Evidence of Identity Standard

Version 1.0 - June 2006
Evidence of Identity Standard
Foreword

This Standard is part of the New Zealand E-government Interoperability Framework (NZ e-GIF) authentication standards. These outline good practice guidance for the design (or re-design) of the authentication component of online services where these services require confidence in the identity of the transacting parties. These standards give effect to the planning advice from the State Services Commission’s 2004 Authentication for e-government: Best Practice Framework for Authentication.

This Standard sets out the process requirements for establishing the identity of individuals seeking government services. It should be used for all services, regardless of the delivery channel (i.e. it applies to both online and offline service delivery). It has been prepared for use by New Zealand government agencies.

This Standard will help to ensure that agencies implement evidence of identity (EOI) processes that are appropriate to the services they deliver and that adhere to current accepted good practice.

EOI refers to the types of evidence that when combined provide confidence that individuals are who they say they are. Government services containing identity-related risk will require an evidence of identity process, the comprehensiveness of which will depend on the level of identity-related risk in the particular service. This Standard provides guidance on how to design and operate these EOI processes appropriately.

Application of this Standard will assist with the management of identity theft and fraud, and the consequences that arise from these activities. However, application of this Standard does not guarantee complete mitigation of these risks nor will it prevent cases of administrative error in relation to the establishment of an individual’s identity. Agencies should, therefore, apply this Standard alongside other good practice initiatives that assist in the reduction of identity theft and fraud and which prevent administrative error.

This Standard supersedes the Evidence of Identity Framework published in October 2004 (www.dia.govt.nz).
Contents

0 Foreword ................................................................................................................................ 3

PART 1 – INTRODUCTION AND OVERVIEW

1.1 Purpose ................................................................................................................................ 8
1.2 Objective ................................................................................................................................ 8
1.3 Standardising EOI business processes ................................................................................ 8
1.4 Contextual factors .................................................................................................................. 8
1.5 Authentication Standards ....................................................................................................... 9
1.6 Scope .................................................................................................................................... 10
1.7 Application of Standard ....................................................................................................... 11
1.8 NZ e-GIF status .................................................................................................................... 11
1.9 Accessing advice about this Standard ................................................................................. 12
1.10 Document structure ........................................................................................................... 12
1.11 Interpretation ....................................................................................................................... 13

PART 2 – MINIMUM STANDARD REQUIREMENTS

2.1 EOI process overview ......................................................................................................... 18
2.2 Minimum EOI process phases ............................................................................................ 19
2.3 Minimum process step requirements ................................................................................ 19

PART 3 – GUIDANCE MATERIAL

3.1 Navigating the guidance material....................................................................................... 26
3.2 Core concepts for establishing identity .............................................................................. 27
3.3 Risk assessment phase ....................................................................................................... 28
3.4 Design and operation phase .............................................................................................. 49
3.5 Service delivery phase ....................................................................................................... 79
3.6 Monitoring and evaluation phase ...................................................................................... 79

Working group representation .................................................................................................. 87
Acknowledgement .................................................................................................................... 87
Copyright .................................................................................................................................. 87
Referenced documents .............................................................................................................. 87
Latest revisions ........................................................................................................................ 89
Review of standards.................................................................................................................. 89
APPENDIX

Introduction ...................................................................................................................................... 90

A – EOI ‘Primary’ documents/records referenced in this Standard .................................................. 91

B – EOI ‘Supporting’ documents/records referenced in this Standard .............................................. 119

C – Change of name, adoption and gender reassignment information ............................................ 121

TABLE

1 – Authentication standards and documents .............................................................................. 10

2 – Phases of EOI process ........................................................................................................... 19

3 – Initial risk assessment ........................................................................................................... 35

4 – Identity-related risk consequences and impacts .................................................................. 39

5 – Service risk categories ........................................................................................................ 46

6 – Matching service risk categories to EOI Confidence Levels ............................................... 47

7 – Matching risk level to appropriate EOI Confidence Level process ...................................... 53

8 – Evidential requirements for EOI Confidence Level processes ............................................. 55

9 – Documents/records used to satisfy Objective A .................................................................... 56

10 – Documents/records used to satisfy Objective E ................................................................... 59

11 – ‘Supporting’ documents/records used to satisfy Objective E ............................................. 60

12 – Documents/records used to establish name usage .............................................................. 61

13 – Performance indicators ....................................................................................................... 82

14 – Issues for evaluation ........................................................................................................... 84

A1 – Documents used for Evidence of Identity Processes .......................................................... 91

FIGURE

1 – Overview of evidence of identity model ............................................................................... 18

2 – Overview of risk assessment process .................................................................................. 32

3 – Formal assessment of identity-related risk ......................................................................... 37

4 – Overview of the design and operation phase ....................................................................... 51

5 – Evidence of identity objectives .......................................................................................... 52

6 – Overview of generic business processes for establishing an individual’s identity .......... 54

7 – Monitoring and evaluation cycle ......................................................................................... 80

CHECKLIST

Checklist for phase 1 risk assessment ......................................................................................... 48

Checklist for phase 2 design and operation .................................................................................. 78
Part 1
Introduction and Overview
1.1 Purpose

The purpose of this Standard is to provide good practice guidance for government agencies about the required process for initial establishment of an individual’s identity. The process applies to government services where confidence in the individual’s identity is required because of the types of risk contained within those services.

Use of this Standard will give agencies greater confidence in an individual’s identity, prior to delivery of a service to that person. This initial establishment of identity is an important means by which agencies can manage the risks to their business objectives that result from the incorrect attribution of identity.

If agencies require third parties to follow the Standard, this can be done by including adherence to the Standard in the initial contract for services.

1.2 Objective

The objective of this Standard is to give the agency greater confidence in an individual’s identity, prior to the delivery of a service to that person. This will help to:

• provide consistency of customer experience when seeking services of a similar nature from different government agencies
• provide confidence for the public that the EOI they are asked to provide is fit for the purpose of the particular service they wish to access from an agency
• reduce the risk of identity theft occurring and any downstream criminal activity that this facilitates, including organised crime
• protect individuals from others stealing and using their identities to access government services
• provide confidence that privacy concerns are addressed for evidence of identity processes used by government.

1.3 Standardising EOI business processes

The minimum requirements outlined in Part 2 relate to the EOI process that an agency MUST follow. How these process steps are implemented may vary, depending on the individual agency’s context and objectives. Guidance material is provided in Part 3 of this Standard to help agencies complete each of the required EOI process steps.

1.4 Contextual factors

There are a number of important contextual factors to be aware of when applying this Standard. These include the following:

• identity-related risk is only an aspect of the overall risk associated with any given agency service (see 3.3.2). Implementation of an appropriate EOI process helps agencies manage the identity-related risk associated with particular services, but may have no effect on other aspects of a service’s risk profile
there is an identity-related risk continuum on which services sit. Where a service sits on this continuum depends on the type and extent of identity-related risk particular to that service (see 3.4.2)

it is essential that the level (if any) of identity-related risk is determined for any given service, before agency decisions are made regarding the EOI process that needs to be implemented. This is because the level of identity-related risk in the service will determine the stringency of EOI requirements placed on individuals seeking to access that service. Just as the identity-related risk levels for services sit on a continuum, so does the level of confidence required in individuals’ identities (see 3.4.7)

creation of false identities can occur through avenues other than at the initial establishment of identity, such as through internal infiltration of an agency’s systems. For this reason, it is critical that an agency implement the EOI Standard alongside, not instead of, other identity-related risk management processes

effective implementation of an EOI process depends on appropriate EOI requirements (i.e. what individuals are required to provide by way of identity-related information and documentation) when accessing particular agency services (see 3.4.16)

effective implementation also depends on the manner in which the EOI process is managed internally. For example, it is critical that agencies not only require the individual to provide the correct documentary evidence, but also that the agency has the appropriate in-house processes in place (such as internal controls and staff training) to ensure that the process achieves the outcomes it has been designed to achieve (see 3.4.20).

1.5 Authentication standards

This Standard is part of the NZ e-GIF authentication standards for online service delivery. This suite of standards (see Table 1) provides detailed guidance for agencies to follow when designing authentication solutions. In particular, the standards enable agencies to determine the level of risk for each of their services and to identify appropriate evidence of identity requirements and authentication key technologies.

Most online services delivered by government agencies are either anonymous (such as when someone downloads a brochure from an agency’s website) or have low levels of identity-related risk (such as when someone changes their address details). Services with low levels of identity-related risk are typically authenticated using minimal levels of evidence of identity requirements and a username and password for ongoing confirmation of identity.

NOTE – Change of address is a generic example. For some services, change of address may have a high level of identity-related risk.

To meet the Networked State Services Development Goal (operation of government transformed through the use of the Internet by June 2010), agencies will need to provide online services that have higher levels of identity-related risk. This will necessarily require the implementation of authentication solutions with more rigorous evidence of identity requirements and higher strength authentication keys.
Table 1 describes the purpose of each of the authentication standards. The standards are listed in the order in which they are intended to be used by agencies.

### Table 1 – Authentication standards and documents

<table>
<thead>
<tr>
<th>Standard/Document name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guide to Authentication Standards for Online Services</td>
<td>Provides a high-level overview of the NZ e-GIF authentication standards.</td>
</tr>
<tr>
<td>Evidence of Identity Standard</td>
<td>Specifies a business process for establishing the identity of government agency customers. Applies to services delivered through both offline and online channels.</td>
</tr>
<tr>
<td>Authentication Key Strengths Standard</td>
<td>Specifies the authentication keys to be used for online authentication and protections necessary for the authentication exchange.</td>
</tr>
<tr>
<td>Data Formats for Identity Records Standard</td>
<td>Specifies data formats for a set of customer information data elements that government agencies may use in customer identity records.</td>
</tr>
<tr>
<td>Password Standard</td>
<td>Specifies requirements for passwords used for online authentication.</td>
</tr>
<tr>
<td>Other authentication key standards (to be developed)</td>
<td>Specifies the requirements for two-factor authentication keys used for online authentication.</td>
</tr>
<tr>
<td>Guidance on Multi-factor Authentication</td>
<td>Provides an overview of multi-factor authentication. May be superseded once other authentication key standards are developed. Not a NZ e-GIF standard.</td>
</tr>
</tbody>
</table>

### 1.6 Scope

#### 1.6.1 Establishing identity versus confirming identity

This Standard’s focus is on an agency’s initial contact with an individual seeking a service or services that have a level of identity-related risk. Agency contact with that individual, thereafter, will require the agency to have a means of confirming that the individual is the same person who established their identity with the agency at the outset. This latter type of contact is not in the scope of this Standard.
Agencies SHOULD determine the channels through which they will deliver services and the methods to be used for confirming the identity of individuals after the initial establishment stage. Where the agency is delivering a particular service through an online channel, the suite of authentication standards MUST be referred to (see 1.5).

1.6.2 Establishing identity versus entitlement

The vast majority of services that require the establishment of identity will also involve a need for the individual to meet eligibility or entitlement criteria. Entitlement criteria are directly linked to the type of service being provided. For example, an entitlement criterion for the issue of a New Zealand passport is that the individual is a New Zealand citizen. In most cases, agency processes used to establish both identity and entitlement for particular services will be implemented simultaneously. However, agencies SHOULD undertake process design activities separately to ensure that the objectives of both the EOI process and entitlement testing processes are met with integrity through the processes implemented.

NOTE – While an EOI process will assist in the management of the identity-related risks associated with a particular service, it will not manage the risk of eligibility or entitlement fraud occurring.

1.7 Application of Standard

This Standard has been developed specifically for use by New Zealand government agencies that deliver services to the public that contain identity-related risk.

For guidance on agency responsibilities for compliance with NZ e-GIF standards at each status level, refer to the latest version of the NZ e-GIF (www.e.govt.nz).

This Standard is applicable whether a particular agency service is delivered through online and/or offline channels.

Private sector organisations may choose to apply this Standard for the services they deliver to the public that contain identity-related risk. This Standard may also be used by agencies, both public and private, for recruitment into positions where confidence in the identity of the person being recruited is required.

NOTE – In some cases complete application of this Standard will not be suitable due to the nature of a service’s customer base (e.g. where the service’s customer base is made up of overseas-based customers, for a law-enforcement related service, or where the identities of certain customers are protected). In these cases, agencies SHOULD use exception processes that are aligned as closely as possible to the content of this Standard.

1.8 NZ e-GIF status

Upon approval by the e-GIF Management Committee, this Standard will enter the NZ e-GIF as Under development (U), and graduate to Recommended (R) after a successful, documented implementation. The standard is expected to graduate to Adopted (A) once there is a track record of proven successful implementation.
Advice regarding the current e-GIF status of this Standard can be obtained from:

e-GIF Operations
State Services Commission
Postal: PO Box 329, WELLINGTON
Phone: 04 495 6600
Fax: 04 495 6669
Email: e-gif@ssc.govt.nz

1.9 Accessing advice about this Standard

The Department of Internal Affairs (DIA) is Custodian of this Standard and MUST be notified in relation to any of the following:

• where an agency requires advice on the meaning or implementation of any aspect of this Standard

• where an agency requires supplementary guidance on issues relating to identity information management

• where an agency that issues documents/records referred to within this Standard (see Appendices A to C) changes the issuance process for that document/record. (This is required because a change in the issuance process may require amendment to how the particular document/record is reflected in the standard.)

The EOI Standard Custodian can be contacted at:
Email: eoistandard@dia.govt.nz

1.10 Document structure

This Standard consists of three parts plus Appendix A, B and C as set out below:

<table>
<thead>
<tr>
<th>Part</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction and Overview</td>
<td>Outlines the purpose, scope and application of this Standard.</td>
</tr>
<tr>
<td>2</td>
<td>Minimum Standard Requirements</td>
<td>Outlines the minimum process step requirements that agencies MUST follow to comply with this Standard.</td>
</tr>
<tr>
<td>3</td>
<td>Guidance Material</td>
<td>Provides guidance material for agencies on how to implement the minimum standard requirements outlined in Part 2. This guidance material is presented in order of the minimum process steps required of agencies. Agencies SHOULD follow this guidance material when implementing the minimum requirements set out in Part 2.</td>
</tr>
<tr>
<td>Appendix A, B, C</td>
<td>Documents/Records referenced in this Standard</td>
<td>Provides detail on the issuance processes behind, and appropriate uses of, the identity-related documents and records referred to within this Standard. The Appendices SHOULD be referred to when agencies are designing the evidential requirements to be placed on service customers.</td>
</tr>
</tbody>
</table>
1.11 Interpretation

The following words, defined in *Key words for Use in RFCs to Indicate Requirement Levels* (RFC 2119), are used in this Standard:

- ‘MUST’ – identifies a mandatory requirement for compliance with this Standard
- ‘SHOULD’ – refers to practices that are advised or recommended.

When cross-referencing other clauses or clause subdivisions within this Standard, the number only is quoted.

The full titles of documents cited in this Standard are given in the list of Referenced Documents at the end of this Standard.

1.11.1 Definitions

For the purposes of this Standard, the following definitions¹ apply:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency</td>
<td>Any government organisation that applies this Standard.</td>
</tr>
<tr>
<td>Anonymous service</td>
<td>A service that does not require the user to be identified or require protection of a user’s identity. For example, access to publicly available online publications.</td>
</tr>
<tr>
<td>Attributed identity</td>
<td>The attributes of a person’s identity that are present from birth, e.g. birth name and date and place of birth. (See Appendix C for change of name information.)</td>
</tr>
<tr>
<td>Benchmark</td>
<td>Evaluate or check processes by comparing with a standard point of reference.</td>
</tr>
<tr>
<td>Biographical information</td>
<td>Record of the events that occur during a person’s lifetime, e.g. birth registration, employment history and marriage or civil union registration.</td>
</tr>
<tr>
<td>Biometric information</td>
<td>Physical and behavioural attributes of a person, e.g. their facial features, DNA profile, retina, iris, voice and fingerprints.</td>
</tr>
<tr>
<td>Biometric recognition</td>
<td>The process of matching an input biometric to stored biometric information. In particular, biometric recognition refers to comparing the biometric input from an individual to the stored biometric template about that individual. Examples of biometrics include face images, fingerprint images, iris images, retinal scans, etc.</td>
</tr>
<tr>
<td>Business processes</td>
<td>A series of steps (i.e. related activities) followed to achieve a given outcome. A process has several key characteristics including specific measures that determine if it is done correctly and that enable it to be repeated multiple times; it consumes resources such as time, money and/or energy; and it responds to quality control mechanisms that can help the process be done more efficiently.</td>
</tr>
<tr>
<td>Consequence</td>
<td>Outcome or impact of an event.</td>
</tr>
<tr>
<td>NOTE –</td>
<td>(1) There can be more than one consequence from one event.</td>
</tr>
<tr>
<td></td>
<td>(2) Consequences can range from positive to negative.</td>
</tr>
<tr>
<td></td>
<td>(3) Consequences can be expressed qualitatively or quantitatively.</td>
</tr>
<tr>
<td></td>
<td>(4) Consequences are considered in relation to the achievement of objectives.</td>
</tr>
</tbody>
</table>

¹ The terms event, frequency, likelihood, monitor and risk are taken from AS/NZS 4360.
### Definitions continued

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Discrepancy</strong></td>
<td>Situations where an individual has supplied identity-related documents or information that may have an inconsistency requiring further investigation.</td>
</tr>
<tr>
<td><strong>e-GIF</strong></td>
<td>E-government interoperability framework – a collection of policies and standards endorsed for New Zealand government information technology (IT) systems.</td>
</tr>
<tr>
<td><strong>Electronic verification</strong></td>
<td>Verification of the accuracy of information through electronic checks of information records such as electronic databases.</td>
</tr>
<tr>
<td><strong>Evaluation</strong></td>
<td>Systematic review of processes to ensure that business processes are still effective and appropriate.</td>
</tr>
<tr>
<td><strong>Event</strong></td>
<td>Occurrence of a particular set of circumstances.</td>
</tr>
<tr>
<td><strong>Evidence of identity (EOI)</strong></td>
<td>The types of evidence that, when combined, provide confidence that an individual is who they say they are.</td>
</tr>
<tr>
<td><strong>Evidence of identity process</strong></td>
<td>Process by which an agency establishes confidence in an individual’s identity.</td>
</tr>
<tr>
<td><strong>Evidence of identity process risks</strong></td>
<td>Any risk created through an EOI process.</td>
</tr>
<tr>
<td><strong>Exceptions/exception case</strong></td>
<td>Individuals (or a group of individuals) who, for genuine reasons, are unable to meet the EOI requirements set out in this Standard.</td>
</tr>
<tr>
<td><strong>False identities</strong></td>
<td>Situations where a person uses an identity that is not their own. In some cases, this can be for legitimate reasons.</td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
<td>A measure of the number of occurrences per unit of time.</td>
</tr>
<tr>
<td><strong>Identification</strong></td>
<td>Process of associating identity data with a particular person.</td>
</tr>
<tr>
<td><strong>Identity</strong></td>
<td>A set of attributes and/or data linked to an individual person.</td>
</tr>
<tr>
<td><strong>Identity data/information</strong></td>
<td>Data/information pertaining to an individual’s identity.</td>
</tr>
<tr>
<td><strong>Identity manipulation</strong></td>
<td>Alteration of one or more elements of identity (e.g. name, date of birth) to dishonestly obtain an advantage.</td>
</tr>
<tr>
<td><strong>Identity – misuse and abuse</strong></td>
<td>Gaining money, goods, services, other benefits or the avoidance of obligations through the use of a false or stolen identity.</td>
</tr>
<tr>
<td><strong>Identity-related risk</strong></td>
<td>Any risk for a particular service that results from an individual’s identity being incorrectly attributed. See 3.3.2.1.</td>
</tr>
<tr>
<td><strong>Identity theft</strong></td>
<td>Theft or assumption of a pre-existing identity, or significant part thereof, with or without consent, and whether, in the case of an individual, the person is alive or dead.</td>
</tr>
<tr>
<td><strong>Internal controls</strong></td>
<td>Any policies, procedures, techniques and mechanisms put in place to minimise process failure and help ensure that actions are taken to address risks.</td>
</tr>
<tr>
<td><strong>Likelihood</strong></td>
<td>Used as a general description of probability or frequency.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>Can be expressed qualitatively or quantitatively.</td>
</tr>
</tbody>
</table>
### Definitions continued

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitor/monitoring</strong></td>
<td>To check, supervise, observe critically or measure the progress of an activity, action or system on a regular basis in order to identify change from the performance level required or expected.</td>
</tr>
<tr>
<td><strong>Primary data source</strong></td>
<td>The original (i.e. issuing) source of identity data/information.</td>
</tr>
<tr>
<td><strong>Primary documents</strong></td>
<td>Those that can be used as part of a process for establishing an individual’s identity (e.g. Birth Certificate, Community Services Card, New Zealand Citizenship Certificate. Other types are set out in Appendix A).</td>
</tr>
<tr>
<td><strong>Pseudonymous service</strong></td>
<td>A service that does not require a person to be uniquely identified but requires that the service agency is able to respond to the user. For example, ‘recognise’ the person when he/she accesses the service on return visits.</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>The chance of something happening that will have an impact on objectives. NOTE –</td>
</tr>
<tr>
<td></td>
<td>(1) A risk is often specified in terms of an event or circumstances and consequences that may flow from it.</td>
</tr>
<tr>
<td></td>
<td>(2) Risk is measured in terms of a combination of the consequences of the event and their likelihood.</td>
</tr>
<tr>
<td><strong>Risk profiling</strong></td>
<td>The process of gathering data on characteristics (e.g. customer behaviours) in order to identify categories of risk.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>An activity conducted between a customer and a government agency, in accordance with the functions for which that agency is accountable.</td>
</tr>
<tr>
<td><strong>Supporting documents</strong></td>
<td>Those that can be used to assist in establishing an individual’s identity where an individual is unable to provide ‘primary’ documents (e.g. bank statement, student ID card, utility account. Other types are set out in Appendix B).</td>
</tr>
<tr>
<td><strong>Trusted referee</strong></td>
<td>A person who is asked to confirm the accuracy of identity information supplied by an individual and who confirms that, to their knowledge, the information corresponds to that individual. The two key elements that should exist for a person to be a trusted referee are:</td>
</tr>
<tr>
<td></td>
<td>• They have personal knowledge of the individual being identified</td>
</tr>
<tr>
<td></td>
<td>• They are trusted by the agency according to the agency’s own criteria of sufficient trust.</td>
</tr>
</tbody>
</table>
Part 2
Minimum Standard Requirements
2.1 EOI process overview

Figure 1 provides a high-level overview of the process steps that an agency MUST carry out when implementing any EOI processes for services that require an individual’s identity to be established.

**Figure 1 – Overview of evidence of identity model**

NOTE – Service delivery itself is not within the scope of this Standard. This Standard relates to service delivery only in cases where an EOI process is required before the service can be delivered to an individual.
2.2 Minimum EOI process phases

The main phases of the EOI process shown in Figure 1 are described in Table 2.

