Internal Affairs
Te Tari Taiwhenua

Privacy impact assessment

igovt identity verification service

Full Service Build

April 2013

Introduction

The igovt identity verification service (igovt IVS) is a key enabler of the New Zealand government's Result 10, ensuring New Zealanders can complete their transactions with government easily in a digital environment.

The igovt IVS lets users verify their identity to service providers via the Internet. To use the igovt identity verification service, people apply in person for an igovt ID. This is not an ID card or a piece of paper. It is an electronic credential made up of four key pieces of information: their full name, date of birth, place of birth and gender. An igovt ID is associated with an igovt logon. To use the service a person logs on using their igovt logon and then chooses whether or not to release the information requested to prove their identity.

The igovt IVS initial implementation phase commenced in 2009, with the service being used by Births, Deaths and Marriages for people who want to order birth, death and marriage non-historical records[1] online. Application for an igovt ID is available to those who hold either a current NZ Passport or NZ Citizenship certificate issued after 1 January 2004.

The igovt IVS Full Service Build project was initiated to deliver the full igovt IVS service offering. This includes the expansion of the service to a wider audience and meeting the legislative requirements in the Electronic Identity Verification (EIV) Bill. This Bill passed its second reading in August 2012, and completed the committee of the whole House stage on 13 November 2012. It is now awaiting its third reading.

Scope

The Department of Internal Affairs (DIA) contracted Information Integrity Solutions (IIS) to conduct a Privacy Impact Assessment (PIA) on the full service build of the igovt IVS.

IIS conducted a previous PIA on the igovt IVS initial implementation phase in December 2009[2].

This new PIA covers the enhancements to the igovt IVS brought about by the full service build, which includes use of immigration and birth data and the use of New Zealand Post Limited (NZ Post) for the photograph and document capture stage to ensure the service build is compliant with the Privacy Act.

DIA also asked IIS to conduct an assessment of privacy risks of the extension of the use of igovt services to the private sector through the partnering arrangement with NZ Post, which is a State Owned Enterprise.

The purpose of the PIA is to identify any potential privacy impacts arising from the proposed functionalities. The main deliverable was a comprehensive PIA Report that included the evaluation of the privacy risks and the associated implications of those risks along with mitigation strategies. This document summarises the findings and details each of the recommendations.

Overall conclusions[3]

Overall, IIS considers that the igovt IVS full service build has maintained the design features that seek to address the risks they identified. DIA has maintained its approach of only collecting, using and disclosing personal information about igovt ID applicants and holders that is necessary for the purposes of the igovt IVS and of discarding any information that is no longer necessary to hold.

The main new privacy risks arise from the fact that individuals can use additional Evidence of Identity (EOI) sources on which to base their application for an igovt ID. These sources, which are birth and immigration data, are not as robust as those for current applicants and are not seamlessly integrated within the igovt IVS in the way that passports and citizenship identity

[1] https://www.bdmonline.dia.govt.nz/NonHistoricRecords

[2] http://www.dia.govt.nz/diawebsite.nsf/Files/PIA-IVS-final/$file/PIA-IVS-final.pdf

[3] Substantively as written in the PIA Report

source systems are. The mechanism for establishing uniqueness has also become more complex. This has meant that there is a much greater reliance on back office system manual checking and the need to scan key identity documents into the igovt IVS. It has also meant that specific individual agency identifiers such as a licence number or document number printed on documents are stored permanently in the igovt IVS (as part of the scanned image). Introducing NZ Post into the igovt ID application process has also required some changes that could introduce privacy and security risks.

The privacy risks IIS identified relating to the igovt IVS full service build and made recommendations about include:

- that the storing of scanned documents, which have printed on them non source EOI agency identifiers such as driver licence identifier or building licence number or document numbers, could undermine the principle of keeping agency specific individual identifiers separate from the igovt IVS. It could increase security risks and create additional interest from law enforcement agencies;
- a possible loss of transparency about the way applicants' information is handled due to the increased number of hands through which the information will be passed;
- increased security and privacy risks due to human error or malicious intention arising from the increase in manual handling of applicants' information;
- possible loss of ability for individuals to access information held about them in the igovt IVS, for example, scanned documents;
- possible security risk and loss of applicant control at the point where the applicant attends at a NZ Post office at the photo capture stage;
- the need to ensure reports of igovt IVS operations are restricted to those consistent with the purposes of the igovt IVS;
- the need to ensure that information about igovt ID status (other than revocation) is only given to agencies for purposes consistent with those of the igovt IVS;
- the risk that complaints and inquiry mechanisms are not adequate to meet the more complex arrangements of the igovt IVS full service build.

