Regulatory Impact Statement

Electronic Identity Verification Bill

Agency disclosure statement

This Regulatory Impact Statement has been prepared by the Department of Internal Affairs.

An all-of-government shared service – the Electronic Identity Verification Service (IVS) – is designed to provide individuals with the option of verifying their identities authoritatively online and in real-time to participating agencies.

The IVS was implemented in December 2009 with a limited scope and without specific governing legislation. It is important that a significant government service such as this be authorised by specific legislation and, since its inception, it has been clear that legislation would be required to ensure the service is able to suit the online identity verification purposes of the widest appropriate range of government services. The legislation will be future-proofed, to enable the use of the service by the private sector, if it is decided to extend its use in this way.

The enactment of the legislation will preserve the ongoing integrity of the service and will maximise the efficiencies that are expected from its full implementation and use, both for the government and for the public. This is a classic instance of regulation providing certainty for the provision and operation of a government service, therefore maximising the benefits that are expected to result both for the public and for government.

None of the options considered will impose additional costs on business, impair private property rights, restrict market competition, reduce the incentives on business to innovate and invest, or be likely to override fundamental common law principles. The preferred option will reduce compliance costs on individuals who choose to use the service, and the costs for agencies that are authorised to join with the service.

8 / 2 / 2011

Carolyn Risk, Chair, Regulatory Impact Analysis Panel
Department of Internal Affairs

Status quo and problem definition

To date, agencies offering services that require identification of the customer have often been faced with the need for the customer to attend at an office in person to prove his or her identity, or for customers to send valuable evidence of identity documents through the post or by courier, in support of their applications. While requirements vary from agency to agency, the presentation and processing of multiple

documents is often necessary. Over the course of each year, individuals are likely to have to visit or deal with several agencies to undertake various transactions which require their identities to be verified. Complying with the evidence of identity requirements for these transactions adds cost, travel and transaction time and inconvenience for customers, and processing costs for agencies. Detecting and acting upon fraudulent applications and other criminal activity committed through the use of false, lost or stolen identity documents can impose costs and additional requirements on agencies and the individuals whose identity information has wrongly been used.

The Internet is transforming service delivery for governments and businesses around the globe. Since the widespread uptake of the Internet in the 1990s, a large amount of government investment in New Zealand has been directed towards making government information and services available online. However, the Internet was built without a way to identify with confidence the parties transacting online. While not every type of online transaction requires identity verification, the potential future demand for a way to verify an Internet-user's identity could be significant. For example, government agencies cannot provide services that involve the payment out of money or exchange of personal information unless they have verified the applicant's identity. Internet technologies offer the benefits of lower transactional costs, but these cannot sensibly be realised without appropriate online security and safeguards.

The growing importance of the online channel

The Internet and its use as a service delivery channel are continuing to grow in importance. Statistics New Zealand reports that, in the 12 months to the end of December 2009, approximately 2.68 million New Zealanders used the Internet (up from 2.2 million as at the end of 2006). Over 1.4 million people made an online purchase (up from 915,000 in 2006), with those aged 25 to 44 years being the most likely to do so. Of the total number of Internet users in 2009:

- 46% had sought information about government agencies;
- 35% had downloaded or completed a government form online; and
- 20% had made payments to government online.

Source: Statistics New Zealand, April 2010, *Household Use of Information and Communications Technologies: 2009*. Excel file, tables 6, 7 and 8, accessible at: http://www.stats.govt.nz/~/media/Statistics/Browse%20for%20stats/HouseholdUseofICT/HOTP2009/huict-2009-tables.ashx

Similar findings from the AUT World Internet Project New Zealand 2009 report indicate that 83% of New Zealanders use the Internet and, in their interactions with government:

- 59% seek information; and;
- 30% use government services.

Source: Smith, P., Smith, N., Sherman, K., Goodwin, I., Crothers, C., Billot, J., Bell, A. (2010). *The Internet in New Zealand 2009*. Auckland: Institute of Culture, Discourse and Communication, AUT University, accessible at: www.wipnz.aut.ac.nz.

The development of a shared identity verification capability for the New Zealand government was initiated in light of the problem that, globally, governments and businesses have been constrained in their ability to offer online services that require an individual's identity to be verified, with there being no consensus about any single

solution that is workable across cultures and sectors. Significant investments have been made to build secure online environments where personal and business transactions can be relied on.

Since the early 2000s, it has been recognised that there would be inefficiencies and inconsistencies if New Zealand government agencies each developed or invested in their own identity verification systems, and inconsistent identity verification processes would proliferate. As a result, access to online government services would become more complex, and expose government services to a higher risk of security and privacy breaches. In addition, multiple identity verification systems would inconvenience the public, as individuals would, for example, be required to remember multiple usernames and passwords. Some services delivered by smaller agencies would never be able to be delivered over the Internet securely and economically because of the costs of doing so. In essence, the New Zealand government would face duplicated costs of ownership, unnecessarily high transactional costs, and inconsistent or inadequate levels of protection for individuals against fraudulent online transactions committed by people using the identity information of another person.