Table 2 – Phases of EOI process

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>This phase involves determining the level of identity-related risk within the services that an agency delivers. The results of the identity-related risk assessment will help determine what, if any, EOI process is required for a particular service.</td>
</tr>
<tr>
<td>Design and operation</td>
<td>This phase involves designing EOI processes that are appropriate to the level of identity-related risk (identified during the risk assessment phase) in the particular service. Guidance is provided to ensure operationally appropriate EOI processes are implemented.</td>
</tr>
<tr>
<td>Service delivery</td>
<td>This relates to the delivery of a service by an agency following confirmation of the individual customer’s identity. As such, it is outside of the scope of the standard.</td>
</tr>
<tr>
<td>Monitoring and evaluation</td>
<td>This phase involves the ongoing monitoring of EOI processes and periodic evaluation to ensure that each agency’s EOI business processes and associated outcomes remain consistent with the EOI process objectives that were established as a result of the risk assessment phase.</td>
</tr>
</tbody>
</table>

2.3 Minimum process step requirements

To achieve the minimum requirements of this Standard, agencies MUST ensure that they implement the following process steps. These process steps each form part of one of the process phases listed in Table 2.

Part 3 of this Standard SHOULD be followed by agencies to guide implementation of the minimum process step requirements.

2.3.1 Risk Assessment Phase

The agency MUST undertake an identity-related risk assessment of each of its services. This risk assessment MUST involve the following steps:

Step 1 – Establish the context and objectives for the agency’s services

When defining the context within which a particular service sits, the agency MUST consider, at a minimum, the following factors:

• the business, social, regulatory, cultural, competitive, financial and political environment in which the service exists
• the agency’s key business drivers
• the resources available to the agency (people, systems, processes)
• the impact on stakeholders (both internal and external to the agency).

NOTE – Guidance on how to establish the context and objectives of agency services is provided in 3.3.4.

Step 2 – Carry out an initial risk assessment
The agency MUST determine whether the service results in any of the following:

<table>
<thead>
<tr>
<th>Financial benefit</th>
<th>Will the individual customer receive a financial payment as a result of the service (e.g. payment of a benefit or grant)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-financial benefit</td>
<td>Will the individual customer receive specific other non-financial benefits as a result of the service (e.g. training)?</td>
</tr>
<tr>
<td>Personal information</td>
<td>Will subsequent information about the individual customer be collected and stored by the agency and/or will the service result in the authorised release of personal or sensitive information?</td>
</tr>
<tr>
<td>Subsequent use for EOI</td>
<td>Will the service result in the issue of a document or data source that can be used subsequently, by the customer, as a form of EOI?</td>
</tr>
</tbody>
</table>

A positive answer to one or more of the above requires the agency to carry out a formal risk assessment (Step 3).

If the initial risk assessment shows that the service does not contain identity-related risk, no further application of this Standard is required.

NOTE – Guidance on carrying out initial risk assessments is provided in 3.3.5.

Step 3 – Carry out a formal risk assessment
The agency MUST identify the consequences that could result from the service being delivered to a person whose identity is incorrectly attributed by the agency. Potential consequences MUST be considered from agency, individual, non-government organisation and general public perspectives.

At a minimum, the agency MUST consider the following risk consequences in relation to the particular service:
• inconvenience, distress, or damage to standing or reputation
• financial loss or liability
• harm to agency programmes or the public interest
• unauthorised release of sensitive information
• personal safety
• downstream effects external to the agency.
Having determined whether any of these consequences apply for the particular service, an evaluation MUST be made of the impact level for each consequence.

The agency MUST determine the overall level of identity-related risk in the service, based on the evaluation of the above risk consequences and analysis of the likelihood of these consequences occurring. Following this, the agency MUST align the service’s overall risk rating with one of the following risk categories.

<table>
<thead>
<tr>
<th>Service risk categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil or negligible</td>
<td>Nil identity-related risk in the service or Negligible level of identity-related risk in the service.</td>
</tr>
<tr>
<td>Low</td>
<td>Low level of identity-related risk consequence in the service.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Moderate level of identity-related risk consequence in the service.</td>
</tr>
<tr>
<td>High</td>
<td>High level of identity-related risk consequence in the service.</td>
</tr>
</tbody>
</table>

Where the service fits within the Nil or negligible risk category, no further application of this Standard is required.

Where the service fits within Low to High risk categories, the agency MUST progress to the Design and Operation Phase of the EOI process.

NOTE – Guidance material on how to carry out a formal identity-related risk assessment is provided in 3.3.6.

### 2.3.2 Design and Operation Phase

**Step 1 – Determine required EOI Confidence Level**

The agency MUST determine the level of confidence required in the identity of the individual, in relation to the level of identity-related risk contained in the particular service.

The risk level assessed for a given service corresponds to the level of confidence required by the agency in establishing the individual’s identity.
The different EOI Confidence Levels for services where identity-related risk exists are:

<table>
<thead>
<tr>
<th>Low Identity Risk Service</th>
<th>Low EOI Confidence Level required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate Identity Risk Service</td>
<td>Moderate EOI Confidence Level required</td>
</tr>
<tr>
<td>High Identity Risk Service</td>
<td>High EOI Confidence Level required</td>
</tr>
</tbody>
</table>

**Step 2 – Design and implement EOI process**

The agency MUST design an EOI process that meets the minimum evidential requirements for the required confidence level identified in Step 1.

NOTE –

1. Descriptions of evidential requirements are outlined in Table 8 in Part 3. Guidance on good practice processes to support these evidential requirements is contained in 3.4.7 to 3.4.9.

2. Where an agency currently has an EOI process in place for the particular service, the design step MUST be used to identify and close any gaps between current processes and the minimum requirements of this Standard.

**Step 3 – Ongoing operation of EOI process**

At a minimum, when implementing an EOI process, the agency MUST consider the following operational aspects to ensure that the agency’s ongoing EOI processes meet good practice in each of these areas:

- privacy considerations
- internal controls
- legal considerations
- transition of business processes (if existing processes need to be modified)
- complaints handling
- communication protocols between agencies.

NOTE – Guidance on these considerations is provided in 3.4.16 to 3.4.25.

### 2.3.3 Monitoring and Evaluation Phase

**Step 1 – Develop Monitoring and Evaluation Plan**

Prior to the EOI process being implemented, the agency MUST ensure that monitoring and evaluation processes are in place to enable ongoing effectiveness of operational EOI processes.
Step 1.1 – Design monitoring plan
The agency MUST select appropriate performance indicators for monitoring the EOI process, which will form the basis for later evaluation. The agency's choice of performance indicators MUST take the following, at a minimum, into account:
• cost to the agency
• ability to collect the required data/information
• reliability of the performance indicator.

For each performance indicator, the agency MUST determine the method of collection and analysis of data/information and the frequency with which collection and analysis will take place.

Step 1.2 – Design evaluation plan
In carrying out evaluation processes, the agency MUST, at a minimum, document the following:
• rationale for all EOI business processes
• key EOI process objectives to be achieved and the context within which the evaluation is being conducted
• performance indicators used as a basis for the evaluation
• results that the agency considers represent outcomes – successful or otherwise.

Agencies MUST determine the frequency with which evaluation activities will take place. This decision MUST be made prior to any EOI processes becoming operational.

Step 2 – Implement Monitoring and Evaluation Plan
Once the Monitoring and Evaluation Plan and the EOI processes are operational, the monitoring and evaluation processes outlined in the Plan (see Step 1) MUST commence.

Step 3 – Modify EOI processes if required
Where evaluation suggests EOI processes are not adequately meeting objectives, the agency MUST consider modifying the EOI processes. For any modified EOI processes the following, at a minimum, MUST be undertaken:
• testing modified EOI processes before they become operational
• updating the Monitoring and Evaluation Plan to reflect the modified EOI processes.

NOTE – Guidance on monitoring and evaluation of EOI processes is provided in 3.6.
Part 3
Guidance Material
3.1 Navigating the guidance material

Part 3 of the Standard provides detailed guidance to assist agencies to meet the minimum standard requirements outlined in Part 2. Guidance is provided on each of the required process steps to ensure that the EOI processes are appropriately implemented.

The following provides an overview of the guidance material with the relevant section references.

<table>
<thead>
<tr>
<th>Guidance material</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment Phase</td>
<td>3.3</td>
</tr>
<tr>
<td>General</td>
<td>3.3.1 – 3.3.3</td>
</tr>
<tr>
<td>Step 1 – context and objectives</td>
<td>3.3.4</td>
</tr>
<tr>
<td>Step 2 – initial risk assessment</td>
<td>3.3.5</td>
</tr>
<tr>
<td>Step 3 – formal risk assessment</td>
<td>3.3.6</td>
</tr>
<tr>
<td>Checklist for phase 1 risk assessment</td>
<td>3.3.7</td>
</tr>
<tr>
<td>Design and Operation Phase</td>
<td>3.4</td>
</tr>
<tr>
<td>General</td>
<td>3.4.1</td>
</tr>
<tr>
<td>No ‘one-size-fits-all’ EOI process</td>
<td>3.4.2</td>
</tr>
<tr>
<td>Factors to balance when designing EOI processes</td>
<td>3.4.3</td>
</tr>
<tr>
<td>Minimum process steps required</td>
<td>3.4.4</td>
</tr>
<tr>
<td>Establishing an individual’s identity</td>
<td>3.4.5</td>
</tr>
<tr>
<td>Step 1 – determine EOI confidence level</td>
<td>3.4.6</td>
</tr>
<tr>
<td>Step 2 – design and implement EOI processes</td>
<td>3.4.7</td>
</tr>
<tr>
<td>Name changes</td>
<td>3.4.8</td>
</tr>
<tr>
<td>Identity-related documentation</td>
<td>3.4.9</td>
</tr>
<tr>
<td>Verification of identity data against source data</td>
<td>3.4.10</td>
</tr>
<tr>
<td>Trusted referees</td>
<td>3.4.11</td>
</tr>
<tr>
<td>In-person verification processes</td>
<td>3.4.12</td>
</tr>
<tr>
<td>Dealing with discrepancies</td>
<td>3.4.13</td>
</tr>
<tr>
<td>Investigative interviewing processes</td>
<td>3.4.14</td>
</tr>
<tr>
<td>Handling individual exceptions</td>
<td>3.4.15</td>
</tr>
<tr>
<td>Privacy considerations</td>
<td>3.4.16</td>
</tr>
<tr>
<td>Risk profiling</td>
<td>3.4.17</td>
</tr>
<tr>
<td>Data quality issues</td>
<td>3.4.18</td>
</tr>
<tr>
<td>Agents/persons acting on behalf of individuals</td>
<td>3.4.19</td>
</tr>
<tr>
<td>Step 3 – Ongoing operation of EOI processes</td>
<td>3.4.20</td>
</tr>
<tr>
<td>Internal controls</td>
<td>3.4.21</td>
</tr>
<tr>
<td>Legal considerations</td>
<td>3.4.22</td>
</tr>
</tbody>
</table>
3.2 Core concepts for establishing identity

Identification is the process of associating identity-related data with a particular person. For many services, it is necessary for the agency to uniquely identify the individuals who are seeking to access services they provide. For such services, identity-related risk should be managed, in part, through an appropriate EOI process.

It is not feasible to prove the identity of individuals wanting to access services with complete certainty. This would require an EOI process so cumbersome and intrusive that the costs would greatly outweigh any benefits. This Standard provides a risk-based approach to establishing identity, whereby identity is established with a degree of confidence appropriate to the service being delivered.

The EOI processes outlined in this Standard are based on a component approach to establishing identity. This approach consists of three key components that, if applied as a whole to an individual case, provide confidence that a person actually owns the identity they claim to own.

The three components for establishing identity involve:

1. Evidence that the claimed identity is valid – i.e. that the person was born and, if so, that the owner of that identity is still alive.

2. Evidence that the presenter links to the claimed identity – i.e. that the person claiming the identity is who they say they are and that they are the only claimant of the identity.

3. Evidence that the presenter uses the claimed identity – i.e. that the claimant is operating under this identity within the community.

Agencies SHOULD assess individuals against each of the above components for services that require a moderate to high level of confidence in the individual’s identity (see 3.4.6). This is because each component provides important evidence about distinct aspects of identity. On its own, each component only provides part of the evidential process required to provide confidence that an individual is the true ‘owner’ of their claimed identity.
3.3 Risk assessment phase

3.3.1 General

This section provides guidance for determining the level of identity-related risk within the services that an agency delivers. The results of the identity-related risk assessment will help determine what, if any, EOI process is required for a particular service.

NOTE – For services delivered across the Internet, the level of identity-related risk can also be used to determine the minimum authentication key requirements for ongoing confirmation of identity. Refer to 6.3 of the Guide to Authentication Standards for Online Services.

The material outlined in this section is consistent with the risk assessment process outlined in the Australian/New Zealand Standard Risk Management (AS/NZS 4360:2004) and associated Risk Management Guidelines (SAA/SNZ HB 436:2004) and Information Security Risk Management Guidelines (SAA/SNZ HB 231:2004). As such, this section can be read within the context of this overarching risk management standard. It is noted that for some services, such as those with an international context, other risk management standards (or similar) may be more appropriate.

It is important that identity-related risk assessments are applied to individual services. This is because agencies often carry out multiple services, which have differing types and levels of identity-related risks inherent in them. As such, each service carried out by an agency MUST be subject to an individual identity-related risk assessment. Public service departments are required to adhere to AS/NZS 4360:2004. Identity-related risk assessments should, therefore, be undertaken as part of the wider risk assessment process that agencies undertake in relation to any given service. Those agencies not required to use AS/NZS 4360:2004 and who apply a different risk assessment model, will need to tailor their identity-related risk assessments accordingly.

NOTE – While the identity-related risk assessment MUST be carried out for each service, an agency may then choose to maintain or implement a single EOI process that covers a range of services, providing these services have similar identity-related risks and risk levels.

3.3.1.1 The rationale for identity-related risk assessments

It is important that the New Zealand state sector maintains a high level of integrity in its processes and that only people entitled to certain services receive them. To this end, the identity-related risk assessment is critical so that appropriate EOI processes are designed in relation to the level of identity-related risk for a particular service.
This is important for the following reasons:

• if an agency is collecting too much identity-related information from an individual, relative to the level of identity-related risk in the service, this may be inconsistent with New Zealand’s privacy requirements

• if an agency is collecting too little identity-related information from an individual, relative to the level of identity-related risk in the service, this may result in the agency not achieving its business objectives for the service (e.g. the erosion of confidence in government agencies or identity theft leading to entitlement fraud).

NOTE – In some instances an agency’s EOI requirements may be prescribed in legislation (e.g. the issuance of the New Zealand driver licence provided for in the Land Transport Act 1998).

3.3.1.2 The importance of understanding identity-related risk

Understanding the identity-related risk associated with any given service is required to ensure that the appropriate EOI processes are designed and implemented to manage those identity-related risks.

Some services will have no inherent identity-related risk or will have an acceptable level of identity-related risk associated with them. Therefore, these services will not normally require EOI processes.

Other services will require an EOI process. These EOI processes will vary in their level of comprehensiveness depending on the level of identity-related risk contained in the particular service. In general, the greater the level of inherent identity-related risk for a service, the more comprehensive and stringent the EOI process will need to be.

Sections 3.3.4 to 3.3.6 provide guidance for agencies on how to determine what level, if any, of identity-related risk exists within their services.

Section 3.4 provides guidance for agencies on how to manage identity-related risk within a service through the selection of an appropriate EOI process.
3.3.2 What is identity-related risk?

Identity-related risk is the risk that corresponds to the incorrect attribution of an individual’s identity. Identity-related risk is a component of the overall risk associated with any service.

3.3.2.1 What are some types of identity-related risk?

Types of risk consequences that can arise from the incorrect attribution of identity include, but are not limited to:

- **Inconvenience, distress, or damage to standing or reputation** (e.g. theft and subsequent use of an identity may have a significant impact on the true owner of that identity. The latter’s ability to participate effectively in the community, and to receive the services they are entitled to receive is diminished. Likewise, if an agency provides services on numerous occasions to people claiming false identities, this can negatively affect that agency’s reputation for being able to carry out its functions effectively)

- **Financial loss or liability** (e.g. payment of a financial benefit to any person using a stolen or fictitious identity, who is not entitled to receive that benefit, creates a direct financial loss to the Crown)

- **Harm to agency programmes or the public interest** (e.g. public or political perception that non-eligible people (i.e. those operating under fraudulent identities) are receiving services from agencies leads to loss of agencies’ credibility with the public)

- **Unauthorised release of sensitive information** (e.g. personal information is released to an unauthorised person, thereby impinging on the privacy rights of the person who the information is about)

- **Personal safety** (e.g. theft of an identity enables access to information required to locate and harm a person whose location details are secret)

- **Downstream effects external to the agency** (e.g. an identity-related document issued to a person on the basis of a fictitious identity by one agency is then used to verify their identity for services with other agencies).

These types of risks can have significant impacts on numerous parties, including government agencies, the individuals whose identities have been stolen, other organisations (both government and non-government) and the public. These impacts may be extremely negative for those affected.
3.3.2.2 How can a false identity be established to misuse and abuse an identity?

Identifying identity-related risks requires an understanding of how a person can obtain a false identity to subsequently misuse and abuse an identity. Misuse and abuse of an identity refers to gaining money, goods, services, information or other benefits or the avoidance of obligations through the use of a false identity.

False identities can be established in the following ways:

- creating a fictitious identity
- altering one’s own identity (identity manipulation)
- stealing or assuming a pre-existing identity (identity theft)
- stealing or assuming a pre-existing identity, which is subsequently manipulated.

NOTE –

(1) Identity theft is used to describe the theft or assumption of a pre-existing identity (or significant part thereof) with or without consent, and whether in the case of an individual, the person is alive or dead.

(2) Identity manipulation involves the alteration of one or more elements of identity (e.g. name, date of birth) to dishonestly obtain dual or more access to services or benefits or to avoid establishing obligations.

(3) False identities are created, in some cases, for genuine reasons (e.g. in order to protect an individual from physical harm).

3.3.2.3 Entitlement fraud

Fraud that is not identity-related also occurs but is outside the scope of this Standard. A person may fraudulently gain money, goods, services, other benefits or the avoidance of obligations through the use of their real identity. For example, false declarations of income or personal situation may be made to gain additional welfare benefits that a person is not entitled to. This Standard is not designed to help reduce entitlement fraud risks and agencies will need to have other strategies in place to deal with this type of fraud.
3.3.3 Identity-related risk assessment process

3.3.3.1 Process overview

Figure 2 provides an overview of the risk assessment process steps (see Steps 1 to 3) that agencies MUST follow in order to determine the level of identity-related risk associated with their particular services.

Figure 2 – Overview of risk assessment process

NOTE –

(1) The process steps are broadly based on those outlined in AS/NZS 4360:2004. Refer to that Standard for more detailed information.

(2) Risk assessments will still be required for other reasons (e.g. potential financial implications, potential reputation damage, etc), even if there is no identity-related risk.
Sections 3.3.4 to 3.3.6 provide guidance on how to carry out a risk assessment that focuses specifically on identity-related risk. Illustrative examples are used to assist agencies complete this assessment.

### 3.3.4 Step 1 – Context and objectives

#### 3.3.4.1 Establish the context

For each service, the agency MUST establish the context in which that service is undertaken. Understanding the context is important for determining the service’s exposure to identity-related risk, and the subsequent design of an appropriate EOI process. Agencies may need to balance EOI process design with conflicting objectives.

The context consists of a number of influencing factors. These include:

- the business, social, regulatory, cultural, competitive, financial and political environment in which the service exists
- the agency’s key business drivers
- the resources available to the agency (people, systems, processes)
- the impact on stakeholders (both internal and external to the agency).

The following scenarios illustrate aspects of the context, and how context can impact on identity-related risk, for two services.

<table>
<thead>
<tr>
<th>Scenario 1 – Grant of New Zealand citizenship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context – New Zealand citizenship entitles the recipient to many benefits.</td>
</tr>
<tr>
<td>The criteria for the grant of citizenship are prescribed by legislation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario 2 – Enrolment at university</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context – Enrolment at university entitles the individual to attend university in courses / programmes for which they qualify. Acceptance of an enrolment potentially entitles the individual to financial support and other benefits such as discounted services. Universities are large organisations that are partly funded by government and that have a strong interest in maintaining reputation and excellence.</td>
</tr>
</tbody>
</table>

**NOTE** –

1. Agencies are likely to have already identified the characteristics and nature of their context as part of their existing risk management practice and strategic planning.

2. SAA/SNZ HB 436:2004 provides a good overview of the aspects that, together, establish the context of a particular service – in particular aspects relating to external and internal environments.

---

2 Includes factors listed in 3.3.4.1 and the organisation’s strengths and weaknesses, opportunities and threats. See section 4 (pp. 27-36) of SAA/SNZ HB 436:2004.

3 Includes factors listed in 3.3.4.1 and culture; structure and capital; and goals and objectives and the strategies that are in place to achieve them. See section 4 (pp. 27-36) of SAA/SNZ HB 436:2004.
3.3.4.2 Define the service’s objectives

For each service the agency MUST determine the particular objectives to be achieved through that service. In addition to the context, this provides an important reference point for assessing identity-related risk.

The following are generic examples of different types of objectives for various services:

- that information is made freely available and is also disseminated (e.g. via mail drop) to a particular region
- that a financial benefit be paid only to people who can satisfy the agency of their identity and who meet specific eligibility criteria set by the agency (e.g. income within threshold levels)
- that a licence be issued only to those who have demonstrated they meet all required criteria (e.g. pass a competency test) and who can satisfy the issuing agency of their identity
- that personal information be provided only to a person authorised to receive that information.

The following scenarios illustrate the objectives for two particular services and how these objectives can impact on identity-related risk.

```
Scenario 1 – Grant of New Zealand citizenship
Objectives for this service include:
• that citizenship is granted to only eligible applicants
• that the citizenship process is accessible, fair and user-friendly
• that all processes comply with the Privacy Act 1993
• that the international reputation of NZ citizenship is maintained.

Scenario 2 – Enrolment at university
Objectives for this service include:
• to confirm eligibility for enrolment
• to confirm numbers of students for a range of administrative purposes (e.g. for funding allocation)
• to gather information about what students want, to obtain relevant personal information about the applicants to assist with other objectives (e.g. targeting information about courses on offer, etc).
```

NOTE – As with establishing the context for a service (see 3.3.4.1), it is likely that the objectives for services will already be well understood by the agency.
3.3.5 **Step 2 – Initial risk assessment**

For each service, the agency MUST carry out an initial assessment to determine whether any specific identity-related risk exists, unless it is obvious to the agency that the service does contain identity-related risk. In the latter case, the agency can progress directly to Step 3 (see 3.3.6).

The initial assessment is intended to determine whether progression with a formal identity-related risk assessment is required for a particular service. In practice, there are numerous services carried out by government agencies where it will be clear that they contain either negligible, or no, identity-related risk.

Consideration of the factors set out in Table 3 will assist agencies to identify whether a service has an identity-related risk associated with it.

**Table 3 – Initial risk assessment**

<table>
<thead>
<tr>
<th>Financial benefit</th>
<th>Will the individual customer receive a financial payment as a result of the service (e.g. payment of a benefit or grant)?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-financial benefit</td>
<td>Will the individual customer receive specific, other non-financial benefits as a result of the service (e.g. training)?</td>
</tr>
<tr>
<td>Personal information</td>
<td>Will subsequent information about the individual customer be collected and stored by the agency?</td>
</tr>
<tr>
<td>Subsequent use for EOI</td>
<td>Will the service result in the issue of a document or data source that can be used subsequently by the customer as a form of EOI?</td>
</tr>
</tbody>
</table>

If none of the above applies to the service then it is likely that no EOI process will be required. Therefore, **no further application of the EOI Standard is required for the service.**

As a guide, services that are unlikely to contain identity-related risk (and, therefore, would not normally require an EOI process) include, but are not limited to:

- where the agency is providing non-sensitive information to an individual (e.g. an application form)
- where the agency is providing non-sensitive advice to an individual (e.g. information on how to access services)
- where the individual is making a payment to an agency (e.g. paying a parking fine).

