

# 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**

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 May be superseded once other authentication key standards are developed.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

## 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](http://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:

<b>Part</b>	<b>Title</b>	<b>Description</b>
1	Introduction and Overview	Outlines the purpose, scope and application of this Standard.
2	Minimum Standard Requirements	Outlines the minimum process step requirements that agencies <b>MUST</b> follow to comply with this Standard.
3	Guidance Material	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 <b>SHOULD</b> follow this guidance material when implementing the minimum requirements set out in Part 2.
Appendix A, B, C	Documents/Records referenced in this Standard	Provides detail on the issuance processes behind, and appropriate uses of, the identity-related documents and records referred to within this Standard. The Appendices <b>SHOULD</b> be referred to when agencies are designing the evidential requirements to be placed on service customers.

## 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 definitions<sup>1</sup> apply:

Term	Definition
<b>Agency</b>	Any government organisation that applies this Standard.
<b>Anonymous service</b>	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.
<b>Attributed identity</b>	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.)
<b>Benchmark</b>	Evaluate or check processes by comparing with a standard point of reference.
<b>Biographical information</b>	Record of the events that occur during a person’s lifetime, e.g. birth registration, employment history and marriage or civil union registration.
<b>Biometric information</b>	Physical and behavioural attributes of a person, e.g. their facial features, DNA profile, retina, iris, voice and fingerprints.
<b>Biometric recognition</b>	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.
<b>Business processes</b>	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.
<b>Consequence</b>	Outcome or impact of an event. NOTE – (1) There can be more than one consequence from one event. (2) Consequences can range from positive to negative. (3) Consequences can be expressed qualitatively or quantitatively. (4) Consequences are considered in relation to the achievement of objectives.

<sup>1</sup> The terms event, frequency, likelihood, monitor and risk are taken from AS/NZS 4360.

## Definitions continued

<b>Term</b>	<b>Definition</b>
<b>Discrepancy</b>	Situations where an individual has supplied identity-related documents or information that may have an inconsistency requiring further investigation.
<b>e-GIF</b>	E-government interoperability framework – a collection of policies and standards endorsed for New Zealand government information technology (IT) systems.
<b>Electronic verification</b>	Verification of the accuracy of information through electronic checks of information records such as electronic databases.
<b>Evaluation</b>	Systematic review of processes to ensure that business processes are still effective and appropriate.
<b>Event</b>	Occurrence of a particular set of circumstances. NOTE – (1) The event can be certain or uncertain. (2) The event can be a single occurrence or a series of occurrences.
<b>Evidence of identity (EOI)</b>	The types of evidence that, when combined, provide confidence that an individual is who they say they are.
<b>Evidence of identity process</b>	Process by which an agency establishes confidence in an individual's identity.
<b>Evidence of identity process risks</b>	Any risk created through an EOI process.
<b>Exceptions/exception case</b>	Individuals (or a group of individuals) who, for genuine reasons, are unable to meet the EOI requirements set out in this Standard.
<b>False identities</b>	Situations where a person uses an identity that is not their own. In some cases, this can be for legitimate reasons.
<b>Frequency</b>	A measure of the number of occurrences per unit of time.
<b>Identification</b>	Process of associating identity data with a particular person.
<b>Identity</b>	A set of attributes and/or data linked to an individual person.
<b>Identity data/information</b>	Data/information pertaining to an individual's identity.
<b>Identity manipulation</b>	Alteration of one or more elements of identity (e.g. name, date of birth) to dishonestly obtain an advantage.
<b>Identity – misuse and abuse</b>	Gaining money, goods, services, other benefits or the avoidance of obligations through the use of a false or stolen identity.
<b>Identity-related risk</b>	Any risk for a particular service that results from an individual's identity being incorrectly attributed. See 3.3.2.1.
<b>Identity theft</b>	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.
<b>Internal controls</b>	Any policies, procedures, techniques and mechanisms put in place to minimise process failure and help ensure that actions are taken to address risks.
<b>Likelihood</b>	Used as a general description of probability or frequency. NOTE – Can be expressed qualitatively or quantitatively.

## Definitions continued

<b>Term</b>	<b>Definition</b>
<b>Monitor/monitoring</b>	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.
<b>Primary data source</b>	The original (i.e. issuing) source of identity data/information.
<b>Primary documents</b>	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).
<b>Pseudonymous service</b>	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.
<b>Risk</b>	The chance of something happening that will have an impact on objectives. NOTE – (1) A risk is often specified in terms of an event or circumstances and consequences that may flow from it. (2) Risk is measured in terms of a combination of the consequences of the event and their likelihood.
<b>Risk profiling</b>	The process of gathering data on characteristics (e.g. customer behaviours) in order to identify categories of risk.
<b>Service</b>	An activity conducted between a customer and a government agency, in accordance with the functions for which that agency is accountable.
<b>Supporting documents</b>	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).
<b>Trusted referee</b>	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: <ul style="list-style-type: none"> <li>• They have personal knowledge of the individual being identified</li> <li>• They are trusted by the agency according to the agency's own criteria of sufficient trust.</li> </ul>