The Electronic Identity Verification Service (IVS)[1] was developed as an all-of-government shared service to provide members of the public with the option of proving their identity to New Zealand government agencies via the Internet, when used in conjunction with the igovt logon service. Cabinet directions are in place to control the investment or building of separate online identity establishment and verification capability by public service departments, the New Zealand Police, the New Zealand Defence Force, the Parliamentary Counsel Office, the New Zealand Security Intelligence Service, the Office of the Clerk, the Parliamentary Service, and all Crown agents.[2]

Significant whole-of-government benefits have been estimated in successive business cases for the IVS. Agencies that are authorised to integrate their online services with the IVS are expected to receive direct and indirect financial benefits through the avoidance of duplicated infrastructure investment and reduction in transaction, customer support and administration costs. Individuals who choose to use the service, where required for online transactions offered by authorised agencies, are expected to benefit through potential reductions in compliance costs, travel time, transaction time, and risks associated with identity crime/fraud. In 2011, the tangible benefits were estimated, over a ten year period, to be between $385 million and $527 million. Should private sector organisations also be authorised to use the IVS (as the law

[1] The current brand name for the service is the "igovt identity verification service" (or "igovt IVS"). However, for the purpose of this analysis, the name "Electronic Identity Verification Service" (or "IVS") is used, to reflect the way in which the service is expected to be described in law. Similarly, references to "electronic identity credentials" in this analysis correspond to "igovt IDs" as they are known in practice.

[2] CAB Min (08) 38/2A and Whole of Government direction given by the Minister of State Services and Minister of Finance under section 107 of the Crown Entities Act 2004, dated 21 July 2008 – *New Zealand Gazette* Notice No 6913, published 18 September 2008. In addition, Public Service and State Services chief executives are expected to use cross-government ICT products and services (such as the igovt services) to meet relevant business needs where they are available, unless there is a compelling business reason not to, and to work with the agencies providing these products to ensure they meet business purposes (*Directions and Priorities for Government ICT,* CAB Min (10) 35/5A, adopted by Cabinet in October 2010 as government policy to direct the ICT activities of State Services agencies).

would allow), those organisations would be likely to experience the same types of benefits through the use of the IVS. The estimates of the benefits associated with the service continue to be reviewed by DIA as costs and savings are further quantified and refined, and in light of changing operational requirements.[3]

The IVS was implemented in December 2009 with one agency, but its use is currently limited to a small community of users. The service is currently available for people who have had their identity verified to a high level of confidence, such as those who have been issued with a New Zealand passport or granted New Zealand citizenship since 2004. Those people are able to make online requests to DIA's Births, Deaths and Marriages registry for certificates and other products for which evidence of identity is required by law.

However, the full implementation and widespread use of the IVS, as originally envisaged, has been constrained in part by a lack of an authoritative policy framework and, in particular, the legislative authority to perform certain functions that would support the IVS's planned full implementation (such as using information matching programmes to support the issue of electronic identity credentials).

Objectives

The scope of this policy initiative is to regulate the ongoing administration and application of the IVS through an appropriate legislative framework that will:

- engender acceptance and trust by the public and agencies using the IVS, and confidence in the fair and equitable application of the service;
- set clear parameters for the IVS and ensure that any changes to the service over time are made in a transparent way that does not undermine public confidence in it;
- provide adequate penalties to deter and punish abuse of the IVS and systems on which the IVS relies;
- ensure compliance with the Privacy Act 1993 and other legislation, especially in relation to the collection, use, and disclosure of personal information;
- allow the IVS to be used for the widest possible range of government services, and also potentially for services provided by the private sector;
- provide an all-of-government approach which is fit for its purpose, enduring, secure, protective of privacy, generally acceptable to potential users, optional for people to use, affordable, reliable, integrates with a range of technology options, and which ensures legal compliance, legal certainty, and non-repudiation, and provides functional equivalence between online and offline transactions.

[3] It is also noted that not all agencies currently provide services requiring identity verification. Projected uptake levels for the IVS used in business cases are, to some extent, based on assumptions about the future creation of online services that will require identity verification processes, and the pace at which agencies will move towards Internet-based service delivery to make cost reductions and to meet an increasing expectation by the public that services will be provided online.