Where a service meets one or more of the criteria in Table 3, a formal identity-related risk assessment is required. For these services, the agency MUST progress to Step 3 (see 3.3.6).
In situations where it is not entirely clear whether a particular service requires a formal identity-related risk assessment, the agency MUST progress that service through a formal identity-related risk assessment (i.e. Step 3 – see 3.3.6).

The following scenarios illustrate an initial risk assessment undertaken for two particular services.

<table>
<thead>
<tr>
<th>Scenario 1 – Grant of New Zealand citizenship</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial benefit?</strong></td>
</tr>
<tr>
<td>No.</td>
</tr>
<tr>
<td>There is no direct financial benefit resulting from the service.</td>
</tr>
<tr>
<td><strong>Non-financial benefit?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>The individual will become a New Zealand citizen and obtain all the rights associated with citizenship.</td>
</tr>
<tr>
<td><strong>Personal information?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>Personal information is collected as an integral part of this service.</td>
</tr>
<tr>
<td><strong>Subsequent use for EOI?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>Citizenship Certificate/record is used to establish identity for other services.</td>
</tr>
<tr>
<td><strong>Given the above results, proceed to Step 3 and undertake a formal assessment of identity-related risk.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenario 2 – Enrolment at university</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial benefit?</strong></td>
</tr>
<tr>
<td>No.</td>
</tr>
<tr>
<td>There is no direct financial benefit resulting from the service.</td>
</tr>
<tr>
<td><strong>Non-financial benefit?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>The individual will be able to access a range of education services if enrolment is accepted.</td>
</tr>
<tr>
<td><strong>Personal information?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>Personal information is collected as an integral part of this service.</td>
</tr>
<tr>
<td><strong>Subsequent use for EOI?</strong></td>
</tr>
<tr>
<td>Yes.</td>
</tr>
<tr>
<td>Proof of enrolment is used as a basis of making a claim to other related services (e.g. applying for a student benefit or loan).</td>
</tr>
<tr>
<td><strong>Given the above results, proceed to Step 3 and undertake a formal assessment of identity-related risk.</strong></td>
</tr>
</tbody>
</table>
3.3.6 Step 3 – Formal risk assessment

Step 3 requires the agency to undertake a formal assessment to determine the level of identity-related risk associated with a given service. The results of this assessment will provide the basis for considering how to manage any identity-related risks identified. This will include identification of the type of EOI process that should be applied for the service.

Figure 3 provides an overview of the process steps an agency needs to follow to carry out a formal identity-related risk assessment for any given agency service.

**Figure 3 – Formal assessment of identity-related risk**
### 3.3.6.1 Identify identity-related risks

During this step, the agency MUST identify the identity-related risks for a particular service.

For each service, an agency needs to identify:
- how different parties may be affected
- which identity-related risk consequences could impact on achievement of its objectives
- the likelihood of those consequences eventuating.

### 3.3.6.2 Who can be affected by the incorrect attribution of identity?

The most obvious identity-related risk associated with services is that a person not entitled to that service receives the benefits of it. This occurs through the incorrect attribution of identity and can impact upon a number of different parties. As part of the identity-related risk assessment, it is important to identify who is affected and to what extent, by any incorrect attribution of identity. Affected parties may include (but are not limited to):

- **Individuals** (e.g. where entitled people apply for a government service and are deemed ineligible because their identity has been used previously by others to claim the same service)
- **Non-government organisations** (e.g. identity-related documents are mistakenly issued to people with false identities and are then used to commit fraud against other agencies)
- **Public** (e.g. where incorrect attribution of identity results in significant losses for agencies and institutions, causing countermeasures to be introduced by those agencies/institutions, with a downstream impact on public charges for those services)
- **Agencies** (e.g. detrimental effect on an agency’s reputation can occur as a result of publicity that the agency has been defrauded by numerous individuals claiming false identities).

### 3.3.6.3 Analyse and evaluate identity-related risk

Overall risk levels are calculated as a combination of consequence and likelihood. This section outlines the process agencies SHOULD follow to determine the identity-related risk consequences (and their level of impact) for a given service.

Many potential risk consequences can arise from the incorrect attribution of identity. These will impact on the parties identified in 3.3.6.2 in a number of different ways and with differing levels of impact or severity.

Table 4 outlines the generic risk consequences that SHOULD be considered in an analysis of identity-related risk. It is not intended as a complete list of possible consequences and agencies MUST continue to be alert to other consequences that could arise. Each risk consequence can potentially impact on numerous parties (e.g. both agencies and individuals).

---

For each risk consequence identified three impact levels – low, moderate and high impact – are described in Table 4.

**Table 4 – Identity-related risk consequences and impacts**

<table>
<thead>
<tr>
<th>Risk consequence</th>
<th>Description</th>
<th>Description of impact levels</th>
</tr>
</thead>
</table>
| Inconvenience, distress, or damage to standing or reputation | The result of incorrect attribution of identity can inconvenience, distress, or damage the standing or reputation of any party in a number of ways. For example, a stolen identity will have a significant impact on an individual in their ability to participate effectively in the community and to receive the services they are entitled to. Widespread misuse and abuse of identity could also potentially impact negatively on the international reputation of New Zealand, leading to a reduction of investment in New Zealand businesses and migration. | **Low** – at worst, limited short-term inconvenience, distress or embarrassment to any party.  
**Moderate** – at worst, serious short-term or limited long-term inconvenience, distress or damage to the standing or reputation of any party (e.g. an individual’s credit rating is unduly affected).  
**High** – severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals, e.g. loss of personal liberty due to error). |
| Financial loss or liability                            | Financial loss or liability as a result of incorrect attribution of identity can cause significant problems for any affected party. For example, a benefit payment to any person who uses a stolen or fictitious identity and who is not entitled to receive that benefit creates a direct financial loss to the Crown. | **Low** – at worst, non-material or inconsequential unrecoverable financial loss to any party, or non-material or inconsequential agency liability.  
**Moderate** – at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.  
**High** – severe or catastrophic unrecoverable financial loss to any party, or severe or catastrophic agency liability. |
<table>
<thead>
<tr>
<th>Risk consequence</th>
<th>Description</th>
<th>Description of impact levels</th>
</tr>
</thead>
</table>
| Harm to agency programmes or the public interest    | Incorrect attribution of identity has the potential to disrupt the effectiveness of agency programmes. This may result in a negative public or political perception that some people are not receiving the services from these agencies that they are entitled to and, vice versa, that people not entitled are receiving agency services. | **Low** – at worst, a limited adverse effect on organisational operations or assets, or public interests. Examples of limited adverse effects are:  
(i) function degradation to the extent and duration that the organisation is able to perform its primary functions with noticeably reduced effectiveness, or  
(ii) minor damage to organisational assets or public interests.  
**Moderate** – at worst, a serious adverse effect on organisational operations or assets, or public interests. Examples of serious adverse effects are:  
(i) significant function degradation to the extent and duration that the organisation is able to perform its primary functions with significantly reduced effectiveness, or  
(ii) significant damage to organisational assets or public interests.  
**High** – a severe or catastrophic adverse effect on organisational operations or assets, or public interests. Examples of severe or catastrophic effects are:  
(i) severe function degradation or loss to the extent and duration that the organisation is unable to perform one or more of its primary functions, or  
(ii) major damage to organisational assets or public interests. |
| Unauthorised release of sensitive information        | Unauthorised release of sensitive information can result in loss of confidence in an agency and directly result in or contribute to negative outcomes (e.g. personal safety, financial loss, job loss) for the affected individual. Personal information needs to be protected and appropriately and closely managed. | **Low** – at worst, a limited release of in-confidence information to unauthorised parties, resulting in a loss of confidentiality with a low impact.  
**Moderate** – at worst, a release of in-confidence or sensitive information to unauthorised parties, resulting in loss of confidentiality with a moderate impact.  
**High** – at worst, a release of in-confidence, sensitive information or information with a National Security classification to unauthorised parties, resulting in loss of confidentiality with a high impact. |
### Risk consequence | Description | Description of impact levels
--- | --- | ---
Personal safety | Incorrect attribution of an identity for an individual can compromise personal safety. For example, an individual incorrectly provided with a driver licence on the basis of another person’s details and who would not qualify on the basis of a driving test can put themselves and/or the public at risk. | **Low** – at worst, minor injury not requiring medical treatment.  
**Moderate** – at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.  
**High** – at worst, risk of serious injury or death.

Downstream effects external to the agency | Incorrect attribution of identity can impact on agencies other than the agency delivering the service. For example, a passport that is issued to a fictitious identity could be used as the basis for fraudulent activities that directly impact on other organisations (both government and non-government). Alternatively, severe downstream consequences may occur if the holder of that passport uses it to engage in a destructive act made possible by using that passport to gain access to another country. | **Low** – at worst, limited short-term effect.  
**Moderate** – at worst, serious short-term or limited long-term effect.  
**High** – at worst, severe or serious long-term effect.

---

It is important to recognise that these consequence categories are often interrelated. In addition, within each of the consequence categories there are likely to be a number of different specific consequences that are affected by factors such as the different customer groups that the agency deals with for the service. As part of any subsequent EOI process that is developed, additional processes based on risk profiling may also need to be developed.

The following scenarios show some of the potential consequences for two services and the level of impact for each consequence.
### Scenario 1 - Grant of New Zealand citizenship

<table>
<thead>
<tr>
<th>Risk consequence</th>
<th>Description of consequence</th>
<th>Impact level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress, or damage to standing or reputation</td>
<td>If a person who has assumed another person’s identity is granted citizenship and uses the assumed identity to commit offences, the legitimate person will suffer inconvenience and distress in having to rectify the situation.</td>
<td>High</td>
</tr>
<tr>
<td>Financial loss or liability</td>
<td>Not applicable for this service. However, downstream consequences may result in financial loss for other agencies (e.g. where New Zealand citizenship is part of the eligibility criteria for another service).</td>
<td>N/A</td>
</tr>
<tr>
<td>Harm to agency programmes or public interest</td>
<td>If citizenship processes are perceived to be inadequate this could lead to a loss of public confidence in the granting of citizenship process.</td>
<td>High</td>
</tr>
<tr>
<td>Unauthorised release of sensitive information</td>
<td>Citizenship Officer provides information to an unauthorised agent who uses that information to track down an individual for negative purposes.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Personal safety</td>
<td>Citizenship is granted to a person who is using a false identity. This citizenship is then used to obtain a passport that could be used to travel internationally to commit offences such as a terrorist act.</td>
<td>High</td>
</tr>
<tr>
<td>Downstream effects external to the agency</td>
<td>A person is granted citizenship on the basis of a false identity and then receives services from various agencies using their Citizenship Certificate as evidence of their identity.</td>
<td>High</td>
</tr>
</tbody>
</table>

### Scenario 2 – Enrolment at university

<table>
<thead>
<tr>
<th>Risk consequence</th>
<th>Description of consequence</th>
<th>Impact level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress, or damage to standing or reputation</td>
<td>If individuals are able to enrol under false identities on a regular basis this could lead to reputation damage for universities.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Financial loss or liability</td>
<td>If enrolments are made on the basis of false identities, this could lead to incorrect funding by the Crown for invalid enrolments.</td>
<td>Low-Moderate</td>
</tr>
<tr>
<td>Harm to agency programmes or public interest</td>
<td>If enrolment processes are perceived to be inadequate this could erode public confidence in universities’ programmes generally.</td>
<td>Moderate</td>
</tr>
<tr>
<td>Unauthorised release of sensitive information</td>
<td>If academic information is released to people claiming to be the ‘owner’ of that information, this could lead to individuals claiming to be the holder of certain qualifications and gaining employment on the basis of those qualifications (e.g. medical practitioners)</td>
<td>Low</td>
</tr>
<tr>
<td>Personal safety</td>
<td>No identifiable risks.</td>
<td>Low</td>
</tr>
<tr>
<td>Downstream effects external to the agency</td>
<td>Successful enrolments are used as the basis for a number of subsequent government services, such as accessing student allowances and loans.</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Having analysed the impact levels for each risk consequence category, the agency SHOULD then determine the overall impact level in relation to the risk consequences. In doing this evaluation the agency SHOULD determine if any risks are more significant than others for the particular service. As a general premise, however, the highest impact level for any of the risk consequence categories will indicate what the overall impact level for the service should be.

**Scenario 1 – Grant of New Zealand citizenship**

Avoiding loss of reputation will be particularly important. One of the reasons for this is that the maintenance of a good international reputation for New Zealand citizenship impacts positively on New Zealanders’ ability to travel freely internationally. As such, this consequence category will need to be given considerable weighting within the overall risk evaluation.

The results shown in the previous citizenship scenario suggest that, overall, the identity-related risk consequences for this service are high.

**Scenario 2 – Enrolment at university**

Maintaining integrity in the New Zealand university system is important. One objective concerning this integrity is to ensure that only individuals who have met prerequisites for entry are enrolled. This will ensure that the correct individuals are matched with their evidence of achievement of those standards. In addition, it is important that the identity of individuals is correctly attributed, as being a student confers a wide range of non-financial (i.e. access to education services) and financial benefits.

The results shown in the previous education scenario suggest that, overall, the identity-related risk consequences for this service are moderate.

3.3.6.4 **Evaluating likelihood**

Overall risk levels are calculated as a combination of consequence and likelihood. Having evaluated the risk consequences for a particular service in 3.3.6.3 the agency SHOULD then assess the likelihood of these consequences occurring.

The extent to which an agency will be able to accurately establish the likelihoods associated with unwanted consequences will vary. However, the following methods may help:

- experience of other services conducted by the agency that have similar identity-related risk exposures
- experience of other agencies’ services that have similar identity-related risk exposures
- relevant published data on the likelihood of particular identity-related consequences occurring for particular service types
- availability of specialist and expert advice.
An agency SHOULD make likelihood assessments according to whatever scale it deems most appropriate to the services being considered. Overall levels for consequence, likelihood and overall risk SHOULD be calculated using the agency’s chosen risk methodology. Wherever possible scales SHOULD be consistent so that different identity-related risks can be compared and EOI processes tailored accordingly. Examples of such scales are included in section 6 of SAA/SNZ HB 436:2004.

Where an agency’s identity-related risk assessments contain significant uncertainty, the agency SHOULD carry out a sensitivity analysis to test the effect of this uncertainty (see section 6 (pp. 46-61) of SAA/SNZ HB 436:2004 for more information on sensitivity analysis).

3.3.6.5 Assessing a service’s overall identity-related risk level

The following scenarios provide an assessment of the overall identity-related risk associated with the granting of citizenship and enrolment at university. In addition to Not Applicable, a three-point scale of Unlikely, Possible and Likely is used in the following scenarios.
### Scenario 1 – Grant of New Zealand citizenship

<table>
<thead>
<tr>
<th>Consequence category</th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress, or damage to standing or reputation</td>
<td>High</td>
<td>Possible</td>
<td>High</td>
</tr>
<tr>
<td>Financial loss or liability</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Harm to agency programmes or public interest</td>
<td>High</td>
<td>Possible</td>
<td>High</td>
</tr>
<tr>
<td>Unauthorised release of sensitive information</td>
<td>Moderate</td>
<td>Unlikely</td>
<td>Low-Moderate</td>
</tr>
<tr>
<td>Personal safety</td>
<td>High</td>
<td>Unlikely</td>
<td>Moderate</td>
</tr>
<tr>
<td>Downstream effects external to the agency</td>
<td>High</td>
<td>Possible</td>
<td>High</td>
</tr>
</tbody>
</table>

**Overall Levels**

<table>
<thead>
<tr>
<th></th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Possible</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

### Scenario 2 – Enrolment at university

<table>
<thead>
<tr>
<th>Consequence category</th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress, or damage to standing or reputation</td>
<td>Moderate</td>
<td>Unlikely</td>
<td>Low-Moderate</td>
</tr>
<tr>
<td>Financial loss or liability</td>
<td>Low-Moderate</td>
<td>Unlikely</td>
<td>Low-Moderate</td>
</tr>
<tr>
<td>Harm to agency programmes or public interest</td>
<td>Moderate</td>
<td>Unlikely</td>
<td>Low-Moderate</td>
</tr>
<tr>
<td>Unauthorised release of sensitive information</td>
<td>Low</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>Personal safety</td>
<td>Low</td>
<td>Unlikely</td>
<td>Low</td>
</tr>
<tr>
<td>Downstream effects external to the agency</td>
<td>Moderate</td>
<td>Unlikely</td>
<td>Low-Moderate</td>
</tr>
</tbody>
</table>

**Overall Levels**

<table>
<thead>
<tr>
<th></th>
<th>Consequence</th>
<th>Likelihood</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Moderate</strong></td>
<td>Unlikely</td>
<td>Low-Moderate</td>
<td></td>
</tr>
</tbody>
</table>

### 3.3.6.6 Assigning a service risk category

Having determined the service’s risk level, the agency MUST allocate the service to a service risk category. This will enable the agency to determine what level of stringency of EOI process is required for the particular service.
Table 5 outlines four service risk categories. This scale will later be used to align services with particular identity-related risk levels to the appropriate levels of required confidence in a customer’s identity. To do this, the agency SHOULD use the overall level of risk associated with the service to assign the appropriate service risk category in Table 5.

NOTE – For services delivered across the Internet, these service risk categories can also be used to determine the minimum authentication key requirements for ongoing confirmation of identity. Refer to 6.3 of the Guide to Authentication Standards for Online Services.

### Table 5 – Service risk categories

<table>
<thead>
<tr>
<th>Service risk categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nil or negligible risk</td>
<td>Nil identity-related risk in the service – this is sometimes referred to as an ‘anonymous’ service</td>
</tr>
<tr>
<td></td>
<td><strong>Negligible</strong> identity-related risk in the service – this is sometimes referred to as a ‘pseudonymous’ service.</td>
</tr>
<tr>
<td>Low risk</td>
<td><strong>Low</strong> level of identity-related risk in the service.</td>
</tr>
<tr>
<td>Moderate risk</td>
<td><strong>Moderate</strong> level of identity-related risk in the service.</td>
</tr>
<tr>
<td>High risk</td>
<td><strong>High</strong> level of identity-related risk in the service.</td>
</tr>
</tbody>
</table>

#### 3.3.6.7 Translating service risk categories to appropriate EOI process

The service risk levels (as determined in 3.3.6.5) correspond with the levels of confidence required by the agency in the individual’s identity.

Determining the level of confidence required in an individual’s identity is based on the premise that a higher level of identity-related risk consequence in a service will require a correspondingly higher degree of confidence in the validity of the claimed identity. The following scenarios illustrate the overall assessment of service risk category for two services.

**Scenario 1 – Grant of New Zealand citizenship**

The service risk consequence level was assessed to be High. This indicates that a high level of confidence in the asserted identity’s validity is required.

**Scenario 2 – Enrolment at university**

The service risk consequence level was assessed to be Low-Moderate. This indicates that a moderate level of confidence in the asserted identity’s validity is required.

NOTE – Applying the appropriate (EOI) Confidence Level to a service is an important aspect of the management of identity-related risk. However, this is not the only means of managing identity-related risks, and agencies SHOULD also determine any other mitigation strategies required to manage the service’s identity-related risk (see 3.4).
Table 6 outlines the translation between the service risk consequence level and the EOI Confidence Level required. Full descriptions of EOI Confidence Levels are outlined in 3.4.6 and the processes for each are outlined in 3.4.7.

**Table 6 – Matching service risk categories to EOI Confidence Levels**

<table>
<thead>
<tr>
<th>Low Identity Risk Service</th>
<th>Low EOI Confidence Level required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate Identity Risk Service</td>
<td>Moderate EOI Confidence Level required</td>
</tr>
<tr>
<td>High Identity Risk Service</td>
<td>High EOI Confidence Level required</td>
</tr>
</tbody>
</table>

NOTE – Services described as having Nil or negligible risk in Table 5 do not require an EOI process and, therefore, do not appear in Table 6.

The following scenarios illustrate the overall assessment of EOI Confidence Level required for two services.

**Scenario 1 – Grant of New Zealand citizenship**

The service risk level was assessed to be High. This translates to a requirement for a High EOI Confidence Level process.

**Scenario 2 – Enrolment at university**

The service risk level was assessed to be Low-Moderate. This translates to a requirement for a Moderate EOI Confidence Level process.

### 3.3.6.8 Services with existing EOI processes

Having completed an assessment of identity-related risk associated with a particular service, the agency SHOULD benchmark any existing EOI processes against those in 3.4 of this Standard to determine what, if any, change is required to bring the current EOI process into alignment with this Standard.

### 3.3.6.9 New services

Where an agency is implementing a new service, the agency SHOULD design EOI processes based on the assessment of identity-related risk for that service, as described in 3.3.5 and 3.3.6, and the relationship between such risks and levels of confidence shown in Table 6.

The types of EOI processes required to meet each of the EOI Confidence Levels are outlined in 3.4.7.
### 3.3.7 Checklist for Phase 1 Risk Assessment

Checklist for ................................................................. (service name)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Date when completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Context and objectives for service defined and documented</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Initial identity-related risk assessment for service documented</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Formal risk assessment for services with identity-related risk:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Risk consequence categories evaluated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Overall risk level assessed and Service Risk Category determined</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Monitor, evaluate and review on .......................................................</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Revisit identity-related risk assessment on .......................................</td>
<td></td>
</tr>
</tbody>
</table>
3.4 Design and operation phase

3.4.1 General

This section provides guidance on:

- the design of EOI processes that are appropriate to the level of identity-related risk in the particular service (the level of identity-related risk in a particular service will have been determined during the Risk Assessment Phase)
- the operational requirements for EOI processes.

NOTE – A Monitoring and Evaluation Plan MUST be completed before an EOI process becomes operational (see 3.6.3).

This section covers the specific core areas that agencies need to be familiar with when designing their EOI processes and making them operational. These include:

- the EOI objectives to be met to identify an individual for particular services (see 3.4.5.1)
- generic EOI processes for providing three different levels of confidence in an individual’s identity (see 3.4.7)
- operational considerations for EOI processes (see 3.4.20).

3.4.2 No ‘one-size-fits-all’ EOI process

There is no ‘one-size-fits-all’ EOI process that can be applied to all services requiring identity to be established. The reasons for this include:

- if a uniform approach were taken, it would risk ‘ratcheting up’ EOI processes for all government services to the level of services requiring a high level of confidence in an individual’s identity. This would be unduly costly for lower risk services that do not warrant such a high level of confidence in an individual’s identity (e.g. a ‘passport’ level EOI process would be inappropriate for joining a public library) and unnecessarily invasive of individuals’ privacy
- not everyone can access the same identity documentation (e.g. non-New Zealand citizens who have different documentation available than New Zealand citizens). A set of uniform EOI requirements may unnecessarily restrict access to certain government services for some people
- each agency has different contexts and objectives that need to be considered when designing appropriate EOI processes.
EOI processes lie across a wide spectrum of needs, ranging from a situation where relatively little EOI is required (e.g. applying for a library card) to one where a significant amount of evidence is required (e.g. applying for New Zealand citizenship). Accordingly, this Standard defines ‘generic’ EOI processes to meet three Confidence Levels – High, Moderate and Low – that are aligned to the assessed level of identity-related risk for a particular service.

