

Review of statutory authorities for information matching

Report by the Privacy Commissioner
to the Minister of Justice pursuant to
section 106 of the Privacy Act 1993 on
the Identity Verification Service
enabling provision:

Electronic Identity Verification Act
2012, s.39

April 2018

Introduction

In this report I assess the ongoing value and suitability of the information matching provision enabling the Department of Internal Affairs (DIA) Identity Verification Service (IVS). The IVS underpins RealMe by checking an individual's application against identity records held by DIA and other agencies.

Section 106 of the Privacy Act 1993 requires the Privacy Commissioner to carry out a review of the operation of each information matching provision which is subject to Part 10 of the Privacy Act 1993 at intervals of not more than 5 years and consider whether:

- the authority conferred by each provision should be continued; and
- any amendments to the provision are necessary or desirable.

Periodic reassessment of information matching arrangements is valuable as the forecast benefits from information sharing between agencies are sometimes not achieved, or decline over time for various reasons. Periodic reassessment ensures that the costs of the programme and the intrusion on privacy remains justified by the benefits to individuals or society.

Commissioner's recommendation

DIA operates a programme of information matches under section 39 of the Electronic Identity Verification Act 2012. The purpose of this programme of matches is to verify identity information provided by an applicant in support of their application for issuance, renewal, amendment, or cancellation of an Electronic Identity Credential (EIC), or to keep the core information contained in an EIC accurate and up to date.

I have assessed the value and suitability of this programme and I recommend that the provision continue without amendment.

My detailed assessment of this programme follows.

Appendix A gives a brief background to information matching, section 106 and the approach I have taken in undertaking this review.



John Edwards
Privacy Commissioner
April 2018

DIA Identity Verification Service (Electronic Identity Verification Act 2012, s.39)

1.1 Programme objectives

To verify identity information provided by an applicant in support of their application for issuance, renewal, amendment, or cancellation of an Electronic Identity Credential (EIC), or to keep the core information contained in an EIC accurate and up to date.

1.2 Recommendation

I recommend that the authority conferred by section 39 of the Electronic Identity Verification Act 2012 should be continued without amendment.

1.3 Programme assessment

Financial cost/benefit and other outcomes

The Identity Verification System underpins RealMe which has been closely monitored since it was launched in 2013. This monitoring has included three independent reviews to test whether the approach remained appropriate. The reviews included assessments of the costs and benefits and were consistently supportive of the role of the Identity Verification Service.

The estimated appropriation for RealMe in 2016/17 was \$17.125 million and budgeted appropriation for 2017/18 is \$26.538 million. RealMe has been funded through successive budget bids. In Budget 2015, the Government funded "RealMe" for \$21.67 million over three years, and in Budget 2017 provided an additional \$16.68 million over two years for "Maintaining RealMe Services". Budget 2017 also provided a departmental capital injection of \$6.5 million for Maintaining RealMe Services. IVS is a supporting system for RealMe and therefore would be included in this figure.

DIA estimates the benefit of reduced enrolment transaction costs at \$7 to \$12 million (depending on which agency avoids having to incur the costs of confirming an identity). Other benefits have been quantified as being of significantly greater value but are not reflected in direct savings. These benefits include:

- the reduced costs to government (central and local) of implementing and running online services requiring authentication and identity verification;
- reduced transaction costs for online services requiring identity;
- improved user experience (consistency); and
- reduction in incidence and impact of identity crime.

Compliance/operational difficulties

There have been no compliance or operational issues identified.

Scale of matching

The scale of the programme is appropriate. When an IVS application is processed the information is matched to the Births, Deaths, Marriages, Citizenship and Passports datasets. Matching against the Immigration dataset only occurs when either the application is based on immigration documents (to verify the application), or the applicant may hold immigration documents (to ensure the application is not a duplicate).

If the applicant has relied upon Hospitality NZ, Police or NZTA identity documents these are also matched. Because these are only checked with the applicant's consent this matching activity does not require legislation to authorise the activity.

Only the information necessary to confirm the identity credentials for a match against a particular dataset is used when making that match.

