



Evidence of Identity Standard Additional Guidance Online Establishment of Individual Identity



Introduction

The Evidence of Identity (EOI) Standard as a framework has been designed to be channel neutral. Version 1 of the Standard focused on establishment of identity while version 2 introduced additional information regarding the ongoing confirmation of identity.

With increased channel shift to the provision of services online and the development of common capability services to support this channel, a need has arisen for additional online specific guidance.

There are three aspects to authentication in the online environment

- The initial establishment of identity;
- The provisioning of an online credential to a person for future confirmation of identity; and
- The activity of ongoing confirmation of identity.

This guidance will address the first of these aspects and to a degree the second. For information on the third please refer to the *Authentication Key Strengths Standard*, the *Password Standard* and the *Guidance on Multi-factor Authentication*.

Initial establishment of identity

Section 7.7 of the EOI Standard covers the design and implementation of EOI processes. A key reference used is Table 8, which outlines the minimum evidential requirements for each EOI confidence level when establishing identity. These minimum requirements are channel neutral.

Below is a version of this table, providing the equivalent evidential requirements for an online identity establishment transaction.

Table 8 – Minimum evidential requirements for EOI Confidence level processes

EOI objective	Low EOI Confidence Level	Moderate EOI Confidence Level	High EOI Confidence Level
A – Identity exists	Provision of key data from 1 document/ record	Provision of key data from 1-2 documents/ records If discrepancies are identified in the EOI data provided by the individual, the data should be verified against source records held by the issuing agency	Provision of key data from 1-2 documents/ records which, where possible, have been validated against source records held by issuing agency
B – Identity is a ‘living identity’	(No specific process)	Business processes for Objective C	Verification against the New Zealand Death Register or Business processes for Objective C
C – Presenter links to identity	(No specific process)	Assertion of an online identity credential, or other business process, that includes or has been issued on the basis of verification by trusted referee or an in-person verification (agency office/on-site based) against a photo document	Assertion of an online identity credential, or other business process, that includes or has been issued on the basis of verification by trusted referee or an in-person verification (agency office/on-site based) against an authoritative source, preferably with a biometric comparison

D – Presenter is sole claimant of identity	Check against agency records	Check against agency records	<p>Check against agency records and</p> <p>Where appropriate to an agency's assessment of service risk:</p> <p><i>New Zealand born applicants:</i> verification of New Zealand Birth Certificate (issued since 1998) data against the birth register</p> <p><i>applicants not born in New Zealand:</i> a check against relevant registers may also satisfy this requirement.</p> <p>If none of these documents or registers are available a statutory declaration concerning any name changes may satisfy this requirement to a limited degree.</p> <p>or</p> <p>Assertion of an online identity credential that has been issued on the basis of one credential per authoritative identity record</p>
E – Presenter uses identity	Provision of key data from 1 document/ record	Provision of key data from 1 document/ record and/or Business processes for Objective C	Provision of key data from at least 2 documents/ records and/or Assertion of an online identity credential that has been issued on the basis of an in-person verification (agency office/on-site based) against an authoritative source

Further information on what is entailed in meeting the evidential requirements for each EOI objective is set out in sections 7.7.4 to 7.7.8 of the EOI Standard.

Online identity establishment implementation

It should be noted that while the table above outlines the minimum business requirements there will be other technical requirements to be met as part of implementation that are not covered here or in the EOI Standard. These include but are not limited to security, data formats, assertion messaging, authentication key strengths etc. The Department of Internal Affairs (DIA) can provide further advice on these aspects.

Provisioning an online credential

It is inherently built in to any online transaction that there is an online credential (e.g. a logon, username, password, token etc) created or established that allows the organisation to recognise the applicant (or customer) when they return in the future.

It is probable in most cases that the online identity credential held by the customer has been linked to a logon. The organisation may be able to reuse the customer's existing logon or alternatively attached the identity to their own logon service.

Note that there is a Cabinet Mandate requiring government agencies to adopt the igovt logon service.

Online identity verification services

The Department of Internal Affairs (DIA) has developed services to aid organisations to verify the identity of customers.

The **Data Validation Service (DVS)** is a secure way to confirm that identity data on a birth certificate, passport or other document is correct. It checks information against the authoritative source data held by DIA, aiding with the meeting of Object A. In the future it will also be able to support validation against the New Zealand Death Register for objective B.

The **igovt identity verification service** lets people assert their core identity attributes (full name, date of birth, place of birth and gender) via the internet. A person with an igovt ID has proved their identity to a high level, including an in-person event and collection of a biometric which has bound them to their online identity credential.

Currently the igovt identity verification service with igovt ID is the only known solution for the complete establishment of identity online to a moderate or high strength.

Further information

Agencies can use the [Risk Assessment Workbook](#) to identify the level of identity related risk of the services to be offered and thereby establish the level of confidence required in the identity establishment process.

Please contact the Department of Internal Affairs (DIA), for additional advice, if you wish to undertake either assessment - eoistandard@dia.govt.nz.