. The Standards are available at <http://www.ag.gov.au/RightsAndProtections/FOI/Documents/AGIS%202011.pdf>

35 Further information on support for identity theft victims is available at www.ag.gov.au/identitysecurity

Chapter 7

Monitoring and Evaluation

7.1 Evaluation of identity proofing processes

- 7.1.1 Organisations **SHOULD** regularly review the initial risk assessment, choice of LoA and design of identity proofing processes in the context of the broader authentication and identity management policies and frameworks, particularly in light of emerging risks due to environmental or technological changes. This review **SHOULD** include an examination of incidents of identity crime and misuse to evaluate the identity proofing processes.
- 7.1.2 Decisions about the frequency of reviews remains at the discretion of the organisation concerned, which **MAY** choose to align such reviews with other processes, such as a schedule of internal audits. Frequency of reviews **SHOULD** be informed by the initial identity risk assessment process.

7.2 Reporting

- 7.2.1 These Guidelines do not oblige any organisation to adopt a particular LoA. However, transparency in the identity proofing processes adopted by government agencies (particularly those which issue documents commonly relied upon as evidence of identity) will help other organisations make an informed decision about the level of confidence they should place in identity proofing processes of other organisations.
- 7.2.2 Organisations **MAY** also seek accreditation from a third party accreditation provider or report their compliance with the Guidelines through their annual or agency reporting processes.

Appendix A

Glossary

A.1.1 The following definitions are used for the purpose of these Guidelines. These definitions have been designed to be as accessible as possible and therefore generally include fewer technical terms than definitions in other similar documents. As they have been adapted for these Guidelines, they should not necessarily be considered as authoritative definitions for broader purposes.

Glossary	
Agency	An agency refers to an Australian Government or Australian state or territory body.
Applicant	The person making the application.
Application	Usually the application is the first step in the enrolment process and identity proofing will be a function of that process.
Assessing officer	The person who is assessing applications and making a decision about whether a person meets the specified identity proofing requirements. The assessing officer may be an employee of the organisation or contracted to assess applications.
Assured identity	A claimed identity that has been subject to an identity proofing process and is thus linked to a person with a defined level of confidence that it is the person's real identity.
(Identity) Attribute	A characteristic that can be used (in combination with other attributes) to uniquely identify a person in a specific context (such as name, data of birth or a unique number).
Australia's identity system / infrastructure	A term used to describe the (government and non-government) organisations that issue documents and other types of evidence of identity and the organisations that rely on their processes to support their identity proofing or authentication processes.
Authentication	A function for establishing the validity and assurance of a claimed identity of a user, device or another entity by testing the credentials supplied by the entity making the claim.
Authoritative source	A repository which is considered by the relying party to be an accurate and up-to-date source of information using best available information (such as a government agency database or an third party identity service provider accredited to the required level of assurance).
Biometric information (biometrics) ³⁶	Biometric information means information about any measurable biological or behavioural characteristics of an individual that can be used to identify the individual or verify the identity of the individual, such as face, fingerprints and voice.
Biometric system	Systems or technologies that automate the identification of individuals using one or more types of biometric information.
Biometric template	Biometric template means a digital or mathematical representation of an individual's biometric information representing information extracted from a sample of the individual's biometric information.
Claim	A statement that something is the case. It is the claim being made that the relying party wishes to confirm before being accepted. For example, a common claim is one of identity.
Commencement of Identity	Commencement of identity is the first registration by a government agency in Australia and includes RBDM birth registrations and issuance of DIBP immigration documents and records. These may also be called cardinal documents.
Credential	A Credential is the technology used to authenticate a user's identity. The user possesses the Credential and controls its use through one or other authentication protocols. A Credential may incorporate a password, cryptographic key or other form of secret. To use a digital identity in requesting access to a resource, a subject presents 'Credentials'. The Credentials (once authenticated) are taken as proof that the subject owns the digital identity being presented, and that the subject is permitted to access the resources/services which are associated with their digital identity.

³⁶ Under the *Privacy Act 1988* biometric information is considered as sensitive information, which provides additional obligations on organisations.