Regulatory impact analysis

Non-regulatory options

As set out above, the IVS was implemented in December 2009 without specific supporting legislation. Since then, it has been operating on a contractual basis with members of the public for use with one participating agency. Decisions that affect the parameters and features of the service are made administratively. However, this is not the preferred option for the ongoing administration of the service. It is important that a significant government service such as this be authorised by legislation. Further:

- there is a risk that, without the proposed legislation, the IVS would, over time, be used for purposes other than those for which it was established;
- there is a risk that existing criminal and civil penalties may not be sufficient to deter abuse of the IVS (both by members of the public and by the administrators of the service);
- there are impediments to administering the service on a contractual basis, for example in respect of holders of electronic identity credentials who are children (as contracts with children are generally unenforceable under the Minors' Contracts Act 1969);
- there is a risk of inconsistencies arising between agencies' interpretation of how existing legislative provisions apply to the IVS, leading to uncertainty about the operation of the service;
- in the absence of authorised information matching programmes, the ability to check information supplied by an applicant to the IVS against other agencies' databases is constrained, especially in respect of the death register. This creates risks that the application process could be exploited by fraudsters using other people's identity information (particularly that of deceased people) to conduct online transactions for fraudulent or other criminal purposes; and
- if the IVS continued to be offered only on a contractual basis, piecemeal legislative change would be required to ensure it could be used for the widest possible range of government services.

Alternative regulatory option

As noted above, the alternative, non-preferred, option would involve attempting to make piecemeal legislative changes to support and expand the IVS's contract-based operation. This would be a weak, impractical, and only partial solution.

Separate legislative changes, for example, to establish authorised information matching programmes and to modify agency-specific legislation as various agencies integrate with the IVS would result in fragmented and inconsistent implementation of the service and cause public confusion about the service. There would be significant delays to integrate the IVS with those agencies that relied on specific legislative change, and this approach would be an inefficient use of public resources, including the House of Representatives' time. Extending the use of the IVS for online services offered by private sector organisations would be complex and fraught with risk, due to the challenge of enabling those organisations to use the service to meet their business needs, while maintaining sufficient controls and safeguards against misuse of the service.

In the absence of such controls, it is highly likely that public trust in the service would be lost, resulting in individuals choosing not to use the service. Without the certainty provided by having a coherent legislative framework governing the IVS, it is also likely that agencies would be reluctant to link their online services to the IVS.

Preferred regulatory option

The preferred option is to establish a legislative framework circumscribing the IVS's purpose, boundaries and other key parameters. The framework would:

- specify who may apply to join the service, and which agencies may make use of the service to verify individuals' identity;
- regulate the administration of the service, and allow fees to be prescribed to recover the costs of the service, with the ability for a fees framework to distribute the recovery of costs from members of the public and participating agencies;
- allow for the checking of an individual's entitlement, or continuing entitlement, to belong to the service through authorised information matching programmes, checks to confirm that an individual's identity information is consistent with information held on other appropriate agencies' records, and other processes;
- govern access to IVS-related information;
- prescribe relevant offences and penalties to deter abuse of the service; and
- consequentially amend existing statutory identity verification provisions (where necessary), to ensure the service can be used for the widest range of services possible.

It is expected that this approach would provide assurance to government and the public about the nature of the service. An appropriate legislative framework would allow flexibility for the IVS to be developed and modified to respond to changing technological and social conditions, without exceeding the key parameters. This approach would minimise compliance costs associated with frequent legislative change.

Consultation

Government: Consultation on the proposed legislative framework to support the IVS was undertaken by the Department of Internal Affairs with: the State Services Commission, The Treasury, Ministries of Agriculture and Forestry, Consumer Affairs, Culture and Heritage, Defence, Economic Development, Education, Health, Justice, Social Development, and Transport, Te Puni Kōkiri, the Departments of Building and Housing, Corrections, and Labour, Archives New Zealand, Inland Revenue Department, Land Information New Zealand, New Zealand Transport Agency, National Library of New Zealand, New Zealand Customs Service, New Zealand Police, New Zealand Security Intelligence Service, Accident Compensation Corporation, Aviation Security Service, Civil Aviation Authority, the Office of the Privacy Commissioner, and the Office of the Ombudsmen. The Department of the

Prime Minister and Cabinet was consulted on specific aspects, and will continue to be kept informed.[4]

Public: Members of the public will have the opportunity to make submissions on the Bill during the select committee process. This follows extensive public consultation about the development of the IVS.

In February and March 2003, public consultation was undertaken on the draft conceptual model for the (then) proposed All-of-government Authentication Programme. Public opinion on the draft Authentication Standards was sought between December 2005 and February 2006. Public consultation on more detailed aspects of the proposed IVS was undertaken over a five week period in November and early December 2007, through group discussions or by making an online or paper-based submission. Responses were generally favourable, supporting the introduction of the proposed service and indicating that a wide variety of people would be likely to use the service.