### 3.4.3 Factors to balance when designing EOI processes

Agencies are expected to design EOI processes that are tailored to their own business requirements when deciding how to implement the relevant EOI confidence level requirements. This involves considering a number of factors and agencies SHOULD undertake a cost/benefit analysis to determine the design features of their EOI processes. Examples of the types of factors that SHOULD be considered as part of this analysis are:

- **Acceptability** – the EOI process SHOULD be generally acceptable to customers, taking into account the different needs of individuals and avoiding the creation of unnecessary barriers. The process SHOULD be convenient, easy to use and as non-intrusive as possible, with due regard to the level of identity-related risk for the service.

- **Legal compliance** – the EOI process MUST comply with relevant New Zealand law, including the Privacy Act 1993, the Human Rights Act 1993, the Public Records Act 2005 and any authorising legislation for the particular service.

- **Security and privacy** – suitable protection MUST be provided for information owned by both individuals and the Crown, and an individual’s right to privacy MUST be appropriately protected.

- **Affordability, reliability and timeliness** – the EOI process SHOULD be affordable, reliable and should not create unnecessary delays for either individuals or government agencies.

It is also likely that EOI processes will be subject to ongoing amendment and modification to take account of environmental changes (e.g. policy changes, new information about methods of misuse and abuse of identity, changes in the processes to obtain identity-related documents, new technologies, etc – see section 3.6).
3.4.4 Minimum process steps required

Figure 4 provides an overview of the steps that agencies MUST follow for design and operation of their EOI processes.

Where an agency already has an EOI process in place for a particular service, it MUST assess that process against the requirements set out in this section. If the current process does not meet the design and operational requirements herein, appropriate changes MUST be made.

**Figure 4 – Overview of the design and operation phase**
3.4.5 Establishing an individual's identity

Establishing an individual’s identity through business processes that are repeatable is challenging. This is particularly so given that:

- the person whose identity is to be established will generally not be known to the person(s) administering the EOI process
- not everyone will have the same documents/records available to assist in establishing their identity
- increasing the certainty about an individual’s identity can involve increasing cost, time and effort for both the individual and the agency.

Further guidance on how identity can be established as a repeatable business process while not over-exposing the agency to excessive cost or risk is set out in 3.4.7 and 3.4.20.

3.4.5.1 EOI objectives

Verifying an individual’s identity involves a number of different components, each of which achieves a different purpose. Figure 5 illustrates each of the components that form the foundation for an agency to establish an individual’s identity.

Figure 5 – Evidence of identity objectives

Not all of the objectives in Figure 5 will necessarily need to be satisfied to establish an individual’s identity. EOI requirements will depend on the level of confidence in the identity that is required for the particular service. For low risk services, not all objectives will need a separate process. For example, enough confidence will be gained in a customer’s identity for a low risk service by just meeting objectives A, D, and E. However, all objectives will need to be specifically met for a high risk service. This is detailed in section 3.4.7 of this Standard.
3.4.6 **Step 1 – Determine EOI Confidence Level**

As part of the risk assessment process an assessment is required about the level of identity-related risk attributable in each service delivered by a particular agency. Four identity-related risk categories are described (see Table 5). Of these risk categories, the lowest category of risk (Category 0) requires no specific EOI process.

The risk level assessed for a given service corresponds to the level of confidence required by the agency in establishing the individual’s identity. Table 7 outlines the EOI Confidence Level required for services where identity-related risk exists.

**Table 7 – Matching risk level to appropriate EOI Confidence Level process**

<table>
<thead>
<tr>
<th>Low Identity Risk Service</th>
<th>Low EOI Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>This service level contains a <em>low</em> level of overall identity-related risk, (service example – the issue of a library card).</td>
<td>The minimum required level of confidence in the individual’s identity is <em>low</em>. The agency only requires evidence that the identity claimed by the individual is a genuine identity, that the presenting individual is the sole claimant, and that the individual claiming the identity uses that identity in the community. EOI provided is accepted by the agency at ‘face value’ without third-party verification unless the agency has cause to suspect that the information provided might not be correct, e.g. if it finds discrepancies in EOI provided.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moderate Identity Risk Service</th>
<th>Moderate EOI Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>This service level contains a <em>moderate</em> level of overall identity-related risk, (service examples – enrolment at a university or the payment of a short-term or one-off financial benefit).</td>
<td>The minimum required level of confidence in the individual’s identity is <em>moderate</em>. The agency requires evidence that the identity claimed by the individual is a genuine identity, that the presenting individual is the sole claimant of the identity, and (if required) that the individual uses that identity in the community. EOI provided is accepted by the agency at ‘face value’ without third-party verification unless the agency identifies discrepancies in the EOI provided by the individual).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Identity Risk Service</th>
<th>High EOI Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>This service level contains a <em>high</em> level of overall identity-related risk, (service examples – the issue of a passport, the issue of a firearms licence, or the issue of permanent residence status).</td>
<td>The minimum required level of confidence in the individual’s identity is <em>high</em>. The agency requires evidence that the identity exists, that the presenting individual is the sole claimant of the identity, and that the individual uses that identity in the community. EOI provided by the individual is, where possible, verified with a third party to confirm its authenticity.</td>
</tr>
</tbody>
</table>

NOTE – For greater detail see Table 8.

It is important to recognise that risk categories and EOI Confidence Levels for services, as outlined in Table 7, are interdependent. In practice, each category and level sits on two continuums of ‘identity-related risk’ and ‘confidence in identity’ respectively. An agency’s placement of a service in one of the above categories provides a useful way of determining what level of confidence is required in customer identities. However, where an agency’s...
service does not fit neatly within one category, or where strict adherence to a particular EOI Confidence Level process is not possible (for example, due to a service’s customer base being made up of minors), the agency will need to take a more practical approach.

NOTE – Where relevant, agencies will need to comply with any legislative requirements that prevent adoption of particular EOI processes (e.g. where the EOI requirements for a particular service are outlined in legislation and cannot be altered without legislative amendment).

3.4.7 Step 2 – Design and implement EOI processes

3.4.7.1 EOI requirements associated with each EOI Confidence Level

Figure 6 provides an overview of the generic processes that an agency will undertake when establishing an individual’s identity. Each EOI Confidence Level requires identity-related objectives to be met to different degrees of assurance and with different levels of process complexity.

Figure 6 – Overview of generic business processes for establishing an individual’s identity
Table 8 outlines the evidential requirements for meeting each of the three EOI Confidence Levels. In some cases, such as when discrepancies are found in the identity-related details provided by an individual, an agency might have cause to suspect that claims of identity made by an individual are not genuine. In these situations, the agency may wish to apply requirements from a higher Confidence Level process to the individual case to resolve those discrepancies.

**Table 8 – Evidential requirements for EOI Confidence Level processes**

<table>
<thead>
<tr>
<th>EOI objective</th>
<th>Low EOI Confidence Level</th>
<th>Moderate EOI Confidence Level</th>
<th>High EOI Confidence Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>A – Identity exists</td>
<td>1 document</td>
<td>1-2 documents (including at least one with photograph, if possible)</td>
<td>1-2 documents (including at least one with photograph, if possible) or Verification against 1-2 source records held by issuing agency</td>
</tr>
<tr>
<td>B – Identity is a ‘living identity’</td>
<td>(No specific process)</td>
<td>(No specific process)</td>
<td>Verification against the death register or Business processes for Objective C</td>
</tr>
<tr>
<td>C – Presenter ‘links’ to identity</td>
<td>(No specific process)</td>
<td>Verification by trusted referee or In-person verification</td>
<td>Verification by trusted referee or In-person verification or Biometric recognition where the agency has authorised access to a database containing the individual’s biometric information and Interview (in cases where suspicion is raised over individual’s identity)</td>
</tr>
<tr>
<td>D – Presenter is sole claimant of identity</td>
<td>Check against agency records</td>
<td>Check against agency records</td>
<td>Check against agency records</td>
</tr>
<tr>
<td>E – Presenter uses identity</td>
<td>At least 1 document/record</td>
<td>At least 1 document/record or Business processes for Objective C</td>
<td>At least 2 documents/records or Business processes for Objective C</td>
</tr>
</tbody>
</table>

Further information on what is entailed in meeting the evidential requirements for each EOI objective in Table 8 is set out in 3.4.7.2 to 3.4.7.6. Appendices A to C also provide information on each document/record referred to in meeting Objectives A to E. Details include:
• features of the document/record
• operational and legislative requirements associated with the document/record (where applicable) and the processes involved before issue or registration
• how using the document/record will help meet the requirements in this Standard.

3.4.7.2 Objective A – The identity exists

For all Confidence Level Processes
Documents/records that can be used to satisfy Objective A include those set out in Table 9. The number and type of documents required will vary depending on the EOI Confidence Level required for the service.

Table 9 – Documents/records used to satisfy Objective A

<table>
<thead>
<tr>
<th>Document/record</th>
<th>Issuing agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand passport*</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Certificate of Identity (issued to non-New Zealand citizens who cannot obtain a passport from their country of origin)*</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Certificate of Identity (issued to people who have refugee status)*</td>
<td>Department of Labour (Immigration)</td>
</tr>
<tr>
<td>New Zealand Refugee Travel Document (RTD)*</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>Emergency Travel Document (ETD)*</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>Firearms Licence*</td>
<td>New Zealand Police</td>
</tr>
<tr>
<td>Overseas passport (with New Zealand immigration visa/permit)*</td>
<td>Relevant Authority in country of issue (visa/permit to be issued by Department of Labour (Immigration)).</td>
</tr>
<tr>
<td>New Zealand Full Birth Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Citizenship Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
</tbody>
</table>

* Document/record contains a photograph of the holder.

For High and Moderate EOI Confidence Level processes
Staff SHOULD be specifically trained in document recognition (see 3.4.9).
For High EOI Confidence Level process only
Verification (where possible) of identity information with the primary source of records will provide added confidence for Objective A. This involves confirming with the issuing agency that the identity data contained on the identity document(s) or details provided correspond to a valid record.

NOTE –
(1) Depending on the service, an agency may not require an individual to provide a document (i.e., it may be appropriate in some cases for an individual to just provide the agency with relevant data about their identity, which the agency then verifies against source records – for example birth details). However, this verification MUST be subject to legislative authority and electronic verification will require resolution of any technical issues (see 3.4.10).

(2) Verification with an overseas primary data source will not be possible in most cases. Therefore, training in authentic document recognition is important for providing a high level of confidence.

3.4.7.3 Objective B – Identity is a ‘living’ identity
For Low and Moderate EOI Confidence Level processes
No specific process is required for this objective.

For Moderate EOI Confidence Level, this objective will be satisfied by the business processes undertaken to meet Objectives A and C.

For High EOI Confidence Level process only
Where possible an agency SHOULD verify against the New Zealand Death Register (administered by Department of Internal Affairs) that no death record matches the claimed identity. Checking the Death Register reduces the possibility of an individual using the identity of a deceased person.

Agencies need to be aware, however, that only deaths that occur within New Zealand are recorded on the Death Register. New Zealanders who die outside New Zealand will not necessarily be identified through a check against the New Zealand Death Register. Therefore, it is possible for New Zealand citizens who have died in another country to have their identities stolen and used by another individual.

Verification against the New Zealand Death Register MUST be subject to legislative authority and electronic verification will involve resolution of any technical and legislative issues (see 3.4.10).
3.4.7.4  **Objective C – Presenter ‘links’ to identity**

Determining that a presenter ‘links’ to an identity is particularly challenging, but is a vital aspect of identity verification processes.

Business processes used to satisfy Objective C include the following:

**For Low EOI Confidence Level process**

No specific process is required. For services where there is a low level of identity-related risk, enough confidence is gained in the individual’s identity through their provision of documents/records that meet Objectives A and E. That is, the agency is able to gain enough confidence in their identity by the fact that an individual has been able to provide EOI to meet these objectives and the individual is not being inconvenienced to a level unreasonable for the low level of identity-related risk within the service being sought.

**For High and Moderate EOI Confidence Level processes**

One or both of the following may be used. For greater confidence both SHOULD be used.

**Trusted referee corroboration** (detailed in 3.4.11)

- This requires an individual to provide:
  - photograph(s) verified by a trusted referee or
  - verification by a trusted referee that the person applying for the service is the same person as indicated by the identification document(s)/records provided to satisfy Objective A.

**In-person verification** (detailed in 3.4.12)

- This requires an individual to appear in-person with:
  - a recent photograph verified by a trusted referee or
  - a photo identification document (from the list of photo identification documents records used to satisfy Objective A).

Where a service requires individuals to physically present themselves to register for a particular service, then in-person processes for EOI may be desirable. Establishing an individual’s identity can be undertaken as part of the overall service delivery process.

However, in many cases an individual is not required to be physically present in order to determine their entitlement for the particular service. In these cases service entitlement may be more efficiently determined through other channels (e.g. phone, email, mail, online applications). In addition, very few agencies support national networks of physical offices. Therefore, without creating widespread infrastructure, in-person verification processes will not be possible. In these cases, agencies SHOULD use other options for satisfying Objective C.

**NOTE** – Biometric recognition software may be used to assist with recognition processes, where the agency already has authorised access to trusted biometric information about the individual against which to match the individual.
For High EOI Confidence Level process only

Interviewing (detailed in 3.4.14)

- Where any discrepancy with a claimed identity is identified, and depending on the assessed level of risk associated with the individual case, the agency may require the individual to attend an interview with its staff.

3.4.7.5 Objective D – Presenter is sole claimant of identity

For all EOI Confidence Level processes

To fulfil this objective the agency SHOULD check the presenter’s details (potentially including biometric information) against their customer records, to ensure that no other individual has claimed the same identity for that service.

Where a duplication of the claimed identity is discovered, the agency SHOULD refer the case for further investigation and, if necessary, amend its database records (see 3.4.21). It is important to be aware that duplication of identity records will not necessarily be the result of a fraudulent application. For example, it may have occurred through legitimately duplicate identity details or administrative error.

3.4.7.6 Objective E – Individual uses the identity in the community

For all EOI Confidence Level processes

The aim of Objective E is to provide further confidence about an individual’s claimed identity. In particular, Objective E is concerned with demonstrating the consistent use of the claimed identity. Documents/records that are used to satisfy Objective E are intended to be used for the corroboration of identity information provided to meet Objective A. As a guide, these documents/records SHOULD be from a trustworthy source, be dated, and include the name and, where appropriate, address of the person applying for the service.

Table 10 lists documents/records that SHOULD be used, where possible, to meet Objective E. The process behind the issue of documents listed in Table 10 is outlined in Appendix A. Agencies SHOULD contact the Custodian of this Standard with any queries relating to the current issue status of any document listed in Table 10.

More information on handling identity-related documents is set out in 3.4.16.1.

Table 10 – Documents/records used to satisfy Objective E

<table>
<thead>
<tr>
<th>Document/record</th>
<th>Issuing agency/organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand Driver Licence*</td>
<td>Land Transport New Zealand</td>
</tr>
<tr>
<td>18+ Card*</td>
<td>Hotel Association of New Zealand</td>
</tr>
<tr>
<td>Community Services Card</td>
<td>Ministry of Social Development</td>
</tr>
<tr>
<td>IR Number</td>
<td>Inland Revenue</td>
</tr>
<tr>
<td>Electoral Roll Record</td>
<td>Ministry of Justice</td>
</tr>
</tbody>
</table>

* Document/record contains a photograph of the holder.
Table 11 lists documents/records that can be used to fulfill requirements for Objective E, where documents/records listed in Table 10 cannot be provided. Some of the listed documents may also be used where address details are required. Further details about these documents/records is provided in Appendix B. Agencies SHOULD contact the Custodian of this Standard with any queries relating to the current issue status of any document listed in Table 11.

Table 11 – ‘Supporting’ documents/records used to satisfy Objective E

<table>
<thead>
<tr>
<th>Document/record</th>
<th>Issuing agency/organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit cards, bank cards and financial accounts</td>
<td>Banks</td>
</tr>
<tr>
<td>International Driving Permit*</td>
<td>Automobile Association of New Zealand</td>
</tr>
<tr>
<td>Confirmation of Permit Status</td>
<td>Department of Labour (Immigration)</td>
</tr>
<tr>
<td>Steps to Freedom Form</td>
<td>Department of Corrections</td>
</tr>
<tr>
<td>Student Identity Cards* or Employee Identification Cards*</td>
<td>Secondary schools and tertiary institutions, and employers</td>
</tr>
<tr>
<td>Utility accounts</td>
<td>Utility companies (e.g. telecommunication, electricity and gas power providers)</td>
</tr>
</tbody>
</table>

* Document/record contains a photograph of the holder.

Tables 10 and 11 do not provide a complete list of documents/records that could be used to meet Objective E. Agencies may choose to accept other types of documents/records to meet Objective E. The issuing process behind documents/records accepted by an agency is analysed to ensure a particular document/record provides adequate confidence to the agency regarding Objective E.

Some of the documents listed in Tables 10 and 11 provide information about a person (such as their bank account or academic record) that is not core identity information (e.g. name, date of birth and place of birth). Agencies need be particularly careful to ensure that only information appropriate to establishing identity is accessed. In cases where the agency requires certain documentation to establish both identity and entitlement to the service, the individual MUST be made aware of the dual purposes for which the documentation is required.

For a number of services, a person’s address may be required in order to progress to service delivery. For such services, requiring individuals to provide documents/records that meet Objective E but that also contain address information will both add confidence in the person’s identity, while at the same time providing address information. This can reduce the total number of documents/records that the person has to provide for a particular service.
The Objective E requirements SHOULD also be flexible enough to ensure a reasonable amount of choice for the individual. For example, individuals SHOULD be able to choose to provide alternative information as EOI rather than provide sensitive personal information such as financial or health information.

Agencies SHOULD also assess the appropriateness of keeping copies of identity-related documents against either recording the core identity-related information from those documents or simply recording that the document or data source was sighted, on what date, and by which staff member. Keeping such copies imposes a responsibility on the agency to protect the copies and the information they contain, while simply recording that the document has been sighted carries no additional responsibility.

### 3.4.8 Name changes

In many situations it is legitimate for individuals to use whatever name they choose. For moderate to high-risk services, agencies will need to balance this choice against their objective of ensuring that the presenting person is the legitimate claimant of a particular identity. Therefore, where an individual is operating under a different name to that on a document they have provided to meet Objective A, the individual SHOULD also be asked to provide information that links their current name to their previous name. The documents/records listed in Table 12 are forms of evidence that will, in many cases, enable this linkage to be made.

**Table 12 – Documents/records used to establish name usage**

<table>
<thead>
<tr>
<th>Document/record</th>
<th>Issuing agency/organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change of Name by Statutory Declaration</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>Change of Name by Deed Poll</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Marriage Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Civil Union Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
</tr>
<tr>
<td>New Zealand Divorce Papers</td>
<td>Ministry of Justice</td>
</tr>
<tr>
<td>Certificate of Annulment</td>
<td>Ministry of Justice</td>
</tr>
</tbody>
</table>

While an agency may need to establish the linkage between the names originally and currently used by an individual, this should not prevent the individual’s ability to be known by their ‘preferred name’ during subsequent contact with the agency.

See Appendix C for further information regarding name change.
3.4.9 Identity-related documentation

Technological advancements such as digital colour printers facilitate the alteration or forging of identity documents. In order to establish individual identities, agencies often require more than one identity-related document, as no single document can currently meet all of the objectives required to establish identity to any level of confidence. For example, a passport does not provide evidence that an individual uses their claimed identity within the community, just as a birth record does not link an individual to the particular identity listed in a record.

3.4.9.1 Types of identity-related documents

For convenience, identity-related documents can be categorised into two types:

- evidence that the identity exists (Objective A documents/records)
- evidence the identity is being actively used within the community (Objective E documents/records).

Identity-related documents are official documents that record a person’s attributed identity, such as a birth certificate, or which contain an individual’s signature and/or photograph (the validity of which has been verified in some way) such as a passport. Documents/records that provide evidence that the person uses the claimed identity in the community are required to provide further corroboration of the individual’s identity.

NOTE – Agencies will need to set their own policies on the specific document/record combinations required (for meeting Objectives A and E). It is important that agencies develop processes for exceptions, where the documents required to meet Objectives A and E cannot be provided by certain individuals or groups of individuals. Agencies SHOULD also design their documentation requirements in line with other documentation requirements for determining eligibility for the particular service (i.e. wherever possible, agencies SHOULD choose identity-related documentation requirements that can also be used to satisfy eligibility requirements).

3.4.9.2 Training for staff – document recognition

Agencies that provide services with moderate to high identity-related risk SHOULD provide their staff with document examination training. Agencies will have to determine for themselves how in-depth this training should be and whether it should be provided by internal staff or by a specialist agency such as the New Zealand Police.

As a minimum, new frontline staff SHOULD be trained to recognise the types of documents that they will most frequently be presented with and shown what features to look for when examining them.

3.4.9.3 Protocols for acceptance of documentation

For services with moderate to high levels of identity-related risk, adherence to the following protocols will provide a higher level of confidence in a presenting individual’s identity, as these protocols make it more difficult for forged or altered documents to be accepted as genuine by agency staff:
• *Accept only original documents or copies certified by the issuing authority of the particular document* – this allows examination of all security features that are not immediately obvious and are difficult to replicate, such as watermarks and embossing. Photocopied documents are relatively easy to alter and should, therefore, not be accepted as evidence of identity

• *Preferably accept only documents that are currently valid* – a valid document is one that has an expiry date that has not yet passed. Documents that are not valid tend to be relatively old and are less likely to contain security features, making them easier to forge or tamper with. Where documents that are not valid are accepted, consideration needs to be given to requiring additional documents/records to corroborate the details contained in the older document

• *Accept only full birth certificates* – many government agencies worldwide no longer issue short birth certificates as they contain less identity-related information and are less reliable. Full birth certificates, in addition to name, date, place and country of birth, also list gender and parental details. The extra information contained on the full birth certificate can prevent duplication of agency records, where two individuals have the same name and biographical information, and gives additional avenues of investigation in cases where an individual’s claimed identity seems dubious

• *For services requiring Moderate and High EOI Confidence Level processes (see Table 8), at least one form of required identification should be a trusted form of photographic identification* (e.g. Passport or Certificate of Identity – see 3.4.7.2).

• *Unless confirmation of long-term name usage is required, only accept evidence of ‘use in the community’ documents (documents/records used to meet Objective E) that are less than one year old*

• *Require documented evidence of any name change* – (e.g. deed poll, marriage certificate, and statutory declaration)

• *Where the authenticity of a particular document is questionable, verify the authenticity of that document with the issuing authority.*

### 3.4.9.4 Overseas-issued documents

Documentation from other countries can vary widely with respect to the issue processes and security features associated with them. For example, a birth certificate from Country A might be computer printed on special paper and contain a watermark and an embossed seal, while a birth certificate from Country B might be handwritten on regular paper with a stamp. Both may be authentic documents. Such variations can be problematic for government agencies that have to determine an individual’s identity without discriminating against them because of their country of origin.