IIS also identified key issues that could arise in relation to the extension of use of igovt services to the private sector, including the RealMe Service[4] and made a recommendation about this. However IIS notes that DIA will be conducting a separate detailed PIA on RealMe and so it did not make detailed comments and recommendations on this.

In a separate request, incorporated into this PIA, IIS was also asked to consider the privacy issues around the use of the igovt logon service by the private sector Common Web Service Provider and made a recommendation about this.

[4] RealMe® is a new service that expands the existing igovt services and adds new functionality, such as verified address. The service is being built in partnership between DIA and NZ Post. More information is available at www.realme.govt.nz

Recommendations and responses

The following are the recommendations and the actions DIA is taking to address them.

Recommendation 1 – Independent and coherent governance structure for use of igovt services

IIS recommends that as a matter of priority DIA develops a coherent governance structure for managing the evolution of igovt services and their use by public sector, quasi private sector, and private sector organisations. The governance structure should include a mechanism for community and private sector stakeholders to participate in decision making about use of igovt services and the terms and conditions of such use. The roles and functions for the governance structure should include:

- *a person responsible for oversight of end-to-end and big picture privacy issues as igovt services evolve and become accessible to a wider range of users;*
- *development of coherent policies and requirements relating to the management and implementation of privacy for all igovt service users;*
- *oversight of the terms and conditions on which new organisations integrate to ensure that the current high standard of security and privacy requirements are maintained and implemented in a consistent way;*
- *the establishment and implementation of mechanisms to monitor compliance with the policies and requirements by all users of igovt services;*
- *the development and implementation of formal and coherent and accountable processes for managing change and dealing with function creep;*
- *establishing an ongoing mechanism for involving of the community and the private sector in decisions about the evolution of use of igovt services.*

DIA employs a Manager igovt IVS Operations, whose role is to oversee the development and operations of the service, including privacy requirements. Legislation, in the form of the Electronic Identity Verification (EIV) Bill sets out many of the terms under which the service operates.

As part of the commercial contract between DIA and NZ Post a Governance Board and Operating Committee have been set up to manage the Partnering Arrangement, monitor performance and progress, change control procedure and decision-making for referred matters. In addition, a User Forum of organisations integrated with the service meets regularly to enable engagement with the wider user community.

Recommendation 2 – Common Web Service Provider use of igovt logon service

IIS recommends that:

- *the Common Web Service provider is transparent about the fact that it is using the igovt logon service;*
- *where a Common Web Service provider using the igovt logon service also provides other identity related services to DIA, DIA ensures that the service provider has strict access controls in place that prevent any system administrator (or other person) from having a view of more than one of these services; government employees using the Common Web Service and igovt logon service have easy access to one-time-password tokens so that they can have more than one moderate strength logon if they choose to do so; and*
- *as identified strongly in the extension of igovt services to the private sector analysis, there are appropriate governance mechanisms to oversee terms and conditions for use of igovt services and to ensure the privacy impacts of change are assessed.*

The previously identified Common Web Service initiative was intending to use the igovt logon service rather than the igovt IVS. As this initiative to use the igovt logon has not progressed, there are no privacy issues to consider. Should a similar service be established in the future, a privacy impact assessment will be undertaken in relation to the igovt service with which it is intending to integrate.

Recommendation 3 – Technology: Encryption of scanned documents and governance for access

IIS recommends that if scanned documents are to be stored in the igovt IVS they should be stored in encrypted form with very limited access to the encryption keys. There should be strong governance and accountability mechanism for deciding when access to the scanned EOI documents will be allowed. The EIV Bill should be amended to cover access to scanned documents as well as photographs.

Encryption of scanned documents was considered during the initial build and it was established that there were sufficient alternative security measures in place that this capability did not need to be purchased at this time. However, development of another system within the Department will result in the capability becoming available and, if required, could be implemented in the future.

The collection, storage, access to, and retention /destruction of scanned copies of identity documents are regulated by the information privacy principles in the Privacy Act 1993, rather than under the Electronic Identity Verification Act 2012. Therefore, the EIV Act does not need to include a specific provision applying to those documents.