Glossary

Document Verification Service	The DVS is a national real-time system that allows participating organisations to compare a customer's identifying information on particular government issued documents with the issuing government agency. The DVS is a secure system that operates 24/7 and matches key details contained on Australian-issued identifying credentials providing a 'yes' or 'no' answer within seconds.
Enrolment	The process from initial application for a service or an identity credential through identity proofing to registration and recording of the person's data and issuance of the service or credential. In addition to identity proofing, enrolment would consider eligibility, recording and issuance, which are all out of scope of these Guidelines.
Entity	Something that has separate and distinct existence and that can be identified in a context.
Evidence of identity	Information that a person may present to support assertions or claims to a particular identity. This evidence is traditionally provided in the form of identity documents or other card-based credentials that contain key attributes (such as name, date of birth, unique identifier) that are considered as the core elements of a person's identity. More recently, evidence of identity can also take the form of information on a person's 'pattern of life' or 'social footprint'.
Fact of Death file	A file generated by RBDMs that lists deaths registered in Australia.
Identity crime	Activities or offences in which a perpetrator uses a fabricated, manipulated, stolen or otherwise fraudulently assumed identity to facilitate the commission of crime.
Identity document	Identity document means any document or other thing that contains or incorporates identification information and that is capable of being used as evidence of identity.
Identity fraud	The gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated, manipulated, stolen or otherwise fraudulently assumed identity.
Identity management	Policies, rules, processes and systems involved in ensuring that only known, authorised identities gain access to networks and systems and the information contained therein.
Identity theft	The fraudulent use of a person's identity (or a significant part thereof) without consent, whether the person is living or deceased.
Identity proofing	Identity proofing is the process of capturing and confirming information to a specified or understood level of assurance to provide organisations with confidence in the identity of a person with whom they are interacting with for the first time.
Identity record	The personal information held by an organisation about a person (note records will generally also contain other types of information).
In-person interaction	An interaction in which the subject and/or applicant must be physically present with, and sighted by, an officer or contractor from the organisation.
Interview	In-depth questioning about a subject and/or applicant's life history and behaviours to determine consistency of story. This may be conducted in-person or remotely.
Issuance	The process involved in providing a person with an identity document or credential. This will be undertaken in conjunction with or following the Registration process, or in a service delivery context it will occur when eligibility is determined.
Level of assurance (or confidence)	The degree of confidence in a person's claimed identity at application (i.e. through identity proofing) or at authentication.
Local	Local refers to a method of processing applications where an in-person interaction occurs and original evidence is physically sighted.
Knowledge based authentication	Knowledge-based authentication is a security measure that identifies end users by asking them to answer specific security questions in order to provide accurate authorization for online or digital activities. A person is challenged to provide one or more answers to questions/ challenges provided by the party undertaking the authentication (i.e. the organisation chooses the questions).

Glossary

Known customer	A person whose identity has previously been verified by another trusted organisation or previously by the same organisation. Where the person already possesses recognised credentials at or above the desired Level of Assurance, authentication of this credential may be accepted as a substitute for all or part of the identity proofing process.
Online verification services	A broad definition covering services or tools which enable people to have claims regarding their identity or other attributes verified online.
Organisation	A generic term to describe a government, business or other non-government organisation.
Registration	Registration is a subset of enrolment. It is the process whereby, having successfully completed the identity proofing process, a person's identity data is recorded.
Relying party	An actor (including organisations and government agencies) that relies on an assertion about a person's identity.
Personal information	Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable. Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.
Remote	Any interaction that happens where there is no in-person interaction, such as submission of an application and provision of evidence via mail, online, video-conferencing or over the phone.
Social (Digital) Footprint	The trail of information recorded in information systems or other types of evidence (such as testimonial from a referee) as a result of normal social, living and employment activities during a person's lifetime. An online social footprint (or 'digital footprint') refers to the trail, traces or 'footprints' that people leave behind online.
Subject	The person contained in the application, whose identity is being examined and, if successful, registered.
Third Party Identity (services) provider	Commercial providers of identity related products or services to other organisations, usually on a commercial basis. These products and services may include: verification of identity information; storage or management of personal information (e.g. digital inboxes); or management of credentials used for identity authentication)
Transaction	A discrete event between a person and a service provider that supports a business or programmatic purpose.
Trusted party	An organisation, authority or its agent (including government or non-government), trusted by other organisations (such as the relying party and other similar organisations) with respect to specified activities and to a specified level of assurance.
Trusted referee	A trusted referee is a person or organisation that holds a position of trust in the community and does not have a conflict of interest, such as an Aboriginal elder or reputable organisation that the person is a customer, employee or contractor of, and is known and listed by the enrolling agency to perform the function of a referee. The Statutory Declarations Act 1959 provides a list of people who hold a position of trust in the community. Similar lists are also generally included in state and territory legislation. Trusted referees may also include guardians or other people nominated to act on a person's behalf whose identities have been verified.
Verification	The process of checking information (e.g. name and date of birth) provided at application by comparing it with previously corroborated information (e.g. against the database of the organisation that issued an identity credential).
Visa	Permission to travel to and enter Australia and/or remain in Australia. 'Visa' should not be confused with 'visa label' which is evidence of the existence of and conditions applied to a visa.