When an individual provides overseas-issued documents, the agency SHOULD ensure that up-to-date advice is available to front-line staff on how to recognise authentic documentation. The following business guidelines should be adopted for EOI Confidence Level A and B processes:
• Non-New Zealand Citizens SHOULD provide evidence of their lawful permit status (e.g. a passport containing a valid permit) – residence permits SHOULD be considered superior to work or study permits as more vetting of the applicant is undertaken before the residence permit is issued

• Only accept translations if they are carried out by the issuing authority of the particular document, an embassy of the issuing country or an authorised translation service in New Zealand – many countries have no regulations regarding the translation of documents, which means that even the presence of stamps and seals gives little assurance as to the authenticity of the translation

• Only accept English translations if they are accompanied by the original document – originals can be re-translated if doubt exists

• Refugees SHOULD be asked to supply a statutory declaration for high-risk services if they do not possess any EOI documents - refugees usually do not have EOI documents other than a New Zealand-issued Certificate of Identity

• Only accept official documents as identity-related evidence – in many countries affidavits and church-issued baptismal certificates are used in lieu of birth certificates. Provided their birth was registered, most people SHOULD be able to obtain official birth certificates from their country of origin (see 3.4.9.5 for further guidance).

3.4.9.5 Resources to assist with document recognition

The following resources are available to assist agencies with the verification of identity-related documents:

• advice about security features of identity-related documents issued by the Department of Internal Affairs (Identity Services) is available to agencies on request from: eoistandard@dia.govt.nz

• advice about the features of authentic identity-related documentation issued overseas is available to agencies on request from: eoistandard@dia.govt.nz

• agencies which deal with overseas-born applicants can visit the following official website run by the United States Department of State: travel.state.gov/visa/reciprocity/index.htm. It has a comprehensive list, by country, of the types of documents that individuals should be able to provide, what they should look like, and where applicants can obtain them from

• the Document Examination Section of the New Zealand Police provides a wide range of services, including training staff in document examination techniques. Contact the Document Examination Section, Office of the Commissioner New Zealand Police c/- Wellington Central Police Station, Corner Harris and Victoria Streets, PO Box 693, Wellington. Email: newzealand.doc.exam@xtra.co.nz.

3.4.10 Verification of identity-related data against source data

Verifying information with the primary data source (i.e. source of issue) reduces the likelihood of individuals successfully presenting counterfeit or altered documents as genuine and is the method that provides the greatest amount of confidence for Confidence Level A processes, although there is still potential for data entry error and internal misconduct. Verification of details with the issuing source provides evidence that:
• the identity details on a document or service application form provided by the applicant have not been altered between creation of the original record and presentation of the information to the service agency
• the presented document or identity details provided by the individual are not counterfeit/fictitious.

Although it is anticipated that information will be collected from the individual concerned, that information may only be verified with a third party if such verification complies with the provisions of the Privacy Act 1993. For example, agencies might verify birth information with the Registrar-General, Births, Deaths and Marriages (BDM) to avoid the need for the individual to obtain a birth certificate or where there is concern that a false birth certificate may have been provided by the individual. Agencies SHOULD consult with their privacy officer or legal advisers to ensure that any business processes of this nature comply with the Privacy Act 1993.

3.4.10.1 Authorised information matching programmes
Part 10 of the Privacy Act 1993 provides a regulatory regime that permits information matching in circumstances where it would otherwise constitute a breach of the Information Privacy Principles. Each authorised information matching programme is established by statute. For example, if an agency wishes to establish an information matching programme to match against registered birth information, this would require an amendment to the BDM Registration Act 1995. As legislation is required for authorised information matching programmes, agencies are advised to involve their legal advisers and privacy officers early in the process. In addition, early consultation with the Office of the Privacy Commissioner is strongly recommended as the Commissioner’s functions include examination of any proposed legislation where “the information might be used for the purposes of an information matching programme…” Agencies can find information about these issues on the Privacy Commissioner’s website (www.privacy.org.nz), particularly the “Information Matching” fact sheet and “Guidance Note for Departments Seeking Legislative Provision for Information Matching: Information Matching Privacy Impact Assessments”.

3.4.11 Trusted referees
Trusted referees are a vital component of the EOI process. In particular, trusted referees can assist an agency with determining whether the presenting person links to the claimed identity.

For the purpose of the EOI Standard, a trusted referee is a person who:
• confirms the accuracy of information supplied by an individual
• confirms that the information, to their knowledge, belongs to that person (this may include biographical and biometric (usually a photograph) information).
The two key elements that should exist for a trusted referee process to be effective are that the referee:

• has the personal knowledge required to verify the individual’s identity
• is trusted by the agency (according to the agency’s own criteria).

### 3.4.11.1 Criteria for trusted referees

Agencies will need to determine who qualifies as trusted referees for a particular service. Ideally a trusted referee will be known to the agency. This means they will have previously had their identity established by the agency, thereby creating a level of trust between the agency and the referee.

In addition, further criteria will need to be set around who qualifies as a trusted referee for specific services. The criteria chosen SHOULD be widely enough defined so that individuals can reasonably be expected to find referees to fulfil the criteria.

Criteria could include that a trusted referee:

• is not related to the applicant
• is not a partner or spouse of the applicant
• is not resident at the same address as the applicant
• has known the applicant for a specific amount of time (e.g. at least 12 months)
• holds a particular position of standing in the community (e.g. registered professional, kaumātua⁵, religious or community group leader)
• has an accessible contact address and phone number
• is registered with the agency as per that agency’s criteria.

NOTE – To meet the High EOI Confidence Level process, there SHOULD be a process allowing the agency to contact the trusted referee directly to confirm their details. At a minimum, trusted referees SHOULD be contacted if any discrepancy is identified as part of EOI checking processes.

### 3.4.11.2 Legislative implications for trusted referee processes

The practice of using trusted referees can be established through operational procedures and may not necessarily need to be enshrined in legislation. Current passport administration in New Zealand provides a precedent for this approach being introduced without legislation.

Agencies SHOULD liaise with their legal advisors when considering implementing a trusted referee process, to ensure that the process is legitimate in regard to the particular legislation that the agency operates within.

---

⁵ Criteria for who is recognised as a kaumātua are determined at the individual agency level.
3.4.11.3 Privacy implications for trusted referee processes

A potential privacy issue arises with agencies requiring the use of trusted referees for particular services, given that the individual will be required to disclose to a trusted referee the service that he/she wishes to access, i.e. should an individual have to let a third party know that he/she is applying for an unemployment or sickness benefit in order to meet the agency’s trusted referee requirements?

It is advisable, if customers are expected to face personal costs or risks (of any nature) from disclosing to a third party the service that they are applying for, that the agency design service application forms in a manner that does not associate the core application data with the trusted referee’s input to the application.

3.4.11.4 Strengths and limitations of trusted referees

Use of trusted referees can be a cost-effective way to provide confidence that an individual ‘links’ to the identity they have claimed as their own.

For a High EOI Confidence Level process, agencies SHOULD contact trusted referees for validation of the information that the applicant, and possibly the trusted referee, has provided, at least for a percentage of applications. In addition, a profiling approach SHOULD be considered for services for which an agency cannot justify contacting each referee for further validation or for services for which the identity of some applicants should be subjected to more rigorous verification than others. This SHOULD include contacting trusted referees where discrepancies in individual applications are detected and on the basis of other risk indicators. Any trusted referee who verified the identity of an allegedly fraudulent customer SHOULD also be investigated.

Specific risk indicators will need to be determined by the individual agency in relation to the nature of particular services. If there is an unacceptable level of doubt in the validity of either the individual’s claimed identity or that of the trusted referee, the agency SHOULD subject the case to more thorough investigation.

3.4.12 In-person verification processes

In-person verification involves the individual appearing in person at a public counter with a photograph verified by a trusted referee, or with a trusted document that contains a photograph (such as a passport). Staff members then assess whether the person in front of them matches the person in the photograph, and/or whether the person before them appears to correspond with the biographical data on the document (e.g. whether they appear to be the correct age and gender).

For an in-person verification process to be effective it should be of the highest integrity. For example, staff SHOULD be trained in person recognition. The costs involved in carrying out a high integrity in-person verification process for all customers are high. Costs include financial cost to the agency and compliance costs for customers (e.g. inconvenience and
EVIDENCE OF IDENTITY (EOI) STANDARD

accessibility issues). Therefore, when deciding whether in-person verification should be adopted by the agency, consideration SHOULD be given to whether the agency requires the individual to appear in-person for other reasons (e.g. to determine the individual’s entitlement to the particular service).

Agencies need to assess the benefits of seeing an individual in person. Factors for consideration include:

- costs and benefits (e.g. whether the compliance costs such as agency infrastructure and travel for the individual is unreasonably high in relation to the benefits gained)
- whether an alternative process will achieve the same result, such as having a trusted referee verify the individual’s identity by signing the back of their photo
- whether in-person contact can fulfil objectives additional to meeting EOI requirements (a number of services already require face-to-face contact with individuals).

3.4.12.1 Strengths and limitations of in-person verification

In-person verification provides potential ‘barriers’ for a person attempting to misuse or abuse identity. This is particularly likely to be the case where an individual is attempting to use a stolen identity.

However, there are also limitations to the effectiveness of in-person verification. Although research has found that photographic facial recognition is not 100% accurate, its success rate is high enough to add a significant degree of confidence to the EOI process, as long as it is used in combination with other forms of EOI. What is unclear, however, is whether face-to-face contact with an individual is any more successful in meeting Objective C (presenting person links to identity) than using other processes, such as using trusted referees.

3.4.13 Dealing with discrepancies

This section outlines secondary EOI processes that SHOULD be used where a discrepancy is detected in the EOI documentation provided by an individual or trusted referee. The process is similar to that required in situations where discrepancies are identified during in-person verification processes (see 3.4.12).

- Staff SHOULD first seek an explanation from the applicant for the service, unless it is clearly apparent that it is a fraudulent matter, in which case the matter SHOULD be forwarded directly to investigations staff.
- If the applicant’s explanation is not satisfactory, then the application SHOULD be investigated further. This may be referred to investigations staff.
- Discrepancies between documents/records regarding names or dates/places of birth SHOULD be resolved before continuing with a service. Agencies should not issue any documents that could be used to subsequently establish identity without resolving such discrepancies, as this may allow an individual to operate fraudulently under more than one identity.
- Agencies SHOULD refer applicants back to the issuing authority to seek amendment and/or replacement of a document if it is incorrect.
• Agencies SHOULD consult with their internal teams who deal with investigating discrepancies about what information from a document is useful to retain for investigative purposes e.g. retain a photocopy or record date of issue and serial number.

• Where documents are suspected to be fraudulent, agencies should not return the documents to an applicant until the individual’s identity has been fully established, unless it is unlawful for the agency to do so. Loss of evidence could significantly jeopardise any action an agency may wish to take against a fraudulent applicant.

3.4.14 Investigative interviewing processes

Investigative interviewing offers a higher degree of confidence than the in-person verification process outlined in section 3.4.12. An investigative interview involves the interviewer collecting identity-related information about an individual prior to the interview and preparing questions that the person claiming that particular identity should reasonably be expected to answer correctly.

Because of the cost, both for the agency and the individual, and the level of agency staff training involved, investigative interviews SHOULD only be used where other EOI processes have not achieved the required level of confidence in an individual’s identity.
3.4.15 Handling individual exceptions

In some cases, individuals will be unable to meet the requirements of EOI processes. For these cases, agencies need to have exception-handling protocols in place. What these protocols involve will be determined by the agency in relation to the particular service and customer base.

Where possible, exception processes SHOULD be as functionally equivalent as possible to a service’s standard EOI processes. If a service requires a Moderate EOI Confidence Level process, the agency SHOULD attempt to meet the objectives for the Moderate EOI Confidence Level process by requiring alternative forms of EOI from the individual. For example, where an individual is unable to provide the required documentation to meet Objective A (i.e. evidence that the claimed identity exists) due to accidental destruction of all documentation, then the agency SHOULD contact the issuing agency of those documents, with the consent of the individual, to verify the existence of the claimed identity.

3.4.16 Privacy requirements

The Privacy Act 1993 covers the collection, disclosure and use of personal information. In designing and implementing an EOI process, agencies MUST ensure that the process implemented is consistent with the Privacy Act 1993. Any consideration of the Act should be on the basis of agencies’ specific legal and privacy advice (see 3.4.22). The information that follows is not intended to substitute for that professional advice but is included to provide agencies with some preliminary guidance on the issues that may need to be considered. The Office of the Privacy Commissioner has developed a “Privacy Impact Assessment Handbook” to assist agencies in examining proposals that involve the collection, use, or disclosure of personal information (available from: www.privacy.org.nz).

3.4.16.1 Key considerations

Privacy issues are integral to the design and implementation of any EOI process. Key responsibilities that agencies SHOULD build into their EOI business processes include ensuring:

- in cases where the customer gives consent to the access of data, that this is supported by adequate proof of that consent through a physical or digital signature (where allowed under the Electronic Transactions Act 2002)

- that individuals have access to and can correct any personal information held about them by the agency

- that information collected for the purpose of verifying an individual’s identity is not used for any other purpose. However, in practice, personal information may be collected for several purposes at the same time. For example, an agency may collect evidence of an individual’s name, address, and date and place of birth in order to verify the individual’s identity, determine their eligibility for the service applied for, and ensure they can contact the individual in future. Agencies using the information for more than one purpose MUST ensure that each purpose for which the information is being collected is clearly explained to the individual (e.g. purposes could be outlined on the application form for the relevant service)
that information is not disclosed to another person or agency – with limited exceptions. If the EOI process includes the use of trusted referees as a way to verify identity, agencies MUST ensure that personal information is not unnecessarily disclosed to the trusted referee if the latter is contacted to verify identity information provided by the individual.

that information systems (electronic or human-based) are secure from inappropriate access by others. For example, agencies need to ensure identity information held on a database is not vulnerable to unauthorised access, or that frontline staff do not disclose identity-related information without sufficient checks to confirm the identity of the person requesting it. Agencies SHOULD periodically review the degree to which their systems and processes achieve the level of security that they have been designed to achieve. Adjustments to systems and processes SHOULD be made where required.

that the appropriate level of an applicant’s consent is obtained consistent with the need to acquire the data relevant for determining the applicant’s identity.

Some of the information collected from individuals during the EOI process will be necessary for agency records (e.g. name and address) and other information may be provided to confirm a person’s identity but does not need to be retained by the agency after the EOI process has been completed. Agencies are responsible for ensuring that they do not keep information that is irrelevant or for which there is no legitimate reason for retention. Agencies need to consider whether there is a legitimate business reason for retaining identity-related information collected from individuals or whether it is sufficient to simply record that the information was sighted.

For information on privacy considerations refer to privacy officers or legal advisers in the first instance. Agencies may also wish to consult the Privacy Commissioner’s website (www.privacy.org.nz).

The Privacy Act 1993 is available from www.legislation.govt.nz

3.4.16.2 Collection of identity-related information from individuals

At the heart of the Privacy Act 1993 are the notions of transparency and autonomy. People cannot exert any control over the accuracy of their data or use of it until they know when data is being collected, who will have access to it and how it will be used. Transparency is central to building customer trust.

The Privacy Act requires agencies to advise individuals about the following:

- why identity-related evidence is being collected
- whether the information is required by law and, if so, which law
- whether the supply is voluntary
- the consequences if the required information is not supplied (e.g. that service provision may be withheld from the individual).
The rationale for meeting objectives within an EOI process, and the documents/records that meet particular EOI objectives, could usefully be provided to the public to aid transparency of the process. For example, utility bills provide confirmation that the person uses that identity in their daily life, and may be used to confirm the person’s current address. Agencies that request these documents SHOULD advise their customers that this is why these documents have been requested.

3.4.17 Risk profiling

Where appropriate, agencies may use risk profiling as a tool to reduce identity-related risk in addition to the EOI process requirements specified in this Standard. Any risk profiling tool considered for adoption by the agency SHOULD be considered from a human rights perspective. The agency SHOULD seek legal advice in the first instance, particularly in regard to any human rights issues that may arise from use of a particular profiling tool.

Risk profiling involves using information collected by an agency about previous cases where misuses or abuses of identity (or other types of crime) were detected and from other sources (such as other government agencies, overseas counterparts and other intelligence sources), to highlight characteristics that are more likely to involve false identities.

Agencies that use risk profiling may need to develop risk profiles as part of the process for establishing an individual’s identity. A risk profile highlights aspects about an individual that may indicate an increased risk of their perpetrating an identity crime. Where an individual application or the particular service fits within a risk profile, an agency may undertake additional processes to further verify the individual’s identity. For example, additional processes could include contacting trusted referees directly to validate information supplied by that referee, requiring the customer to attend an investigative interview, etc. The type of additional processes an agency chooses to undertake will need to be established as part of the overall EOI process design.

Risk profiles SHOULD be updated to ensure their ongoing currency. Relevant incident and/or intelligence information will provide valuable input to the refinement of agency risk profiles. As such, accountability mechanisms within agencies will be required to ensure updating happens in a timely manner.
3.4.18 **Data quality issues**

Accuracy of identity data is of key importance for any EOI process that an agency operates. EOI processes, once implemented, SHOULD be periodically audited for accuracy of identity information produced. Where unacceptable inaccuracies are found, the cause of the inaccuracies SHOULD be identified and resolved wherever possible.

As a general rule, the greater the risk associated with inaccuracies in the identity data, the greater the effort that should be expended to improve and maintain the accuracy of the identity data held. This will also help to ensure that agency practices comply with Information Privacy Principle 8 of the Privacy Act 1993.

3.4.19 **Agents/persons acting on behalf of individuals**

EOI processes SHOULD be designed on the basis that personal information will be collected from the individual concerned when that individual applies for a government service. Agencies that receive service applications from agents or caregivers who are acting on behalf of an individual need to have processes in place to ensure that the agency/caregiver has authority to act for the recipient and that any personal information is provided with the individual’s consent or some lawful authority (e.g. power of attorney or order issued by the Family Court under the Protection of Personal and Property Rights Act 1988).

Where an agent is a named individual, agencies SHOULD consider whether they SHOULD verify that the agent is the named agent of the customer. This is recommended for services with moderate to high levels of identity-related risk.

3.4.20 **Step 3 – Ongoing operation of EOI processes**

Sections 3.4.21 to 3.4.25 provide guidance on areas that agencies MUST consider prior to EOI processes becoming operational.

3.4.21 **Internal controls**

Internal controls are an agency’s first line of defence in safeguarding assets and preventing and detecting errors and fraud. Poor internal controls can jeopardise the effectiveness of any EOI process.

Agencies SHOULD analyse their EOI process to determine the points at which internal controls need to be implemented to prevent process failure. EOI internal control activities are any policies, procedures, techniques, and mechanisms that minimise the risk that EOI processes will not meet their objectives. They include a diverse range of activities, such as:

- controls over information processing
- physical control over vulnerable assets
- segregation of duties
- access restrictions to, and accountability for, resources and records.
There are a range and variety of EOI control activities that SHOULD be adopted by agencies carrying out EOI processes. An agency’s internal controls SHOULD be flexible enough to allow control activities to be tailored to fit particular contexts. The specific control activities used by one agency may be different from those used by other agencies, due to a number of factors. These factors could include specific threats faced by the agency and risks incurred, differences in agency objectives, size and complexity of the agency, operational environment, sensitivity and value of data, and requirements for system reliability, availability, and performance.

3.4.21.1 Operational considerations
An agency’s human resource planning SHOULD allow for adequate EOI checking to be undertaken by staff. Agencies need to ensure that the workload given to staff is manageable. If staff members are unduly pressured for time or to meet targets there is a risk that their vigilance in identifying discrepancy cases may diminish. Complaints and errors SHOULD be analysed to determine their cause so that remedies can be applied appropriately and in a timely manner (see 3.4.24).

Agencies SHOULD also ensure that they have adequate controls in place to prevent staff members perpetrating internal fraud, which can undermine the integrity of an agency’s EOI processes.

3.4.21.2 Staff training
Staff training SHOULD be comprehensive to ensure staff have an adequate understanding of a service’s EOI requirements and of the potential consequences should they fail to follow proper procedures. Specific areas where training is likely to be required include (but is not limited to):

• document recognition and using resources to assist with document recognition (see 3.4.9.2 and 3.4.9.5)
• in-person verification processes (see 3.4.12)
• the Privacy Act 1993 (see 3.4.16)
• dealing with cases where individuals cannot meet EOI requirements (see 3.4.15 and 3.4.19).

3.4.21.3 Physical control over vulnerable assets
An agency SHOULD establish physical control to secure, limit access to, and safeguard vulnerable assets such as documents or records that might be vulnerable to risk of loss or unauthorised use. Physical files and records SHOULD be tracked in such a way that an audit trail clearly indicates where and with whom the files are located. Audit trails in computer systems SHOULD show records of all users, access information, the time and date of access, and before and after images of any changes.
3.4.21.4 Segregation of duties

Key duties and responsibilities SHOULD be divided or segregated among different people to reduce the risks of error and internal fraud. This SHOULD include separating the responsibilities for authorising services, processing and recording them, reviewing the services, and handling any related assets. No one individual should control all key aspects of a service’s delivery. This is especially important when issuing any record that may potentially be used as evidence of identity for subsequent services.

3.4.21.5 Accurate and timely recording of services

Service delivery SHOULD be promptly recorded and processed to maintain its relevance and value to the control of operations and for later evaluations. This applies to the entire process or life cycle of a service from the initiation and authorisation through to its final classification in summary records.

3.4.21.6 Access restrictions to and accountability for identity-related records

Access to resources and records SHOULD be limited to authorised individuals, and accountability for their custody and use SHOULD be assigned and maintained. Periodic reviews and monitoring of data are necessary to help reduce the risk of errors, fraud, misuse, or unauthorised alteration.

3.4.21.7 Appropriate documentation of service delivery and internal controls

Internal controls and all services need to be clearly documented and the documentation SHOULD be readily available for examination. All documentation and records SHOULD be properly managed and maintained. Internal control monitoring SHOULD assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

3.4.21.8 Records management

Records of EOI processes SHOULD be captured into a corporate records system, maintained for as long they are required, then disposed of legally and in accordance with the Public Records Act 2005.

3.4.22 Legal considerations

In identifying and implementing any changes to business processes to meet the requirements of this Standard, agencies SHOULD identify any legal issues that might need to be addressed and ensure that they are dealt with appropriately. Examples of such issues include:

- the need to make amendments to any Act or Regulation concerning the information to be collected from the applicant or the processes that applicants undergo in order to receive a particular service from the agency
- the need to obtain and act on legal advice associated with any changes in business processes, such as the introduction of more stringent identity verification checks that require the collection and sharing of greater amounts of personal information, and the implications of the Privacy Act 1993 on the range of strategies that the agency might consider to enable the carrying out of these verification checks.
3.4.23 Transition of business processes

The extent to which agencies will need to alter their current EOI processes to comply with this Standard will vary widely between agencies and, in some cases, between different business groups within agencies.