Recommendation 4 – Technology: Reduce reliance on scanned documents

IIS recommends that DIA works with DoL[5] and any other New Zealand agencies that are sources of EOI to develop the technology necessary to reduce the need for EOI and related documents to be stored in the igovt IVS. DIA should also determine when these documents will be no longer needed and a process for deleting them from the igovt IVS at that point.

DIA has designed the igovt IVS application process to guide each applicant to the apply option that relies least on scanned documents, where possible, as this is also the simplest and fastest avenue for the customer. As arrangements for automated checking processes are established over time, the reliance on scanned documents will be reduced.

Regulations will provide that, in general, igovt ID credentials (and all associated information) will be retained for 11 years after it is cancelled or has expired. However, credentials for false identities for undercover police or New Zealand Security Intelligence Service (NZSIS) officers must be deleted 1 month after those credentials are no longer needed. Credentials that are revoked because they were found to be false or fraudulent may be retained indefinitely, or deleted as appropriate. The deletion of the credential includes the deletion of supporting information, which includes scanned documents. These regulations have been set in consultation with the Privacy Commissioner.

Recommendation 5 – Business as usual and technology: Audit and logging

DIA (in conjunction with NZ Post where appropriate) should ensure there is a process for assessing which activities in the full igovt IVS build should be audited and logged. The process should ensure that activities are only logged if there is good reason consistent with the purposes of the igovt IVS full service build.

[5] This refers to Immigration New Zealand, formerly part of the Department of Labour (DoL) now the Ministry of Business, Innovation and Employment.

For the purposes of security and transparency all activity within the igovt IVS service is logged. Access to these logs is restricted to the person on whose account the activity was conducted and the DIA back office roles which provide support to igovt ID holders.

DIA has a Quality Assurance process for determining the auditing requirements of these logs. In this context that process would involve consultation with the Risk and Assurance group of DIA.

Recommendation 6 – Business as usual: Informing Service Users

DIA should engage experts in plain language and online usability to ensure that Service Users are easily able to access and understand the important information about how igovt IVS and NZ Post (and any other participants) will collect, use and disclose information about Service Users. The information Service Users need to know most should be prioritised and made most accessible.

DIA should develop a strategy for publicising changes to privacy policies and corresponding changes to privacy notices as they occur over time.

DIA, through its partnership with NZ Post, as part of the integration of igovt IVS into RealMe® have involved a number of experts including Springload, Clemenger Group Limited and Empathy Limited 2012. DIA has also independently conducted internal usability testing.

Changes to privacy policies and other terms and conditions are notified to all users through the logon screen, one month prior to the change.

Recommendation 7 – Business as usual: Expert advice to assess and manage security risks in manual processing

IIS recommends that once the igovt IVS back office processes are more fully spelled out, DIA engage a security expert at both the development and implementation stage to assess the security risks of the processes and advise on how to minimise these risks.

DIA engaged security experts Axenic to review the igovt IVS to ensure the design supports the system security goals and reviewed logical security requirements and controls for the system. This report is currently being drafted and DIA will respond to any recommendations appropriately.

Recommendation 8 – Accountability: Regular monitoring and audit of back office processes

IIS recommends that once policies and procedures for back office processing are in place, DIA regularly monitors, and conducts audits of, them to ensure that staff comply with them.

DIA has a Quality Assurance process for the monitoring and auditing of back office processes.

Recommendation 9 – Technology: Balance between User access and protection through encryption

IIS recommends that scanned documents and photographs stored in the igovt IVS should be stored in an encrypted form.

See the response to Recommendation 3.

Recommendation 10 – Business as usual: Policies, procedures and training for staff to avoid inaccuracies in data entered into the igovt IVS

IIS recommends that, to minimise inaccuracies in igovt IVS data, DIA and DoL develop detailed policies, procedures and training for igovt IVS back office staff and DoL staff involved in verifying information supplied by igovt ID applicants and other processes involved in the verification and image determination stages of an igovt ID application process.

DIA has developed and documented policies, procedures and training materials for all staff involved in the igovt IVS Full Service. It should be noted that many of the roles carried out in the full service involve leveraging the resources and skill sets that are already in use and proven within DIA and Immigration New Zealand as part of core business. Where the activities are specific to the igovt IVS, training within DIA is provided from a single source, and delivered to Immigration New Zealand as train-the-trainer. On-training of new staff, by people formerly in the role, is not permitted - they are to be referred to the designated trainers.