Appendix B

Suggested evidence types and weightings

- B.1.1 This annex outlines the types of evidence that **MAY** be accepted as evidence of a person's identity operating in the community over time (Objective 3) and to provide a linkage between the person and the claimed identity (Objective 4).
- B.1.2 Table 4 lists the types of evidence that **MAY** be acceptable and the recommended weighting that **SHOULD** be applied to this as PRIMARY and SECONDARY evidence³⁷. Appropriate weightings **MAY** need to change as organisations update identity proofing and other security practices and the method of provision (such as whether provided in-person or if information is verified with the issuing body).
- PRIMARY evidence is generally government issued evidence types with robust identity proofing processes, issuance and management processes. Where it is a physical document, it will generally contain a photograph and security features.
 - SECONDARY evidence includes evidence types from government or non-government sources that are supported by moderate identity proofing processes, issuance and management processes.
- B.1.3 Organisations **SHALL** determine their own policies on the specific types and combinations of documents, records or other evidence that they will accept in order to meet this objective. Evidence types **SHOULD** be selected from **Table 4**, unless an organisation is able to justify that an alternative evidence provides an equivalent level of assurance. Note this does not mean an organisation has to accept all evidence types listed below. For example, it may be impractical to assess a person's digital footprint and an organisation may instead choose to verify physical documents. Consideration of the appropriate types and amounts of information that are needed for this purpose **SHOULD** be balanced against privacy considerations regarding collection of information. Organisations do not need to accept all types of evidence listed in **Table 4**. Similarly, organisations **SHOULD** only accept those types of evidence for which they can be confident in the underlying privacy and security practices (particularly for online verification tools).
- B.1.4 For those agencies which issue similar identity documents across state and territories (such as driver licences) a consistent list of acceptable evidence types **SHOULD** be agreed between jurisdictions.
- B.1.5 Evidence of identity operating in the community (objective 3) **SHOULD** provide a record of activity over time (e.g. an academic transcript would provide evidence of identity operating in the past while verification of a current Medicare card would provide evidence of the identity operating in the present). Evidence of identity operating in the community will also ideally provide evidence of activity over time where possible (e.g. use of a credit card, not just issuance of the card).

³⁷ The suggested weightings have been subjectively assessed based on available information about the identity proofing process behind issuance, the strength of the credential and ongoing management processes, Weightings will thus need to be updated as further information about issuance processes becomes available.

- B.1.6 Objective 3 **MAY** also include evidence of residential address, particularly for people residing in Australia. While this is not necessarily a key identity attribute, it can provide an extra barrier to criminals who have managed to create a fraudulent online identity and are looking to avoid any physical links.
- B.1.7 Before relying upon a new type of identity evidence issued by another organisation, an organisation **SHOULD** undertake its own assessment of the supporting identity proofing, issuance, and broader management processes. Any queries regarding current or new forms of evidence can be directed to the Attorney-General's Department at identity.security@ag.gov.au.