Agencies SHOULD identify the optimum transition strategy, given the particular type and extent of changes that need to be implemented by their organisation. Key considerations in planning the transition will include whether:

- any changes to existing Acts or Regulations are required to implement the changes to EOI processes required
- the changes to business processes require action by other agencies in order to give effect to these new business processes (for example, the introduction of automated information matching by another agency). If so, the transition plan needs to address these dependencies
- the changes will impact on the functions of another agency or service. If so, the changes SHOULD be discussed with the relevant agency or service unit before they are made
- there are any other issues that could constrain or prevent the agency from implementing the required changes. If so, these issues need to be investigated and addressed before the agency finalises its transition plan so that implementation of the changes can occur effectively.

3.4.24 Complaints handling

It is possible that changes to EOI processes to ensure compliance with the EOI Standard will result in changes to the number and/or type of complaints from individuals transacting with the agency. For example, individuals may consider the EOI requirements to be overly intrusive, unnecessary and so on. Each agency SHOULD make appropriate resource provision for this possibility when designing and testing these new EOI processes.

Although most agencies are likely to already have appropriate mechanisms in place for handling complaints from customers, the need for expertise to process/investigate some types of complaints, such as complaints concerning potential breaches of the Privacy Act 1993, may be greater with the introduction of EOI processes.

Agencies SHOULD also have procedures in place for dealing with complaints where they have incorrectly recorded identity-related information about an individual. Under the Privacy Act 1993 agencies SHOULD correct any personal information they hold about the individual. Alternatively, the agency can include a statement of changes sought by the individual and the reasons why it was not deemed appropriate to make the changes.

If an agency fails to put in place appropriate administrative procedures for dealing with errors in identity details, or does not deal with any such complaints according to its procedures, this may result in an investigation by an Ombudsman, pursuant to the Ombudsmen Act 1975.
3.4.25 Communication protocols between agencies

Agencies SHOULD ensure that they monitor and evaluate the performance of their EOI processes and act in a timely manner on any issues that may need to be communicated to other agencies. Agencies SHOULD ensure, however, that any communications between agencies are in compliance with the Privacy Act 1993.

Examples of such situations include:

- the discovery of an EOI document issued by another agency that is found to be:
  - fraudulently obtained
  - falsified in some way
  - fraudulently used

- the discovery of evidence (such as credible information) indicating that one or more EOI documents issued by another agency has been, or is likely to be, fraudulently obtained, falsified in some way, or fraudulently used

- the discovery of personal information regarding the activity of any person who is found to have committed or who is suspected of any illegal activity in relation to identity or the use of identity-related documentation.
### 3.4.26 Checklist for Phase 2 Design and Operation

Checklist for ................................................................................................... (service name)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EOI Confidence Level determined (based on Service Risk Category)</td>
</tr>
</tbody>
</table>
| 2 | Design an EOI process, or modify existing EOI process, appropriate to EOI Confidence Level:  
• ‘Gap’ analysis completed (where there are existing EOI processes)  
• Minimum evidential requirements for EOI Confidence Level met  
• Transition of business processes planned |
| 3 | Implementation of EOI process (either new or modified process)  
• Internal controls implemented  
• Legal aspects (including privacy) signed-off  
• Complaints handling implemented  
• Communication protocols with other agencies implemented |
| 4 | Monitor, evaluate, and review on............................................................ |
3.5 Service delivery phase

The service delivery phase is not in scope of this Standard, with the exception of any EOI process that is required before the service can be delivered to an individual. Information on EOI processes is covered in 3.4.

3.6 Monitoring and evaluation phase

This section provides guidance on the monitoring and evaluation processes when establishing the identity of individuals\(^6\). It should assist agencies to develop a formal EOI process Monitoring and Evaluation Plan.

The purpose of the Monitoring and Evaluation Phase is to ensure that, once implemented, each agency’s EOI business processes and associated outcomes remain consistent with their objectives.

3.6.1 Continual improvement of EOI processes

Agencies need to modify their EOI processes where monitoring and evaluation results indicate that EOI process objectives are not being satisfactorily met and are consequently exposing the agency to unacceptable identity-related risk. This is an iterative process, as shown by the ongoing cycle of monitoring, evaluation and process improvement in Figure 7.

In carrying out EOI process evaluation, agencies need to systematically consider what their objectives are in relation to their EOI processes, and what might adversely influence the achievement of those objectives (i.e. the EOI process risks). Just as the context and nature of the risks dictate the types of risk analysis and risk evaluation carried out, context also dictates the design and implementation of appropriate monitoring and evaluation procedures.

Events such as the use of forged EOI documents allow an agency to improve its understanding of the likelihood and consequences of the risks, and influence the ongoing maintenance of appropriate business processes to address them. In essence, monitoring processes provide this information and evaluation processes analyse it in order to identify any required improvements. For example, risk profiles (see 3.4.17) may be modified on the basis of information collected as part of monitoring processes in place of an EOI process.

\(^6\) Services that require evidence of identity will have been determined during the risk assessment phase (see 3.3).
Figure 7 – Monitoring and evaluation cycle

Phase 4
Monitoring and evaluation

Step 1 – Monitoring and Evaluation Plan
Identify performance indicators to monitor

Step 2 – Ongoing monitoring and evaluation
Ongoing monitoring of EOI processes
Periodic evaluation of effectiveness of EOI processes

Step 3 – Amend EOI processes
Design more appropriate EOI processes as necessary
Test and implement new EOI processes

Phase 2 – Operation and design
Operational EOI processes

Phase 3 – Service delivery
Agency undertakes EOI process

Phase 1 – Risk assessment
Ongoing risk processes

Phase 1 – Risk assessment
Test and implement new EOI processes

Figure 7 – Monitoring and evaluation cycle

Phase 4
Monitoring and evaluation

Step 1 – Monitoring and Evaluation Plan
Identify performance indicators to monitor

Step 2 – Ongoing monitoring and evaluation
Ongoing monitoring of EOI processes
Periodic evaluation of effectiveness of EOI processes

Step 3 – Amend EOI processes
Design more appropriate EOI processes as necessary
Test and implement new EOI processes

Phase 2 – Operation and design
Operational EOI processes

Phase 3 – Service delivery
Agency undertakes EOI process

Phase 1 – Risk assessment
Ongoing risk processes
3.6.2 Monitoring and evaluation approaches

Identity-related risks vary between services. Monitoring and evaluation processes should, therefore, be tailored to the individual contexts of each agency.

This Standard does not prescribe maximum or minimum intervals between monitoring and evaluation cycles. These decisions are the responsibility of each individual agency. However, agencies SHOULD ensure they document the basis for their approach to monitoring and evaluation and SHOULD maintain up-to-date documentation for auditing and quality assurance purposes. It is recommended that agencies review their EOI process monitoring and evaluation practices at least every two years.

3.6.3 Step 1 – Develop Monitoring and Evaluation Plan

A Monitoring and Evaluation Plan SHOULD be completed prior to an EOI process becoming operational. This Plan SHOULD be completed as part of the Design and Operation Phase. If this is not practical, information about monitoring and evaluation processes SHOULD be incorporated into the business and risk management documentation that relates to the particular service.

3.6.3.1 Monitoring processes and performance indicators

Selecting appropriate indicators to measure the effectiveness of EOI processes is extremely important. Performance indicators need to inform assessments about the degree to which the EOI processes meet the agency’s EOI-related objectives.

An agency will need to factor in the following considerations when choosing its performance indicators:

- cost to the agency
- ability to collect the required data/information
- reliability of the performance indicators.

Table 13 provides a list of types of performance indicators that could be used for monitoring EOI processes. It is not an exhaustive list. Agencies SHOULD select performance indicators most relevant to their specific risks and desired outcomes, ensuring that they only monitor performance against a manageable number of indicators.
### Table 13 – Performance indicators

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Example of measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergence of any new EOI process risks</td>
<td>For example, analysis of discovered fraudulent activities to determine whether new modes of operation are being used to misuse and abuse identity relation to agency services.</td>
</tr>
<tr>
<td>Quality of administrative activities</td>
<td>For example, measurement of the proportion of processing errors found within EOI processes. An example error could be that individuals’ identities were established without the required EOI documentation being confirmed by a staff member.</td>
</tr>
<tr>
<td>Compliance with the Privacy Act</td>
<td>For example, the proportion of EOI processes for identifying individuals that are found (from an audit or similar) to have been in breach of the Privacy Act due to the actions of staff involved with the service.</td>
</tr>
<tr>
<td>Staff training and performance</td>
<td>For example, measurement of the results of tests of staff ability to correctly identify authentic and non-authentic documents of the type used for the EOI processes they administer.</td>
</tr>
<tr>
<td>Cost and effort associated with EOI processes</td>
<td>For example, measurement of the cost, time or other measure invested in the design and operation of EOI processes compared with the outcomes of those processes in relation to identity abuse rates or customer satisfaction.</td>
</tr>
<tr>
<td>Feedback from other agencies</td>
<td>For example, analysis of the number of instances where other agencies have reported the use of identity-related documents issued by the agency that contain errors or which are stolen or counterfeit.</td>
</tr>
<tr>
<td>Alignment between EOI processes and objectives</td>
<td>For example, measurement of any increase in the number of false identities detected per annum through implementation of an EOI process designed to better detect false identities.</td>
</tr>
</tbody>
</table>

The examples of performance indicators contained in Table 13 highlight the importance of identifying specific cause and effect relationships between the achievement of business objectives and the indicators being measured. Where strong cause and effect relationships exist, changes in the results of data collection will indicate corresponding changes in the achievement of business objectives. Each agency’s choice of performance indicators SHOULD enable the agency to remain informed about the degree to which its business objectives are being met.

### 3.6.3.2 Collection of data/information

Various methods can be used to collect monitoring data/information. These range from simply gathering feedback or descriptions of success or failure, to systematically gathering qualitative and/or quantitative data for statistical analysis. Collection methods include:

- routine checks of EOI process steps
- audit of EOI processes
- maintenance of a risk register for EOI processes
- maintenance of a database recording details of EOI process errors or failures
• costing information about EOI processes
• collection of customer complaints regarding EOI processes, and any other customer feedback
• surveys of customer satisfaction.

3.6.3.3 Appropriateness of monitoring
The types and amount of monitoring chosen SHOULD provide agencies with information in a timeframe and format that allows decisions about the suitability of the EOI processes to be assessed.

In the event of any unacceptable departure from, or mismatch between, these EOI processes and objectives, the monitoring processes SHOULD allow process changes to be designed and implemented before significant problems arise.

3.6.4 Evaluation processes
The following aspects of evaluation MUST be taken into account during plan development.

3.6.4.1 Designing evaluation processes
As a general rule, an agency’s EOI processes SHOULD be changed when the criteria for success of those processes are not met and the expense and/or effort required to improve the outcomes is justified. Evaluation processes allow assessment of adequacy and identification of appropriate improvements.

In carrying out evaluation processes, agencies MUST document the:
• rationale for all EOI business processes
• key EOI process objectives to be achieved and the context within which the evaluation is conducted
• performance indicators used (see 3.6.3) as a basis for the evaluation
• results (against those performance indicators) that the agency considers represent contribution to outcomes – successful or otherwise.

Evaluation processes SHOULD be designed to properly inform decisions about the appropriateness of the EOI processes so that those processes can be amended as appropriate. Evaluation processes SHOULD be tailored to the specific situation in which they are being carried out. These processes SHOULD be designed in conjunction with the monitoring processes for agency EOI processes.

The design of evaluation processes is particularly important if specific interventions are to be assessed. For example, if a new business process is introduced in order to reduce the number of processing errors, the effect of the new process on the number of errors will need to be measured to gauge the success of the new process. Information will also need to be retained about the previous process so improvements can be measured. Where such changes to process are expected to affect another agency, the changes SHOULD be agreed on by all affected agencies prior to implementation.
It is important that agencies identify and document the factors that will be taken into account during the evaluation of EOI processes. This assists any external review of the appropriateness of the EOI processes and helps the agency to implement and maintain appropriate EOI processes.

### 3.6.4.2 Issues for evaluation

Table 14 provides examples of the types of issues that an agency may evaluate in relation to its EOI processes. This is not a complete list and the issues chosen for evaluation will need to take into account the agency context and objectives within which particular services operate.

#### Table 14 – Issues for evaluation

<table>
<thead>
<tr>
<th>Issue</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solutions to address identity-related risks</td>
<td>For example, evaluation of whether new EOI checks on applications for welfare benefits resulted in an increase in the discovery rate of identity-related benefit fraud.</td>
</tr>
<tr>
<td>Implications of ongoing initiatives, such as communication with agencies about downstream effects to existing operational procedures</td>
<td>For example, the discussion with other agencies of possible measures to counter EOI process concerns that have been raised. The introduction of any new EOI checks SHOULD be weighed up in light of the expected benefits that they would bring to the affected agencies and the expected costs and operational changes that would need to be incurred with the new EOI checks (i.e. cost/benefit analysis). Performance indicators relating to those EOI checks, such as the number of discovered false identity events per year, would need to be identified and the resulting information periodically evaluated.</td>
</tr>
<tr>
<td>Possible solutions to EOI process problems identified, such as breaches of the Privacy Act</td>
<td>For example, evaluation of the effectiveness of staff training courses aimed at improving staff’s compliance with the Privacy Act, as evidenced by a reduction in the number of breaches of the Act by staff.</td>
</tr>
<tr>
<td>Adequacy of staff training and performance</td>
<td>For example, the performance of staff measured by regular assessments of the quality of their EOI process-related activities (such as quality of document verification checks and customer liaison activities).</td>
</tr>
<tr>
<td>Possible improvements to EOI processes, such as efficiency gains</td>
<td>For example, an agency might identify patterns of EOI-related concerns (such as attempts to use non-authentic EOI documentation). The agency may then channel future EOI processing to selected staff members who have been trained more comprehensively. In doing so, the agency might aim to reduce its processing costs while maintaining or even improving its level of success in meeting its business objectives. Monitoring those business outcomes provides the agency with the information required to evaluate whether such initiatives are achieving their desired outcome.</td>
</tr>
</tbody>
</table>
Where evaluation results in information that may be of use to other agencies or to the Custodian of the standard, and which can appropriately be shared, agencies are encouraged to share the results of their evaluations (e.g. where an agency’s evaluation activities identify changes in the nature of methods of misusing or abusing identity being perpetrated by individuals).

### 3.6.5 Step 2 – Ongoing monitoring and evaluation

Once an EOI process becomes operational, the monitoring and evaluation processes SHOULD commence.

#### 3.6.5.1 Frequency of monitoring and evaluation activities

Monitoring and evaluation will be undertaken at different frequencies depending on the particular context within which a service exists. Monitoring and evaluation can be undertaken:

- **Continuously** – in some situations, such as in rapidly changing environments, it may be appropriate to monitor the adequacy of EOI processes, more or less continuously (e.g. in cases where a particular service results in the issue of identity documentation that can be used subsequently)

- **Periodically** (on a discrete-interval basis) – this approach is likely to be appropriate for the evaluation of most services

- **Episodically** (event dependent) – this is likely to be the most appropriate approach after the completion of major changes to business processes.

In all situations the underlying rationale for the choice of frequency is the need to keep pace with the rate of change in the data or information that is being measured, so that any unacceptable deviations from desired performance of the EOI processes are avoided wherever possible, or resolved where this has not been possible.

The frequency of monitoring and evaluation needs to be influenced by both the rate at which the identity-related risks can change and the extent to which any changes are important. In many cases, a change in one of these factors also affects the other.

The intervals between evaluation cycles can be increased when the circumstances being evaluated have not materially changed from the circumstances that were evaluated last. Accordingly, each agency SHOULD revise its evaluation processes in light of experience gained from previous monitoring and evaluation cycles.

**NOTE** – Episodic evaluation can be either in addition to or instead of periodic evaluation, depending on the extent to which outcomes may deviate from business objectives.
3.6.5.2 *Changing monitoring processes*

The type of monitoring SHOULD be changed if the current monitoring does not allow a timely and adequate assessment of the appropriateness and effectiveness of the EOI processes relative to the EOI objectives being assessed.

More monitoring SHOULD be undertaken when additional monitoring of the same type is expected to yield additional information that justifies the additional effort. Justification relates to how valuable the additional monitoring is expected to be relative to the expense or effort of conducting it.

Changes to monitoring regimes often involve changes to both the types of monitoring and the overall amount of monitoring that is undertaken, particularly until the agency establishes a good understanding of its exposure to identity-related risk and the extent to which its EOI processes address it. Once these positions have been established, agencies will be able to more efficiently adjust their monitoring and evaluation activities to maintain the identity-related risks associated with their services at an acceptable level.

3.6.6 *Step 3 – Amend EOI processes*

Where evaluation processes indicate that EOI processes are not sufficiently reducing identity-related risk or meeting objectives, consideration MUST be given to amending EOI processes.

Any amendments to an agency’s EOI process MUST be subject to the same consideration as the initial design (see 3.4.7). In addition, any amended process SHOULD be fully tested before becoming part of the ongoing operation.
Working group representation

The following agencies/organisations were represented on the EOI Standard Working Group:
Department of Internal Affairs
Ministry of Justice
Department of Labour
Inland Revenue
Land Transport New Zealand
Ministry of Education
Ministry of Health
Ministry of Social Development
New Zealand Police
Office of the Privacy Commissioner (Observer status)
State Services Commission

Acknowledgement

The Department of Internal Affairs and the State Services Commission gratefully acknowledge the contribution of time and expertise from all those involved in developing this Standard.

Copyright

This document is subject to Crown copyright. This material may be used, copied and redistributed free of charge in any format or media, provided that the source and copyright status is acknowledged (i.e. this material was produced by the Department of Internal Affairs © Crown copyright 2006).

Referenced documents

Joint Australian/New Zealand Standards

www.standards.co.nz

www.standards.co.nz

www.standards.co.nz

New Zealand Legislation

Adult Adoption Information Act 1985
Arms Act 1983
Births, Deaths and Marriages Registration Act 1995
Citizenship Act 1977
Civil Union Act 2004
Electoral Act 1993
Electronic Transactions Act 2002
Human Rights Act 1993
Immigration Act 1987
Land Transport Act 1998
Land Transport (Driver Licensing) Rule 1999
Ombudsmen Act 1975
Passports Act 1992
Protection of Personal and Property Rights Act 1988
Privacy Act 1993
Public Records Act 2005
Sale of Liquor Act 1989
Social Security Act 1964
Tax Administration Act 1994

Other
Bradner, S. March 1997. *Key words for use in RFCs to indicate requirement levels (RFC 2119).* www.ietf.org


www.privacy.org.nz

www.privacy.org.nz

www.e.govt.nz

www.e.govt.nz


Version 1.0. www.e.govt.nz


**Related websites**

www.dia.govt.nz
www.legislation.govt.nz
www.privacy.org.nz
www.ssc.govt.nz
www.travel.state.gov/visa/reciprocity/index.htm

**Latest revisions**

This Guide is to be reviewed from time to time by the working group so that it keeps up to date with changes in technology and business requirements in the sector.

Users should ensure they access the latest revisions of the NZ e-GIF authentication standards including amendments (if any). These can be found at www.e.govt.nz. Users should also access the latest revisions of the documents included in the list of referenced documents already set out in this Guide.

**Review of standards**

Suggestions for improvement of this Standard are welcomed. They should be sent to the Department of Internal Affairs (the EOI Standard Custodian) at:

Email: eoistandard@dia.govt.nz
Appendices – Introduction

Appendices A, B and C provide information on:

- ‘primary’ documents that can be used as part of a process for establishing an individual’s identity
- ‘supporting’ documents that can be used to assist in establishing an individual’s identity, where an individual is unable to provide ‘primary’ documents
- change of name, adoption and gender reassignment.

NOTE –

(1) Only information of relevance to the use of these documents within an EOI process is included. Other aspects of the issue process behind each of the documents/records have been omitted.

(2) Appendix A outlines the processes and requirements behind current documents and data sources, i.e. relevant at the time of publication of this Standard. There may be previous or future versions of documents where processes and requirements differ from this information.
Appendix A – EOI ‘Primary’ documents/records referenced in this Standard

Table A1 provides an overview of documents and the EOI objectives they can be used to satisfy. Documents/records that are used to meet Objective C (presenting person links to identity) MUST be used in conjunction with either in-person or trusted referee verification that the photo in the document is that of the claimant of the identity. Included in Table A1 is a column for documents that can be used to provide evidence of a name change.