Alternative methods to achieve results

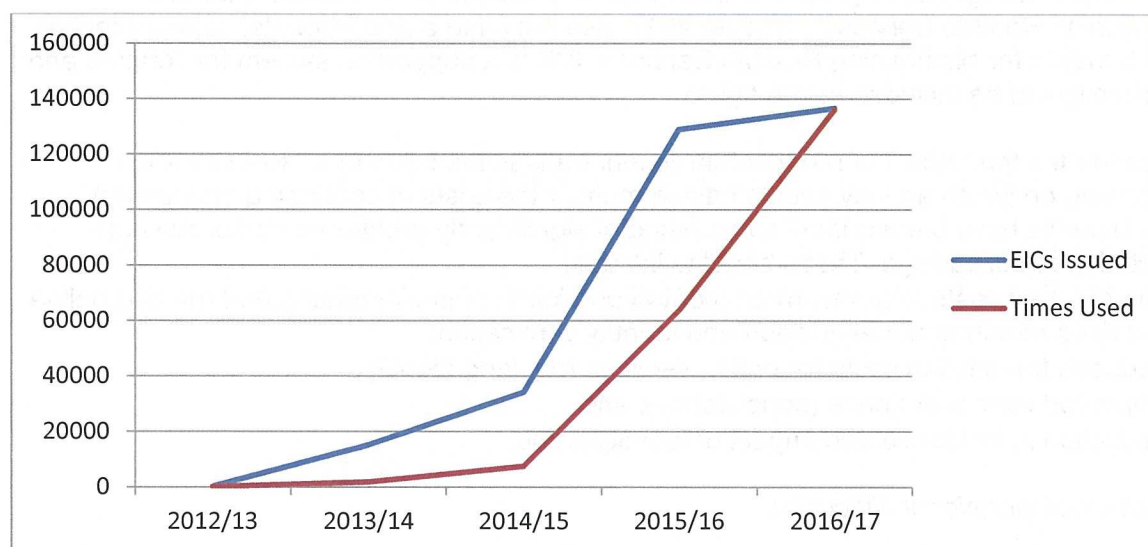
I consider that the IVS programme is likely to be the most effective way to confirm identity against New Zealand government identity records for electronic identity credentials. Alternative approaches could include: all individuals registering directly with each agency, or agencies relying on third party log-on services (for example allowing logging on using Facebook credentials). These all have disadvantages in cost and security.

Amendment to the information matching provision

DIA have no suggested amendments to the provision authorising this programme. I am satisfied that the provision is suitably constrained and does not require amendment.

1.4 Programme results

The IVS matching programme was implemented in 2013. Prior to the set up of the matching programme 1,729 EICs were issued in 2011/2012 based on existing online credentials and one of these EICs was also revoked that year.



	2012/13	2013/14	2014/15	2015/16	2016/17
EICs issued	227	15,220	34,162	128,935	136,606
EICs cancelled	0	10	8	25	31
Number of challenges to discrepancies	0	0	0	0	0
INZ matching	50	6,446	13,067	28,965	38,135
Use of EICs	132	1,775	7,457	63,725	136,017

From April 2015, people could apply for an EIC along with their passport application.

The number of agencies and services which users can access using RealMe has slowly grown. A full list of agencies and services can be found on the website:
<https://www.realme.govt.nz/what-it-is/where-to-use-realme/>

1.5 Programme operation

The Identity Verification Service underpins an electronic identity credential, such as RealMe, allowing people to prove that they are who they say they are in online transactions.

When people apply for electronic identity credentials the information matches that occur depend on which information and documents they provide to establish their identity. Some checks are made during the online application process for people who apply using their passport or citizenship certificate. Checks of the birth, death, marriage, civil union, name change, passport, citizenship or immigration records may also be made by IVS staff, for any type of applicant.

The checks are necessary to ensure that only one electronic identity credential is issued based on any of the various identity records that an individual might use.

All activity on an individual's record, including searches, creates an auditable 'footprint' that provides protections against inappropriate browsing of personal information and could also be used in any investigation into misuse of an electronic credential.

1.6 Programme Authorisation

This programme was authorised in 2012 and started operation in 2013.

Appendix A: Background to Information matching

Information matching involves the comparison of one set of records with another, usually to find records in both sets that belong to the same person. Matching is commonly used to detect fraud in social assistance programmes, or to trace people who owe debts to the Crown, but can also be used ensure people get entitlements as in the case of the unenrolled voters programmes.

Oversight of this activity is important to safeguard individuals and maintain transparency and trust in government. The Privacy Act regulates information matching through controls directed at:

- authorisation – ensuring that only programmes clearly justified in the public interest are approved;
- operation – ensuring that programmes operate within the information matching framework; and
- evaluation – subjecting programmes to periodic review.

Section 106

Section 106 of the Privacy Act requires the Privacy Commissioner to undertake periodic reviews of the operation of each information matching provision and to consider whether:

- the authority conferred by each provision should be continued;
- any amendments to the provision are necessary or desirable.

A periodic review is necessary to assess the ongoing value and suitability of a programme in light of experience operating the programme. A programme may lose effectiveness over time if hit rates have peaked or the wider context has changed.

To conduct these reviews I primarily consider the information matching guidelines set out in section 98 of the Privacy Act. In particular I focus on whether each provision:

- continues to achieve its objective by providing significant monetary benefits or other comparable benefits to society;
- raises concern because of the scale of matching (because of the number of agencies involved, the frequency of matching, or the amount of personal information being disclosed); and
- is operating within the information matching controls in the Privacy Act.