Table 4: Example of evidence types

Type of evidence	Suggested weighting
Objective 3: Evidence of Identity Operating in the Community	
Objective 4 evidence (see below) ³⁸	Primary
DFAT issued Certificate of Identity	Secondary
DFAT issued Document of Identity	Secondary
DFAT issued United Nations Convention Travel Document	Secondary
Foreign government issued documents (e.g. driver licences)	Secondary
Medicare Card	Secondary
Enrolment with the Australian Electoral Commission	Secondary
Security Guard/Crowd Control photo licence	Secondary
Evidence of right to a government benefit (DVA or Centrelink)	Secondary
Consular photo identity card issued by DFAT	Secondary
Police Force Officer photo identity card	Secondary
Australian Defence Force photo identity card	Secondary
Commonwealth or state/territory government photo identity card	Secondary
Aviation Security Identification Card	Secondary
Maritime Security Identification Card	Secondary
Firearms licence	Secondary
Credit reference check	Secondary
Australian tertiary student photo identity document	Secondary
Australian secondary student photo identity document	Secondary
Certified academic transcript from an Australian university	Secondary
Trusted referees report	Secondary
Bank card	Secondary
Credit card	Secondary
Other authoritative online sources of evidence verified by a Third Party Identity Provider	Secondary
Tax File Number	Secondary

APPENDIX B

SUGGESTED EVIDENCE TYPES AND WEIGHTINGS

Type of evidence	Suggested weighting
Evidence of digital footprint ³⁹	Secondary
Objective 2 evidence of commencement of identity (at LoA 2 only) ⁴⁰	Secondary
Objective 4: Evidence of a linkage between a person and a claimed identity	
Australian passport (including Ordinary, Frequent traveller, Diplomatic, Official and Emergency)	Primary
Foreign passport ⁴¹	Primary
Australian driver licence	Primary
DIBP ImmiCard	Primary
<i>If no other primary evidence types available to establish linkage: Australian government issued proof of age card/photo card⁴²</i>	Primary
<i>If no other primary evidence types available to establish linkage: Australian secondary student identity document (issued by a government agency or Australian school only)⁴³</i>	Primary (only for applicants aged under 18 years)

38 The same evidence type may be used to meet both objectives e.g. an Australian passport may be used to establish a link between the person and the claimed identity (objective 4) and used in combination with a SECONDARY evidence type to demonstrate identity operating in the community (objective 3).

39 Also known as internet life verification, this may include verification of online activity such as email/mobile/social footprint.

40 Although there is no requirement to meet objective 2 at LoA2 (but it is required at LoA 3 and 4), Australian birth certificates or immigration records may be used as a secondary evidence type to meet objective 3.

41 Where evidence is available regarding the robustness of foreign passports it may be appropriate for organisations to request additional evidence in support.

42 Where a PRIMARY evidence type is used which cannot be verified with the issuing authority, organisations should ensure other evidence types are provided that can be verified with an authoritative source, such as the issuing authority.

43 See footnote 42.

Appendix C

Guidance on use of third party identity service providers

- C.1.1 Third party identity service providers are organisations with the capacity to verify with an authoritative source that information (e.g. name, date of birth, address etc.) provided by an individual matches that sources' records. These services may include the verification of specific documents or broader information that helps to establish a person's online social footprint.
- C.1.2 The *Third Party Identity Service Providers Assurance Framework*⁴⁴ sets out the compliance criteria and accreditation requirements for Australian Government agencies seeking to engage third party providers. The Framework can also be used as a reference by state and territory agencies and non-government organisations.
- C.1.3 An organisation seeking to use third party identity services to provide and/or check evidence of identity **SHOULD** take steps to ensure that these services are being provided by a reputable organisation. The degree to which such organisations can be considered as reputable will need to be determined by the relying party. General considerations **MAY** include⁴⁵:
- whether the organisation is accredited under the *Third Party Identity Service Providers Assurance Framework*
 - whether the organisation is a registered legal entity
 - organisational governance and risk management arrangements
 - compliance with privacy and other relevant legislation
 - appropriate contractual arrangements with owners/trustees of personal information
 - whether the relying agency has sufficient visibility and confidence over the providers policies and procedures, including privacy and information security policies and practices, and
 - whether other government agencies or the broader private sector consider the provider to be a reputable organisations.
- C.1.4 Any queries regarding use of third party identity service providers can be directed to the Attorney-General's Department at identity.security@dag.gov.au.

44 Available at www.finance.gov.au/policy-guides-procurement/authentication-and-identity-management

45 Further specifications are included in the Third Party Identity Service Providers Assurance Framework





IDENTITY SECURITY ● ● ●