Table A 1 – Documents used for Evidence of Identity Processes

<table>
<thead>
<tr>
<th>Document</th>
<th>Issuing Agency</th>
<th>Objective</th>
<th>Name Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand Passport</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Emergency Travel Document</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Refugee Travel Document</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Certificate of Identity (issued under the Passports Act 1992)</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Certificate of Identity (issued under the Immigration Act 1987)</td>
<td>Department of Labour (Immigration)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Firearms or Dealer’s Licences</td>
<td>New Zealand Police</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Birth Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>New Zealand Citizenship Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>New Zealand Death Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>New Zealand Driver Licence</td>
<td>Land Transport New Zealand</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>18+ Card</td>
<td>Hospitality Association of New Zealand</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Community Services Card</td>
<td>Ministry of Social Development</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

7 A That the identity exists  B Identity is living  C The presenting person links to the identity  D Presenter is sole claimant of the identity  E Use of the identity in the community

8 The witness must not be a relative or part of the family group of the applicant; be a partner of the applicant; or live at the same address as the applicant. The witness must have a known the applicant for at least 12 months (or since birth for children less than 12 months); be 16 years or over; and be a holder of a valid New Zealand passport or from one of these groups: lawyer, teacher, minister of religion, police officer, kaumatua, registered medical professional, justice of the peace, applicant’s employer.
<table>
<thead>
<tr>
<th>Document</th>
<th>Issuing Agency</th>
<th>Objective(^7)</th>
<th>Name Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electoral roll record</td>
<td>Enrolment Centre of New Zealand Post</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>IR Number</td>
<td>Inland Revenue</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>New Zealand Marriage Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>New Zealand Civil Union Certificate</td>
<td>Department of Internal Affairs (Identity Services)</td>
<td></td>
<td>√</td>
</tr>
</tbody>
</table>

For each document/record listed in Table A1, details are provided in Appendix A on the following:

<table>
<thead>
<tr>
<th>Issuing agency</th>
<th>Agency responsible for issuing the document.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>The purpose of the document.</td>
</tr>
<tr>
<td>Information</td>
<td>Details on identity information contained in the document and other non-identity information such as document number and dates of issue and expiry.</td>
</tr>
<tr>
<td>Document features</td>
<td>Details about features of the documents, such as security features.</td>
</tr>
<tr>
<td>Validity</td>
<td>Period that the document is issued for.</td>
</tr>
<tr>
<td>Issuance process</td>
<td>Details about the processes, specifically for evidence of identity, involved in the issue of the document.</td>
</tr>
<tr>
<td>Legislation</td>
<td>Enabling legislation, if any, for issue of the document.</td>
</tr>
<tr>
<td>Standard fit</td>
<td>Descriptions of EOI objectives that the document can be used for.</td>
</tr>
<tr>
<td>Further information</td>
<td>Link to further information available on the Internet.</td>
</tr>
</tbody>
</table>
# New Zealand Passport

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>An official government document certifying identity and citizenship and granting permission to travel abroad.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained in a passport includes:  
• first/given name(s) and surname/family name(s)  
• date of birth  
• place of birth  
• gender  
• photo of individual  
• nationality.  
Other information in a passport includes:  
• passport type  
• issuing state  
• issuing authority  
• passport number  
• dates of issue and expiry. |
| **Document features** | The form of the New Zealand passport is governed by an international convention to which New Zealand is a signatory. Currently it is a booklet with a data page, a number of visa pages and a number of security features.  
Further information about security features contained in the New Zealand passport is available by contacting the Department of Internal Affairs. |
| **Validity**       | Passports issued from 21 April 2005 have a maximum validity of five years. Passports issued before this date have a maximum validity of ten years. |
| **Issuance process** | To legally obtain a New Zealand passport, an applicant must be a New Zealand citizen.  
First-time applicants must fill out a passport application form and provide evidence of event details, which have occurred in New Zealand such as birth, citizenship, and change of name. Electronic verification against birth and death records occurs as part of the issue process to verify that information provided is genuine.  
Applicants for a passport renewal must provide their current or expired New Zealand passport and, if applicable, documentation that confirms their change of name (e.g. a Marriage or Civil Union Certificate).  
A witness who meets specified criteria\(^9\) must fill out a ‘proof of identity’ section verifying the applicant’s identity. The witness must also provide contact details and certify that the photo provided represents a true likeness of the applicant and is less than 12 months old. |

---

\(^9\) The witness must not be a relative or part of the family group of the applicant; be a partner of the applicant; or live at the same address as the applicant. The witness must have a known the applicant for at least 12 months (or since birth for children less than 12 months); be 16 years or over; and be a holder of a valid New Zealand passport or from one of these groups: lawyer, teacher, minister of religion, police officer, kaumatua, registered medical professional, justice of the peace, applicant’s employer.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard fit</strong></td>
<td>A passport can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity). A passport provides confirmation of an individual’s name and date and place of birth, and what they look like. It also provides confirmation that the individual is a New Zealand citizen. The photo inside the passport enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the passport.</td>
</tr>
<tr>
<td><strong>Further information</strong></td>
<td><a href="http://www.govt.nz">www.govt.nz</a></td>
</tr>
</tbody>
</table>

10 As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
New Zealand Emergency Travel Document

<table>
<thead>
<tr>
<th>Issuing Agency</th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>The New Zealand Emergency Travel Document (ETD) is a short-term, machine-readable travel document issued to New Zealand citizens who have previously been issued a New Zealand passport, which is lost, stolen or damaged while overseas, and who need to travel urgently.</td>
</tr>
</tbody>
</table>
| **Information**| Information about a person contained in a ETD includes:  
  • first/given name(s) and surname/family name(s)  
  • date of birth  
  • place of birth  
  • gender  
  • photo of individual  
  • nationality.  
  Other information in an ETD includes:  
  • ETD type  
  • issuing state  
  • issuing authority  
  • passport number  
  • dates of issue and expiry. |
| **Document features** | The form of the ETD is governed by an international convention to which New Zealand is a signatory. Currently it is a booklet with a data page, a number of visa pages and a number of security features.  
  ETDs have been issued from 26 October 2004. The document has been introduced to improve the overall security of New Zealand travel documentation by ensuring New Zealanders overseas have access to a secure and internationally accepted short term emergency travel document. As manual passports will no longer be issued, the introduction of the ETD will reduce the number of manual passports (which are less secure) in circulation.  
  Further information about the security features contained in the ETD is available by contacting the Department of Internal Affairs. |
| **Validity** | An ETD is valid for up to 12 months. |

11 The term manual passport refers to non machine-readable passports.
### Issuance process

To obtain an ETD an applicant must be a New Zealand citizen who has previously been issued a New Zealand passport.

The process for issue of an ETD is comparable to that for the renewal of a New Zealand passport. This includes proof of identity from a witness, cross-checking against the passport record, and death record checking.

As with the passport process, a witness who meets the criteria\(^\text{12}\) must fill out a ‘proof of identity’ section certifying the applicant’s identity. They must also provide contact details and certify that the photo represents a true likeness of the applicant and is less than 12 months old.

To receive a New Zealand passport, after the issuance of an ETD, an individual must subsequently submit a newly completed passport application.

### Legislation


### Standard fit

An ETD can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity).

An ETD provides confirmation of an individual’s name and date and place of birth, and what they look like. It also provides confirmation that the individual is a New Zealand citizen.

The photo inside the ETD enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the ETD\(^\text{13}\).

### Further information

[www.dia.govt.nz](http://www.dia.govt.nz)

---

\(^{12}\) Criteria: The witness must not be a relative or part of the family group of the applicant; be a partner of the applicant; or live at the same address as the applicant. The witness must have known the applicant for at least 12 months (or since birth for children less than 12 months); be 16 years or over; and have a daily contact telephone number and be available during normal business hours.

\(^{13}\) As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
## New Zealand Refugee Travel Document

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>An official government document, issued to people who are not New Zealand citizens and whose refugee status has been confirmed by the Department of Labour (Immigration), which enables travel abroad.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained in a Refugee Travel Document (RTD) includes:  
  - first/given name(s) and surname/family name(s)  
  - date of birth  
  - place of birth  
  - gender  
  - photo of individual  
  - nationality.  
  Other information in an RTD includes:  
  - type  
  - issuing state  
  - issuing authority  
  - document number  
  - dates of issue and expiry. |
| **Document features** | A booklet with a data page containing identity information about the individual.  
It is issued in accordance with United Nations protocols. |
| **Validity**       | An RTD is valid for between one and four years. |
| **Issuance process** | Applicants complete an ‘Application for a Certificate of Identity or Refugee Travel Document’. Another person, who meets criteria, fills in a ‘Proof of Identity’ section.  
Department of Internal Affairs staff check that the applicant does not already hold a New Zealand passport and compare information from the Department of Labour (Immigration) with that on the application.  
Applicants must have proof of refugee status and provide two passport-style photographs and any one of:  
- a Certificate of Identity (from the Department of Labour (Immigration))  
- a birth certificate  
- a passport from their country of origin  
- the travel document they used to enter New Zealand  
- a New Zealand Residence Permit/Returning Resident’s Visa/Work Permit or Visitor’s Visa  
- a letter from the Department of Labour (Immigration) confirming residence or refugee status.  
Applications are most commonly accompanied by one of the last two options in this list.  
Identity details are based on information from the Department of Labour (Immigration). |

---

14 Criteria that must be met are that they have known the individual for more than 12 months; are over 18 years of age; have a daytime contact telephone number; are not a relative; and do not live at the same address as the applicant.
### Legislation


### Standard fit

An RTD can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity).

An RTD provides confirmation of an individual’s name, nationality, date and place of birth, and what they look like. It also provides confirmation that the individual is not a New Zealand citizen and has refugee status.

The photo inside the RTD enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the RTD.\(^ {15} \)

### Further information

| Further information | www.dia.govt.nz |

---

\(^ {15} \) As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.

---

NOTE – RTDs can be issued solely on the basis of a statutory declaration, without corresponding EOI to reinforce the data. This document, therefore, should not be used on its own to verify the holder’s identity.
New Zealand Certificate of Identity (issued under the Passports Act 1992)

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>An official government document, issued to people who are not New Zealand citizens and who are unable to obtain a passport of their own nationality, which enables them to travel abroad.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained in a Certificate of Identity includes:  
  - first/given name(s) and surname/family name(s)  
  - date of birth  
  - place of birth  
  - gender  
  - photo of individual  
  - nationality.  
Other information in a Certificate of Identity includes:  
- type  
- issuing state  
- issuing authority  
- document number  
- dates of issue and expiry. |
| **Document features** | A booklet with a data page containing identity information about the individual. It is issued in accordance with United Nations protocols. |
| **Validity**       | A Certificate of Identity is valid for between one and four years. |
| **Issuance process** | Applicants complete an Application for a Certificate of Identity or Refugee Travel Document. Another person, who meets set criteria\(^{16}\), fills in a 'Proof of Identity' section.  
Department of Internal Affairs staff check that the applicant does not already hold a New Zealand passport and compare information from the Department of Labour (Immigration) with that on the application.  
Applicants must provide two passport-style photographs and any one of:  
- a Certificate of Identity (from the Department of Labour (Immigration))  
- a birth certificate  
- a passport from their country of origin  
- the travel document they used to enter New Zealand  
- a New Zealand Residence Permit/Returning Resident’s Visa/Work Permit or Visitor’s Visa  
- a letter from the Department of Labour (Immigration) confirming residence or refugee status.  
Applications are most commonly accompanied by one of the last two options in this list. Identity details are based on information from the Department of Labour (Immigration). |

\(^{16}\) Criteria that must be met are that they have known the individual for more than 12 months; are over 18 years of age; have a daytime contact telephone number; are not a relative; and do not live at the same address as the applicant.
A Certificate of Identity can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity).

A Certificate of Identity provides confirmation of an individual’s name, nationality, date and place of birth, and what they look like. It also provides confirmation that the individual is not a New Zealand citizen.

The photo inside the Certificate of Identity enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity\(^\text{17}\).

NOTE – Certificates of Identity can, in some cases, be issued solely on the basis of a statutory declaration, without corresponding EOI to reinforce the data. Therefore, this document should not be used on its own to verify the holder’s identity.

\(^{17}\) As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
# New Zealand Certificate of Identity (issued under the Immigration Act 1987)

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Labour (Immigration)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>An identity document issued to people who are not New Zealand citizens and are unable to obtain a passport of their own nationality. A Certificate of Identity is generally issued to refugees or people who have entered New Zealand with no form of documentary evidence on their identity.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained in a Certificate of Identity includes:  
  • name of holder  
  • date of birth  
  • country of birth  
  • photo of the individual.  
  Other information in a Certificate of Identity includes:  
  • date of issue  
  • Certificate of Identity number. |
| **Document features** | A folded card-type document that contains a photograph of the owner. |
| **Validity**       | Variable, on a case-by-case basis. A Certificate of Identity is normally valid for one or two years. |
| **Issuance process** | Certificates of Identity are issued by the Department of Labour (Immigration) and in accordance with policies from the United Nations High Commissioner for Refugees.  
  As a minimum requirement to establish identity, the applicant must sign a statutory declaration. The circumstances surrounding the issue of this document make it difficult to verify their details. |
| **Legislation**    | Immigration Act 1987. |
| **Standard fit**   | A Certificate of Identity can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity).  
  It provides information on an individual’s name, nationality and date and place of birth, and what they should look like. It also indicates that they are not a New Zealand citizen and will either have refugee status or no other form of documentary evidence to prove their identity.  
  The photo inside the Certificate of Identity enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity.  
  The viewer (e.g. an agency staff member) can establish that the presenter links to the information inside the Certificate of Identity. |
| **Further information** | www.immigration.govt.nz |

---

**NOTE** – Certificates of Identity can, in some cases, be issued solely on the basis of a statutory declaration, without corresponding EOI to reinforce the data. Therefore, this document should not be used on its own to verify the holder’s identity.

---

18 As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
## New Zealand Firearms Licence/Firearms Dealer’s Licence

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>New Zealand Police</th>
</tr>
</thead>
</table>
| **Purpose**        | A Firearms Licence allows an individual to have and use various types of firearms.  
A Firearms Dealer’s Licence is for arms dealers who buy, sell or make firearms by way of business. |
| **Information**    | Information about a person contained on Firearms and Firearms Dealer’s Licences includes:  
- given name(s) and family name  
- date of birth  
- photo of the individual.  
Firearms and Firearms Dealers’ Licences also contain a licence number. |
| **Document features** | Credit-card-size licence that includes a photograph of the owner. |
| **Validity**       | A Firearms Licence is valid for 10 years unless revoked or surrendered.  
A Firearms Dealer’s Licence is valid for one year. |
| **Issuance process** | Applications for a New Zealand Firearms Licence must be made in person at an Arms Office. The applicant must fill out a ‘New Zealand Firearms Licence Application Form’ and provide:  
- an old firearms licence (if applicable)  
- two recent passport-style photos  
- original documents meeting the current police ‘proof of identity point system’, which requires applicants to produce original documents totalling 100 points (e.g. a current passport is worth 70 points, and a birth certificate 40 points)  
- contact details of two referees – one must be the applicant’s spouse or next of kin, the other over 20 years of age and not related to the applicant.  
The applicant must sign the application in front of a Member of the Police, who is also required to fill out a witness section and verify the photo is that of the applicant.  
The applicant is vetted according to the Firearms Licence Vetting Guide. It verifies the applicant’s suitability to possess and use firearms (and places some emphasis on determining their identity). Applicants and all referees are interviewed, with referee questions specific to identity. |
| **Legislation**    | Arms Act 1983. |

19 An Arms Office is any police station or police office appointed as such by the Commissioner. The Commissioner has declared all police premises to be Arms Offices for the purpose of receiving applications for a firearms licence.
### Standard fit

A Firearms Licence or Firearms Dealer’s Licence can be used to meet the requirements of Objective A (that the identity exists), and in part, Objective C (presenting person links to the identity).

The Firearms Licence or Firearms Dealer’s Licence provides confirmation of an individual’s name, date of birth and what they should look like.

The photo on the Firearms Licence or Firearms Dealer’s Licence enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information on the Firearms Licence or Firearms Dealer’s Licence\(^\text{20}\).

### Further information

www.police.govt.nz

\(^\text{20}\) As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
# New Zealand Birth Certificate

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>To provide an official record of births registered in New Zealand.</td>
</tr>
</tbody>
</table>
| **Information**    | Contains registered information about an individual’s birth, including:  
|                    | • given/first name(s) and surname/family name(s)\(^{21}\)  
|                    | • gender  
|                    | • still-birth/multiple birth  
|                    | • date and place of birth  
|                    | • information about the parent(s) – given/first name(s) and surname/family name(s); date and place of birth and occupation.  
|                    | NOTE – Information about change of name, adoption and gender reassignment is set out in Appendix C. |
| **Document features** | An official birth record is registered information contained within the New Zealand Birth Register, and provides confirmation that a birth occurred in relation to the named individual and their parents.  
|                    | A birth certificate is a printed subset of the birth record. |
| **Validity**       | A birth certificate has no validity period associated with it. |
| **Issuance process** | A Preliminary Notice of Birth is sent to the Registrar\(^ {22}\) within five working days of the birth by the hospital, doctor, midwife or occupier of the premises where the birth took place.  
|                    | A Notification of Birth for Registration is sent to the Registrar by the child’s parent(s). There is no set time limit, but registrations more than two years after the birth must be referred to Registrar-General.\(^ {23}\)  
|                    | Details on the Preliminary Notice of Birth and those on the Notification of Birth for Registration are linked on the Births Registry system. The child’s birth record and registration details are now in the system. Registration cannot occur without the notice of birth having been entered.  
|                    | The Birth Register is a public register. As such, any individual can be issued a birth certificate or printout of the birth record, providing the request is in respect of a named individual and that they supply the required information (e.g. the name, date and place details contained on the birth record). |
| **Legislation**    | Births, Deaths, and Marriages Registration (BDMR) Act 1995. The BDMR Act requires all births in New Zealand to be registered. If applicants claim to have been born in New Zealand but cannot produce their birth certificate\(^ {24}\) or their official birth record cannot be verified, they should be advised to register their birth with Births, Deaths and Marriages (Department of Internal Affairs).\(^ {25}\) |

\(^{21}\) Any New Zealand Birth Certificate issued after the new name has been registered will show both the name registered at birth and all changes of name for that person.  

\(^{22}\) “Registrar” means a person for the time being holding office under section 81(1) of the BDMR Act; and includes the Registrar General and every Deputy Registrar-General.  

\(^{23}\) “Registrar-General” means the Registrar-General appointed under section 79(1) of the BDMR Act and includes every Deputy Registrar-General.  

\(^{24}\) Except where the applicant’s birth record is closed for a particular reason.  

\(^{25}\) A small number of individuals are not registered. For example, at 13 October 2003, 220 out of 57,574 births (or 0.38% of the total) were still unregistered from 1998. Births, Deaths and Marriages sends notifications that children need to be registered, but this process is reliant on the parent(s) or guardian(s) supplying the information.
<table>
<thead>
<tr>
<th><strong>Standard fit</strong></th>
<th>A birth certificate or verification against the birth record can only be used to meet the requirements of Objective A (that the identity exists). The birth certificate should not be used as the sole form of evidence for asserting an individual’s identity, as it does not provide any link to the person presenting it (for example, in the way a passport does). Birth certificates contain a warning to the effect that “this certificate is not evidence of the person presenting it”.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Further information</strong></td>
<td><a href="http://www.govt.nz">www.govt.nz</a></td>
</tr>
</tbody>
</table>
New Zealand Citizenship Certificate

<table>
<thead>
<tr>
<th>Issuing Agency</th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>An official government document, issued to people who are granted New Zealand citizenship (either by grant or descent).</td>
</tr>
<tr>
<td>Information</td>
<td>Information about a person contained on a Citizenship Certificate includes:</td>
</tr>
<tr>
<td></td>
<td>• name of individual (at time of citizenship grant or registration)</td>
</tr>
<tr>
<td></td>
<td>• gender</td>
</tr>
<tr>
<td></td>
<td>• date of birth</td>
</tr>
<tr>
<td></td>
<td>• place of birth</td>
</tr>
<tr>
<td></td>
<td>• effective date of citizenship.</td>
</tr>
<tr>
<td>Document features</td>
<td>A landscaped A4 size printout of the above information, containing security features.</td>
</tr>
<tr>
<td>Validity</td>
<td>There is no validity period associated with a Citizenship Certificate.</td>
</tr>
<tr>
<td>Issuance process</td>
<td>To meet the criteria for the issue of a New Zealand citizenship certificate, an individual must:</td>
</tr>
<tr>
<td></td>
<td>• obtain citizenship by descent, or</td>
</tr>
<tr>
<td></td>
<td>• obtain citizenship by grant.</td>
</tr>
<tr>
<td></td>
<td>Applicants for citizenship by descent or grant must provide original documentation that establishes their identity. This includes:</td>
</tr>
<tr>
<td></td>
<td>• two identical passport-style photographs (one certified by a witness as a true likeness of the applicant)</td>
</tr>
<tr>
<td></td>
<td>• birth certificate(s)</td>
</tr>
<tr>
<td></td>
<td>• passport(s) (from their current country of citizenship)</td>
</tr>
<tr>
<td></td>
<td>• travel document(s)</td>
</tr>
<tr>
<td></td>
<td>• marriage certificate(s) (if applicable)</td>
</tr>
<tr>
<td></td>
<td>• proof of name change (if applicable)</td>
</tr>
<tr>
<td></td>
<td>• Certificate of Identity (generally from refugees).</td>
</tr>
<tr>
<td></td>
<td>The individual’s identity is determined by combining this information. Details from the application are entered into the citizenship system. Case officers assess applications and, once the grant of citizenship is approved applicants must take an oath or affirmation of allegiance at a Citizenship Ceremony to receive their Citizenship Certificate. This is not a requirement if receiving citizenship by descent and in some other exceptional cases.</td>
</tr>
<tr>
<td></td>
<td>NOTE – Photos of the applicant are scanned into the system and linked to their file (the photo does not appear on their Citizenship Certificate). The witness who certified the photo is not contacted to verify identity; the photos are used to match those in documentation accompanying the application (e.g. a passport).</td>
</tr>
</tbody>
</table>
### Standard fit

A Citizenship Certificate can be used to meet Objective A (that the identity exists). It provides confirmation of an individual’s name and date and place of birth. Information on the certificate is consistent with original documentation (provided by the applicant for identification purposes).

Although a photo of the applicant is kept on the citizenship system, it does not appear on the certificate. This means a Citizenship Certificate should not be used to meet Objective C (presenting person links to identity).

| Further information | www.dia.govt.nz |

**Evidentiary Certificates**

These certificates provide confirmation of citizenship and are available for New Zealand born citizens, or where a citizen’s details have changed since the issue of the certificate e.g. through a change of name or gender reassignment. These are not common and are issued in the form of an open letter on official letterhead.
## New Zealand Death Certificate

<table>
<thead>
<tr>
<th>Issuing Agency</th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>To provide an official record of deaths registered in New Zealand.</td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td>Contains registered information on an individual’s death, including:</td>
</tr>
<tr>
<td></td>
<td>• given/first name(s) and surname/family name(s)</td>
</tr>
<tr>
<td></td>
<td>• given/first name(s) and surname/family name(s) at birth</td>
</tr>
<tr>
<td></td>
<td>• date, place and cause(s) of death</td>
</tr>
<tr>
<td></td>
<td>• name of certifying doctor</td>
</tr>
<tr>
<td></td>
<td>• date last seen alive by certifying doctor</td>
</tr>
<tr>
<td></td>
<td>• gender</td>
</tr>
<tr>
<td></td>
<td>• age and date of birth</td>
</tr>
<tr>
<td></td>
<td>• place of birth</td>
</tr>
<tr>
<td></td>
<td>• usual residential address</td>
</tr>
<tr>
<td></td>
<td>• occupation</td>
</tr>
<tr>
<td></td>
<td>• date and place of burial/cremation</td>
</tr>
<tr>
<td></td>
<td>• age of children</td>
</tr>
<tr>
<td></td>
<td>• parent(s) given/first name(s) and surname/family name(s)</td>
</tr>
<tr>
<td></td>
<td>• parent(s) given/first name(s) and surname/family name(s) at birth</td>
</tr>
<tr>
<td></td>
<td>• parent(s) occupation</td>
</tr>
<tr>
<td></td>
<td>• relationship details of the deceased.</td>
</tr>
<tr>
<td><strong>Document features</strong></td>
<td>An official death record is the registered information contained within the New Zealand death registry, and provides confirmation that a death occurred in relation to the named individual and their parents. A Death Certificate is a printed subset of the death record.</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td>A Death Certificate has no validity period associated with it.</td>
</tr>
<tr>
<td><strong>Issuance process</strong></td>
<td>A Notification of Death for Registration is sent to the Registrar within three working days after disposal of the body. This form is accompanied by either a Medical Certificate of Causes of Death, a Medical Certificate of Causes of Foetal and Neonatal Death, or an Order for Disposal.</td>
</tr>
<tr>
<td></td>
<td>The Births, Deaths and Marriages system registers this information and links it to a birth record for births since 1998. Where a match with a birth record has been identified, both files are flagged. If a birth certificate is subsequently issued, the word ‘deceased’ appears on it.</td>
</tr>
<tr>
<td></td>
<td>Once the information is registered, anyone can request any named death certificate.</td>
</tr>
<tr>
<td></td>
<td>Any government agency that wishes to know if a birth that has been registered was the birth of a person who has since died, or a still-birth, may apply to the Registrar-General for information and the Registrar-General is obliged, on payment of the prescribed fee, to have a search undertaken and provide the applicant with the result of that search.</td>
</tr>
</tbody>
</table>

26 The absence of a New Zealand death certificate does not conclusively indicate that an identity is living, rather that an identity has not died in New Zealand.

27 “Registrar” means a person for the time being holding office under section 81(1) of the BDMR Act; and includes the Registrar General and every Deputy Registrar-General.

28 “Registrar-General” means the Registrar-General appointed under section 79(1) of the BDMR Act and includes every Deputy Registrar-General.
**Standard fit**

A Death Certificate or electronic verification against the Death Register information can only be used to meet the requirements of Objective B (that it is a living identity).

Verifying applicant details against death records will help to determine whether an identity has been recorded as deceased. However, having no record that a person has died does not necessarily mean that they are still alive (see note below).

**Further information**

www.govt.nz

**NOTE –**

1. Death notifications are generated and sent to agencies that Births, Deaths and Marriages has statutory obligations to notify (e.g. Registrar of Electors).