A key message expressed by participants in this process was that legislation is required to preserve the key parameters of the IVS, including the ability to opt in or out of the service, and requiring the individual's consent for information to be passed to agencies and other privacy protections. Participants also said that the IVS should be reviewed regularly to ensure it was operating within those parameters. This was considered especially important if the use of the IVS is to be extended to the private sector, to ensure that commercial organisations do not exploit identity information. It was considered that, without legislation, subsequent governments could too easily change the nature and boundaries of the service, leading for example to it becoming compulsory or it being used for surveillance purposes. A legislative framework was considered important to engender public acceptance of the IVS, and confidence in the fair and equitable application of the service.

The policy content of the Bill was developed in line with the results of that consultation, and requirements have been refined in light of the Department's and the public's use of the IVS since December 2009.

Private sector: Private sector organisations will also have the opportunity to make submissions on the Bill during the select committee process, and have also been involved in discussions about the IVS's operation to date.

During 2010, the Department held discussions with interested private sector organisations about their potential use of the igovt services (the IVS and the igovt logon service). Information provided by 13 medium to large-sized private sector organisations (particularly within the financial services sector) suggested a high degree of interest in integrating with the IVS once supporting legislation for it was in place.

Conclusions and recommendations

Enabling the IVS to be used by any member of the public, and for the widest possible range of online services, cannot be achieved without legislative change. Even if it

[4] A number of these agencies have also been engaged, over the course of several years, in discussions and decisions about funding the IVS and other parts of the Identity Common Capability Programme, of which the IVS is part.

could, the ongoing operation of the IVS "has substantial implications for the workings of representative government and for the public's participation and interaction with government".[5] It should, therefore, be subject to the scrutiny and transparency provided by the legislative process. Continuing to operate the service on a contractual basis, as it has been since December 2009, has a number of significant risks, and limits its use to a small section of the public.

Regulating the administration of the IVS through legislation would mean that its boundaries (including its opt-in nature) could not arbitrarily be changed, and ensures there is clear authority for controls to be exercised to protect the service from abuse. It is, therefore, necessary and important that a significant government service such as this be authorised by specific legislation.

Implementation

As noted above, since December 2009 the IVS has been used on a contractual basis with certain eligible individuals, specifically people who have received a New Zealand passport, been granted New Zealand citizenship or been registered as a New Zealand citizen by descent since 2004. Once granted an electronic identity credential, those individuals have been able to order certificates and printouts from non-historical records held by the Births, Deaths and Marriages registry within the Department of Internal Affairs.

The Bill, once enacted, will enable the service to be made available to the general public and be used for transactions with a wider range of organisations. At this stage, it is intended that the legislative framework would be brought into force in 2012. To ensure a smooth and coordinated transition from the limited service phase, it is intended that the substantive provisions of the Act would be brought into force by way of Order in Council. Transitional provisions will specify that those individuals who have been using the limited service, and any applications lodged but not completed before the Act's commencement, will be subject to the Act's provisions.

Information about the function and development of the IVS will continue to be available through a dedicated website, www.i.govt.nz, as well as more generally through the DIA's website. The DIA provides information about the application process and terms of conditions of the IVS, and this information will be expanded to reflect the requirements of the governing legislation, once enacted. Information about the IVS will also continue to be made available to the public through other media, including in connection with authorised agencies' online services that will be connected with the IVS.

Monitoring, evaluation and review

Regular privacy impact assessments have been undertaken during the IVS's development. Security reviews, including reviews by external security experts, have been undertaken during the IVS's development and continue to occur as part of usual business operations. Regular auditing of the IVS by the DIA is also occurring.

[5] Comment by the Privacy Commissioner, in letter dated 6 April 2006 to Deputy Commissioner Information, Communications and Technology, State Services Commission.

Under the legislative framework, the chief executive of the DIA will be responsible for setting standards and specifications with which agencies will need to comply in respect of their use of electronic identity credentials. The chief executive may require agencies to report on their use of electronic identity credentials, and may suspend IVS use by agencies that fail to comply with the relevant standards and specifications. Agencies' use of the service will be authorised by regulations made under the legislation.

It is proposed that the Privacy Commissioner would have a general independent oversight role for the IVS, and would be able to require the chief executive of DIA to provide reports, from time to time on the IVS's operations, so that any privacy issues are proactively monitored. This would help to guard against 'function creep' – that is, to ensure electronic identity credentials do not, over time, become de facto universal identity cards. The Privacy Commissioner would also be consulted about establishing information matching programmes, and arrangements with public sector and private sector agencies for confirming that an individual's identity information is consistent with information held on those agencies' records. The operation of the IVS would also be subject to complaints to the Privacy Commissioner, review by the Ombudsmen and judicial review.

These measures support the attainment of the IVS's public policy objectives, particularly those relating to security and privacy. Ultimately, the number of individuals and agencies joining, using, and withdrawing from the service will also inform whether the service is meeting its objectives.

The ongoing administration of the Act will also be subject to regular review by the DIA.