The Quality Assurance processes that have been developed for monitoring and auditing will also ensure that back office duties are performed consistently. In the future, Facial Recognition software will also be employed to support the image determination stage.

Recommendation 11 – Safety-net: Helping Service Users correct inaccuracies

IIS recommends that DIA provides easily accessible help for individuals seeking to correct their igovt ID using the processes provided for in the EIV Bill. DIA should monitor the incidence of inaccuracy of information held in the igovt IVS in order to identify and address any inaccuracy problems with its or Immigration New Zealand*'s administrative processes relating to the application and issuance of igovt IDs.*

The Helpdesk for the igovt IVS is run by the DIA Contact Centre, enabling it to access expertise and the majority of authoritative data used to create the igovt ID.

The Quality Assurance processes for monitoring and auditing will also ensure that inaccuracies, and any systemic problems leading to them, are addressed. DIA is also required to report on this subject to the Office of the Privacy Commissioner on an annual basis.

Recommendation 12 – Business as usual and technology: Deletion of scanned documents when automated processes available

IIS recommends that DIA develops a schedule for deletion of scanned EOI documents. In addition igovt IVS full service should be designed in a way to make it possible to delete scanned documents in the future should automated means of checking EOI documents become available. This could include offering Service Users the option of undergoing a process that will remove the need to store their scanned EOI documents and enable them to be deleted from the igovt IVS.

See the response to Recommendation 4.

Recommendation 13 – Business as usual: Reporting

IIS recommends that there should be a process for assessing what reports are and are not necessary for ensuring the proper operation of the igovt IVS and flowing from this, rules about what reports relating to the operation of the igovt IVS are, and are not, allowed and in what circumstances. DIA should establish a change and governance procedure to ensure that changes to the types of reports conducted are assessed to ensure they are only generated for purposes consistent with the igovt IVS.

DIA has Quality Assurance processes to determine auditing and reporting requirements and an underlying principle is that no individual identifying information appears in reports. Development of reporting requirements will also involve consultation with the Office of the Privacy Commissioner.

Recommendation 14 – Business as usual: Assess in detail notification of igovt ID status

IIS recommends that DIA develop a guideline which outlines the basis on which it will exercise its discretion under Clause 20(2) of the EIV Bill to provide information about a change in status of an igovt ID to an agency participating in the igovt IVS. The guideline should ensure that DIA only exercises this discretion when it is necessary for a purpose that is directly related to the purposes of the igovt IVS. DIA should consult with the Privacy Commissioner in developing the guideline.

The EIV Bill outlines the circumstances for the setting of various igovt ID statuses and explicitly sets out the notification requirements for 'Revoked' igovt IDs. There is no discretion in the case of a revoked igovt ID – it must be notified to all agencies with whom the igovt ID was used. Notifications requiring discretion under Clause 20(2) are expected to be rare and will require case by case consideration. If similarities are found to exist, then the Quality Assurance process will develop the appropriate policies and procedures in consultation with the Office of the Privacy Commissioner.

Recommendation 15 – Safety-net: Review of inquiries and complaints handling processes

IIS recommends that DIA reviews its inquiries and complaints handling processes to assess whether they are sufficiently coordinated and responsive to handle the increase in number and complexity of inquiries and complaints that will occur with the igovt IVS full service build and the addition of NZ Post as a partner. DIA should ensure that it discusses in detail the processes to be followed by NZ Post to ensure that the increase in integration at the process and the technology level is accompanied by a smooth, one-stop-shop integration at the human and customer service level. DIA should ensure it collects data about complaints processes (internally and from Users) and regularly reviews it for continuous improvement in its processes.

The Helpdesk for the igovt IVS is run by the DIA Contact Centre, enabling it to control resource levels to meet demand and to have access to the skill-sets required for complex queries.

Integration with the igovt IVS service through RealMe is a joint exercise with NZ Post and DIA with well-documented processes and overarching governance. The Quality Assurance processes for monitoring and auditing will also ensure that issues are effectively addressed. This includes the existence of registers for recording complaints and a requirement to report annually to the Office of the Privacy Commissioner.

Further information

For further information regarding this assessment contact the Department of Internal Affairs at igovt@dia.govt.nz