2. There are currently no provisions to share death information with foreign death registries, and currently Births, Deaths and Marriages do not access foreign registries to match death and birth information. So there is a potential risk associated with verifying against death records, in that individuals may have died overseas and not be recorded as ‘deceased’ within the New Zealand death register.
## New Zealand Driver Licence

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Land Transport New Zealand</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>A driver licence provides evidence that the individual named and photographed has a licence to drive.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained on a driver licence includes:  
  - given name(s) and family name  
  - date of birth  
  - their signature  
  - their address (optional)  
  - photo of the individual.  
  Other information on a driver licence includes:  
  - issue and expiry dates  
  - donor indicator (DONOR or blank)  
  - driver licence number  
  - card version number  
  - class of licence  
  - graduated classes/endorsements  
  - class/endorsements for conditions. |
| **Document features** | Credit-card-size document with a photograph of the holder and their signature. |
| **Validity**       | Valid for a period of ten years. |
| **Issuance process** | Applications must be made in person to a licensing agent. The applicant must fill out the necessary driver licence application and bring with them one form of primary identification, in accordance with EOI requirements specified in Clause 1 ‘Identification’ Land Transport (Driver Licensing) Rule 1999. Forms of primary identification include: New Zealand passport*; New Zealand driver licence or overseas driver licence*, certificate issued under the Citizenship Act 1977 and Firearms Licence*.  
  Applicants must also provide one form of evidence showing their name and address, such as: an account issued in the previous 12 months; a utility (e.g. telephone or power) account issued in the previous six months; or an appropriate form of identification issued within the previous 12 months that includes their address.  
  Customer service representatives process the application and, if applicable, take the applicant’s photo and an electronic impression of the signature.  
  * Must be current or have expired within the two years prior to the date of application. |
| **Legislation**    | Land Transport Act 1998. |

---

29 A licensing agent is the Director or a person to whom the Director has delegated functions and powers under section 205(2) of the Land Transport Act 1998 in relation to the issuing, renewal and replacement of driver licences.
A New Zealand driver licence on its own can be used to meet Objective E (use of the identity in the community). It can also be used to satisfy, in part, Objective C (presenting person links to the identity), so long as it is considered alongside documents that satisfy Objective A (that the identity exists).

A driver licence provides confirmation of an individual’s name and date of birth and what they should look like. It also provides confirmation that the holder is allowed to drive vehicles subject to their licensing classes.

The photo on a driver licence enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information on the driver licence. As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.

| Standard fit       | A New Zealand driver licence on its own can be used to meet Objective E (use of the identity in the community). It can also be used to satisfy, in part, Objective C (presenting person links to the identity), so long as it is considered alongside documents that satisfy Objective A (that the identity exists). A driver licence provides confirmation of an individual’s name and date of birth and what they should look like. It also provides confirmation that the holder is allowed to drive vehicles subject to their licensing classes. The photo on a driver licence enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information on the driver licence. | Further information | www.ltsa.govt.nz |
# 18+ Card

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Hospitality Association of New Zealand</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>The 18+ Card is used in lieu of a passport or driver licence as proof of age identity to purchase alcohol or gain admittance into licensed premises.</td>
</tr>
</tbody>
</table>
| **Information**    | Information about a person contained on an 18+ Card includes:  
• given name(s) and family name  
• date of birth  
• their signature  
• photo of the individual.  
Other information on an 18+ Card includes:  
• expiry date  
• card number. |
| **Document features** | Credit-card-size document with a photograph of the holder. |
| **Validity**       | Valid for a period of ten years. |
| **Issuance process** | To obtain an 18+ Card applicants must provide a recent passport-style photo and one of the following forms of evidence of identification:  
• NZ passport*  
• NZ driver licence*  
• Overseas passport*  
• Certificate of Identity (issued under the Passports Act 1992)*  
• Refugee Travel Document.*  
Or, if applicants use any of the following documents, they must also have an Identifier Statement completed and photo endorsed.  
• Citizenship Certificate  
• Certificate of Identity (issued under the Immigration Act 1987)*  
• A confirmation of residence permit  
• New Zealand birth certificate  
• Birth certificate from overseas country containing information equivalent to that contained in a New Zealand birth certificate.  
* Must be current or has expired in the two years prior to the date of application.  
The applicant must also produce one of the following additional forms of evidence confirming the name and address of the applicant:  
• an account statement, issued to the applicant in the 12 months immediately preceding the date of the application, from a bank, building society, credit union, or credit card issuer  
• a telephone, gas, or electricity account issued to the applicant in the 6 months immediately preceding the date of the application  
• a letter from an employer or educational institute, which is dated not more than 12 months preceding the date of application and includes the name and address of the applicant. |

---

31 To be completed by a person who is over 20 years of age, possesses a current Passport or NZ Driver Licence, and has known the applicant for one year or more. This person is not allowed to be a relative, spouse or partner, or living at the same address as the applicant.
<table>
<thead>
<tr>
<th><strong>Legislation</strong></th>
<th>Sale of Liquor Act 1989.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard fit</strong></td>
<td>An 18+ Card on its own can be used to meet Objective E (use of the identity in the community). It can also be used to satisfy Objective C (presenting person links to identity), as long as it is considered alongside documents that satisfy Objective A (that the identity exists). An 18+ Card provides confirmation of an individual’s name and date of birth and what they should look like. The photo on an 18+ Card enables in-person verification – whereby the viewer (e.g. an agency staff member) can establish that the presenter links to the information on the 18+ Card. For many people, particularly youth, this is the only form of photographic identification that they may have.</td>
</tr>
<tr>
<td><strong>Further information</strong></td>
<td><a href="http://www.hanz.org.nz">www.hanz.org.nz</a></td>
</tr>
</tbody>
</table>

32 As long as the person comparing the photo in the passport to the individual standing in front of them is confident that they match.
# Community Services Card

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Ministry of Social Development</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>A document that enables holders to obtain subsidies when visiting the doctor or paying for prescriptions.</td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td>Information about a person contained on a Community Services Card includes:</td>
</tr>
<tr>
<td></td>
<td>• given name(s) and family name</td>
</tr>
<tr>
<td></td>
<td>• the individual’s signature (on the back of the card).</td>
</tr>
<tr>
<td></td>
<td>Other information on a Community Service Card includes:</td>
</tr>
<tr>
<td></td>
<td>• client number</td>
</tr>
<tr>
<td></td>
<td>• issue and expiry dates.</td>
</tr>
<tr>
<td><strong>Document features</strong></td>
<td>A credit-card-type document. It does not contain a photograph of the holder.</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td>Validity of 3 to 24 months from date of issue, depending on the cardholder’s situation.</td>
</tr>
<tr>
<td><strong>Issuance process</strong></td>
<td>Applicants must complete an Application for Community Services Card form and provide proof of income and identity to show they are entitled to the Card. First-time applicants are required to have a Proof of Identity section completed by a person who:</td>
</tr>
<tr>
<td></td>
<td>• is over 18 years of age</td>
</tr>
<tr>
<td></td>
<td>• has known the applicant for at least 12 months</td>
</tr>
<tr>
<td></td>
<td>• is not a relative</td>
</tr>
<tr>
<td></td>
<td>• does not live at the same address as the applicant.</td>
</tr>
<tr>
<td></td>
<td>Applicants not born in New Zealand are required to send a copy of their visa or Citizenship Certificate.</td>
</tr>
<tr>
<td></td>
<td>Applicant details are checked to confirm eligibility. There are no requirements to provide documentation establishing identity, although processing officers may ask for further information in certain circumstances (e.g. for proof of income).</td>
</tr>
<tr>
<td><strong>Legislation</strong></td>
<td>Social Security Act 1964.</td>
</tr>
<tr>
<td><strong>Standard fit</strong></td>
<td>A Community Services Card can be used to meet Objective E (use of the identity in the community).</td>
</tr>
<tr>
<td><strong>Further information</strong></td>
<td><a href="http://www.govt.nz">www.govt.nz</a></td>
</tr>
</tbody>
</table>
## Electoral roll record

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Ministry of Justice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>A publicly available publication, by electorate, listing details of everyone who is enrolled to vote at the date the roll is printed.</td>
</tr>
</tbody>
</table>
| **Information**    | Information contained in the electoral roll about individuals includes:  
  • full name  
  • residential address  
  • occupation.  
  A letter of confirmation of enrolment is posted by the Registrar once the elector has been enrolled.  
  Copies of the electoral roll can be purchased in hard copy. |
| **Document features** | See above. |
| **Validity**       | Prior to major electoral events an enrolment update campaign is undertaken, whereby all registered electors are mailed a copy of their enrolment details and given the opportunity to update them, if necessary. |
| **Issuance process** | All eligible electors must enrol as a voter. To qualify, they must:  
  • be 18 years of age or older  
  • be a New Zealand citizen or a permanent resident and have lived in New Zealand for 12 months continuously at some stage. |
| **Legislation**    | Electoral Act 1993. |
| **Standard fit**   | An electoral roll record can be used to meet Objective E (use of the identity in the community). Agencies can either:  
  • verify applicant details against the printed electoral roll  
  • request that the individual supply their confirmation of enrolment letter. |
| **Further information** | [www.govt.nz](http://www.govt.nz) |
## IR number

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Inland Revenue (IR)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>A registered number corresponding to an individual or organisation for taxation purposes. All individuals receiving income in New Zealand are required to have an IR number.</td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td>Individuals being issued with an IR number for the first time or receiving confirmation of an existing number are issued with a lightweight card that contains their full name and the IR number. Statements from Inland Revenue also contain this information plus their address.</td>
</tr>
<tr>
<td><strong>Document features</strong></td>
<td>See above.</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td>An IR number has no validity period associated with it.</td>
</tr>
</tbody>
</table>
| **Issuance process** | Applicants must complete the appropriate application form and send a photocopy of one of the following documents for identification purposes:  
  - Birth certificate  
  - New Zealand passport  
  - 18+ Card  
  - Overseas passport  
  - Certificate of Citizenship  
  - Photo-ID driver licence.  
  Processing officers check name and date of birth information against current data. If there is a match, they send the applicant’s previous IR number. A new IR number is issued if there is no match with current data. |
| **Standard fit**   | An IR card or statement can be used to meet Objective E (use of the identity in the community). |
| **Further information** | [www.govt.nz](http://www.govt.nz) |
New Zealand Marriage Certificate

<table>
<thead>
<tr>
<th>Issuing Agency</th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>To provide an official record of marriages registered in New Zealand.</td>
</tr>
</tbody>
</table>
| **Information**                | Contains registered information about a couple’s marriage at the time of the marriage, including:  
  - given/first name(s) and surname/family name(s) of each partner  
  - given/first name(s) and surname/family name(s) at birth of each partner  
  - date and place of birth of each partner  
  - usual occupation of each partner  
  - relationship status  
  - date and location when the marriage was solemnised  
  - usual residential address  
  - parent(s) given/first name(s) and surname/family name(s) for each partner  
  - parent(s) surname/ family name(s) at birth for each partner. |
| **Document features**          | The marriage record is the registered information pertaining to marriages contained within the marriage register. A Marriage Certificate is a printed subset of the record that provides confirmation that a marriage took place in relation to the bride and bridegroom and their parent(s). |
| **Validity**                   | A Marriage Certificate has no validity period associated with it. |
| **Issuance process**           | To initiate the process, one of the parties getting married must first complete a Notice of Intended Marriage and sign a statutory declaration on the form.  
  If the individuals are ‘legally free’ to marry, a Marriage Licence is issued and is valid for three months. During this period the marriage ceremony takes place, and the marriage celebrant returns a copy of the Particulars of Marriage to the Registrar within 10 working days of the ceremony. If the marriage ceremony does not take place during this period, it is recorded that the ‘Marriage did not take place’.  
  Department of Internal Affairs staff enter this data on the marriage register once the marriage has taken place.  
  At the time of marriage, the parties are given a copy of the Particulars of Marriage that can be used as an official document to confirm that a marriage took place.  
  Once the information is registered anyone can request a copy of a Marriage Certificate provided they provide baseline details that are contained on the record (e.g. names of parties to the marriage and the date and place of the marriage). |
| **Standard fit**               | The Marriage Certificate can be used to prove officially that one partner can use the other partner’s surname as her/his own surname. As such, a Marriage Certificate only provides corroborative evidence about the use of a married name.  
  Because the identification of applicants is based upon a statutory declaration and anyone is able to request a named Marriage Certificate, this Certificate should not be used as a primary form of identification. |
| **Further information**        | [www.govt.nz](http://www.govt.nz) |

---

33 “Registrar” means a person for the time being holding office under section 81(1) of the BDMR Act; and includes the Registrar General and every Deputy Registrar-General.
# New Zealand Civil Union Certificate

<table>
<thead>
<tr>
<th><strong>Issuing Agency</strong></th>
<th>Department of Internal Affairs (Identity Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>To provide an official record of civil unions registered in New Zealand.</td>
</tr>
</tbody>
</table>
| **Information**    | Contains registered information about a couple’s civil union at the time of entering the civil union, including:  
  • given/first name(s) and surname/family name(s) of each partner  
  • given/first name(s) and surname/family name(s) at birth of each partner  
  • date and place of birth of each partner  
  • usual occupation each partner  
  • relationship status  
  • date and location when the civil union was solemnised  
  • usual residential address  
  • parent(s) given/first name(s) and surname/family name(s) for each partner  
  • parent(s) surname/family name(s) at birth for each partner. |
| **Document features** | The civil union record is the registered information pertaining to the civil union contained within the civil union register. A Civil Union Certificate is a printed subset of the record that provides confirmation that a civil union took place in relation to each partner and their parent(s). |
| **Validity**       | A Civil Union Certificate has no validity period associated with it. |
| **Issuance process** | To initiate the process, one of the parties entering into the civil union must first complete a *Notice for Intended Civil Union* and sign a statutory declaration.  
  If the individuals are ‘legally free’ to enter into a civil union, a *Civil Union Licence* is issued and is valid for three months. During this period the civil union ceremony takes place, and the civil union celebrant returns a copy of the *Particulars of Civil Union* to the Registrar within 10 working days of the ceremony. If the civil union ceremony does not take place during this period, it is recorded that the ‘Civil Union did not take place’.  
  Department of Internal Affairs staff enter this data on the civil union register once the civil union has taken place.  
  At the time of the civil union, the parties are given a copy of the *Particulars of Civil Union* that can be used as an official document to confirm that a civil union took place.  
  Once the information is registered anyone can request any named Civil Union Certificate provided they can provide baseline details that are contained on the record (e.g. names of parties to, and date and place of, the civil union). |
| **Legislation**    | Civil Union Act 2004. |
| **Standard fit**   | The Civil Union Certificate can be used to prove officially that one partner can use the other partner’s surname as her/his own surname. As such, a Civil Union Certificate only provides supporting evidence about the use of a partner’s surname.  
  Because the identification of applicants is based upon a statutory declaration and anyone is able to request a named Civil Union Certificate, there is a risk with using the certificate or corresponding data as a primary form of identification. |
| **Further information** | www.govt.nz |

34 “Registrar” means a person for the time being holding office under section 81(1) of the BDMR Act; and includes the Registrar General and every Deputy Registrar-General.
Appendix B –
EOI ‘Supporting’ documents/records referenced in this Standard

This section has examples of supporting evidence that can be used to meet Objective E of the EOI requirements process, where the individual is unable to provide the relevant documents/records that are specified in Appendix A.

These documents may also, in some cases, be used to verify/provide evidence that an individual lives at a given address.

The examples are not exhaustive and agencies may choose to use alternatives. In doing so, they should assess whether the alternative’s level of identity verification is similar to that of these examples.

Credit cards, bank cards and financial accounts

• These are cards or statements issued to bank account holders that allow them to access funds electronically or outline their account activity.

• Bank cards are issued in the account holder’s name and sometimes include their photo. To open an account at a bank, the customer is required to provide documentation to establish their identity that usually includes:
  • photo ID (eg. driver licence or passport)
  • birth certificate
  • form of address (eg. utility account)
  • proof of income (eg. payslips, bank statement, letter from employer)
  • IR number.

• Accounts are opened on the basis of this information. Generally, there are no verification checks to further identify the customer.

International Driving Permit (issued by the Automobile Association of New Zealand)

• An International Driving Permit (IDP) is an internationally recognised document. It is a translation of a current driver licence. It is not a driver licence in its own right, so the original driver licence must be carried with it.

• An IDP is issued for touring purposes only. The IDP is valid for 12 months from the date of issue. It can only be issued to a full licence holder who is over 18 years of age. It is not available for commercial use. Most countries allow use of an IDP for a maximum of 12 months. Work permit holders and permanent residents may apply for a New Zealand driver licence.
Confirmation of Permit Status
(issued by Department of Labour – Immigration)

- This letter is generally issued to permit holders who have misplaced or lost their permits or to people who may have entered New Zealand as a minor included on their parents’ travel documents. Confirmation of Permit Status letters are issued on official letterhead and generally include the individual’s customer number, name, date and country of birth, permit number, permit type, date of issue and date of expiration. To obtain a Confirmation of Permit Status an individual must provide either their customer number and/or enough EOI to satisfy the issuing officer.

Steps to Freedom (issued by Department of Corrections)

- Steps to Freedom forms are issued to prisoners upon release to enable them to access financial services from Work and Income. This document is issued under the Social Security Act 1964 and provides identity information about the individual. This information is obtained via the prison service, through the judicial system.

- Work and Income accept the Steps to Freedom form as validating identification. First-time applicants are also required to provide primary identification.

Student identity cards and employee identification cards

- These are cards issued to students or employees of schools/institutions or organisations that are generally used for internal identification purposes. They are similar to a driver licence, with a photo of the person and some biographical data such as their name and date of birth. The card may include a unique identifier, such as a student ID or employee number.

- These cards are generally issued on the basis of student application forms or information provided by employees.

Utility accounts

- These are accounts established with service providers such as telecommunication and energy companies.

- The services these companies provide require regular contact between the customer and the service provider, with statements in document form generated to communicate account details. These statements can be used in some circumstances to illustrate that an individual is a customer of a company, and that they live or have lived at a particular address.

- Identification requirements for individuals to ‘open’ an account generally involve providing name and address information (particularly for phone and energy accounts, as the service is provided to a particular address). However, this information usually goes unverified against any source until there is an issue with the account.
Appendix C – Change of name, adoption and gender reassignment documents/records referenced in this Standard

Change of name

In order for changes of name for adults or children to be officially recognised, they need to be registered with Births, Deaths and Marriages of the Department of Internal Affairs (Identity Services). This requires completion of a Statutory Declaration (an officially signed and witnessed statement).

If the new name is accepted, it is then registered by Births, Deaths and Marriages. Any New Zealand birth certificate issued after the new name has been registered will show both the name registered at birth and all changes of name for that person. Changes of name by Deed Poll ceased in September 1995.

NOTE – In some countries it is common to advertise a change of name in a prominent nationwide newspaper, and this may be accepted in lieu of an official certificate.

Process for individuals aged over 18

Individuals aged over 18 and born in New Zealand must supply either their:
- New Zealand birth certificate, or
- New Zealand passport (issued in the birth name).

Individuals born outside New Zealand must supply either their:
- Birth certificate, or
- Some other evidence that satisfies the Registrar-General of their date and place of birth, and their name at birth.

Only original documents are accepted, and any translated documents must be accompanied by the original document. If an individual is married or enters into a civil union, a change of name can be noted on the marriage or civil union registration. This is only possible if the marriage or civil union took place in New Zealand.

Process for changing the name of a child

In most circumstances a change of name for a child must be made by the guardians of the child. This usually means both parents, even if they are not married or living together. Even if only one parent has custody, both parents must sign the form. If any other guardians have been appointed, they must also make a Statutory declaration.

If a guardian is not able to sign, the reason why one guardian may need to act alone must be described in the Statutory Declaration. This may be for reasons such as:
- he/she is missing (provide details)
- he/she is dead
- he/she is not known
- is unable to act because of unsound mind or medical condition.
There are some other circumstances where the Family Court may allow one guardian to act alone to change the child’s name. Applicants will need papers issued by the Court to support the change of name.

If no guardians are available, a change of name form may be completed by the Chief Executive of the Department of Child, Youth and Family Services.

Guardians fill out different forms depending on the age of child, whether they are born in New Zealand or outside New Zealand and relationship status. For details on this refer to: www.dia.govt.nz

**Proof of change/usage of name**

Evidence that may be used to confirm use of a partner’s surname include:

- New Zealand Marriage Certificate  
  (issued by Department of Internal Affairs –Identity Services)
- New Zealand Civil Union Certificate  
  (issued by Department of Internal Affairs –Identity Services)
- Dissolution of a marriage (divorce) papers (issued by the Ministry of Justice)
- Marriage declared void (annulment) papers (issued by the Ministry of Justice).

Applicants must provide the Ministry of Justice with either a birth certificate, passport or driver licence, in conjunction with proof of marriage and proof of address, to file for a divorce or annulment.

**Adoption records**

When a person is adopted, the original birth record is closed and a new birth record created. The adoptive parents become the legal parents of the adopted person, and the new name given by the adoptive parents becomes the person’s new legal name.

In some cases, if a child has been adopted overseas, the adoption may be registered in New Zealand, in a similar fashion to New Zealand adoptions, if the adoption meets certain criteria.

The Adult Adoption Information Act 1985 allows for adopted individuals to find out about their birth parents, and their pre-adoptive identity. A birth certificate issued from that original record must show that it relates to the person’s pre-adoptive identity, because that is not the person’s current legal identity. That certificate cannot be used for official purposes.
Gender reassignment
Any person aged 18 (or guardians of a child under 18) may apply to a Family Court for a declaration that a birth certificate issued for that person should show a different gender to that which currently appears on their birth registration (or should show a certain gender where that person was born of indeterminate gender), where the Court is satisfied that the person has undergone the necessary treatment for that person to maintain that new identity.

On receipt of such an Order, the Department of Internal Affairs (Identity Services) creates a new post-sex-change registration for the person. The earlier record of the person’s birth entry is, in effect, cancelled. The effect of the re-registration is that a new identity is created so that, to all intents and purposes, the person has always been a person of their nominated sex. Any birth certificate(s) issued for the person will show the new sex, and any new names that have been included since the new registration was made, as if those names were the person’s names since birth. Section 64(4) of the Births, Deaths, and Marriages Registration (BDMR) Act 1995 provides that such a birth certificate may, by virtue of the serial number it bears, be capable of indicating that sexual assignment/reassignment information has been included on it. However, in practice, this has not been the case.

Access to information relating to a person’s identity prior to the registration of sexual assignment or reassignment is restricted. Only the Registrar-General may grant access to such information, and only where satisfied that the person seeking the information is the person to whom the information relates; or that the information is required in connection with the administration of an estate or trust, or by a marriage celebrant or Registrar for the purposes of investigating whether or not the parties to a proposed marriage are a man and a woman (section 77(6) of BDRM Act refers); or where 120 years has passed since the birth of the person to whom the information relates. Otherwise, access can only be granted on the order of a Family Court, a District Court or the High Court for limited purposes (section 77(8) of BDRM Act refers).

In addition, there is provision for the Registrar-General to notify any Government agency that has an interest in ensuring that people do not have more than one identity of details relating to people who have registered gender assignment or reassignment.