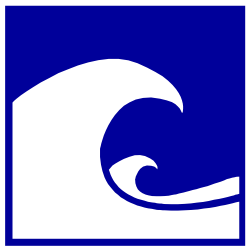


PACIFIC PRIVACY CONSULTING

AUTHENTICATION FOR E-GOVERNMENT

Privacy Impact Assessment Report

December 2003

AUTHENTICATION FOR E-GOVERNMENT

Privacy Impact Assessment Report

by
Pacific Privacy Consulting
in association with
Xamax Consultancy

for
E-government Unit
State Services Commission
New Zealand

December 2003

Nigel Waters, Pacific Privacy Consulting
Consultants in Privacy and Fair Information Practices
12A Kelvin Grove, Nelson Bay, NSW, 2315, Australia
Telephone: (02) 4981 0828. Fax: (02) 4981 0995 Mobile 0407 230342
E-mail: nigelwaters@iprimus.com.au

Roger Clarke, Xamax Consultancy
E-mail: Roger.Clarke@xamax.com.au

Executive Summary

This Privacy Impact Assessment analyses the privacy implications of the proposed all-of-government identity authentication scheme. It looks at compliance with the Privacy Act 1993, but also at wider privacy issues and concerns.

A fairly detailed description of the proposed authentication system (Section 2) has been included in order that readers new to the project can understand the analysis which follows. Readers who are already familiar with the project may wish to go straight to the Analysis (Section 3), or even the Findings and Conclusions (Section 4), and then refer back if necessary.

The relatively early stage of the authentication project at which the assessment has been carried out has both advantages and disadvantages. It allows the assessment to perform its function of potentially influencing both the design and the business case. But because the design is not yet fully developed or stable, it also means that the analysis is to some extent speculative, and must necessarily anticipate 'worst case' privacy implications. It is desirable that further privacy analysis be undertaken as the project develops.

The government's approach to authentication has from the start recognised the importance of privacy and related security issues. The scheme design has attempted to minimise adverse privacy consequences and some of the design features will be privacy enhancing if they can be maintained.

The proposed scheme should be able to operate consistently with the Privacy Act 1993, but this is largely because that law will defer to the more specific authorising legislation that it is assumed will provide the basis for the scheme. While the Privacy Act will require some specific design features and safeguards, compliance with the Privacy Act will not in itself deal with the more significant privacy issues that the scheme raises.

The scheme unavoidably lays the foundation for a national population register. Although it is not currently intended to develop such a register, experience suggests that there will inevitably be increasing pressure for a widening of both the scope and the functions of the scheme.

Some of the design features already test the limits of the constraints placed on the project at the outset to satisfy privacy concerns – including the voluntary 'opt-in' principle; limited information exchange, a minimal role for biometrics and the commitment to no identity card.

Whether public concerns about the privacy impact of the scheme and about the potential for future scope- and function-creep can be managed depends partly on how deeply safeguards and limits are embedded in the scheme. Most of the recommendations in this Report are directed to this end.

Other recommendations suggest a clearer articulation of the need for the scheme (Recommendation 1); and review of the scheme design in relation to multiple Credentials (Recommendation 2); confirmation of identity rather than release of names (Recommendation 3); authentication of roles (Recommendation 4), and the use of the photograph and biometric (Recommendations 8 and 10).

The stated primary purpose of the proposal is to enable individuals to verify their identity for the purposes of accessing government services electronically. One consequence of a central authentication scheme is to raise the stakes in the battle against identity fraud and theft. If successful, it will reduce the incidence of those crimes and enhance one aspect of individuals' privacy, albeit to the detriment of other aspects. However, failures or errors will potentially compound the problem, leading to even more serious consequences for individuals and losses to organisations.

If the scheme is implemented, it is essential that all the possible points of failure be identified in advance and contingency plans be made to deal with them. This must include a strong independent review body with the jurisdiction and powers to provide individuals with real remedies.

Recommendations

Note: This list is drawn from the recommendations which are interspersed in the body of the report. Paragraph numbers in brackets are those of the location of the recommendation (following the paragraphs cited).

Note: reference to 'authorising legislation' is deliberate, on the assumption that there will be a specific Act of Parliament providing for all the key ingredients for the authentication scheme. Where 'legislation' is used instead, the recommendation is neutral as to whether it is in the authorizing, or other, legislation.

Recommendation 1. A clear articulation of the justification for the scheme, and a quantified analysis of the underlying problems it addresses, are necessary in order that the business case for the scheme can be assessed alongside the privacy impact. (3.16)

Recommendation 2. The conceptual basis of the scheme should be revisited with a view to allowing for registration of multiple identities, linked only where necessary and justified. (3.24)

Recommendation 3. Consideration should be given to varying the design so as to allow simple confirmation of the validity of a client name, rather than only release of all registered alternate names. (3.33)

Recommendation 4. There should be further analysis of the demand for authentication of roles as opposed to individuals. (3.54)

Recommendation 5. The authorising legislation should require that service agencies expressly justify any requirement for clients to authorise release of all alternate names. (3.58)

Recommendation 6. Publicity for the scheme should clearly outline the option of multiple keys and explain the privacy advantages. (3.59)

Recommendation 7. The authorising legislation should prohibit the production of cards or documents containing both Credential confirmation numbers or Key Serial Numbers and any ID data. (3.63)

Recommendation 8. Further consideration should be given to the overall costs and benefits of retaining the biometric template and/or the photographic image itself. (3.70)

Recommendation 9. The authorising legislation should expressly limit the purposes for which the photograph, digital image or biometric of the image can be used. (3.72)

Recommendation 10. Before any further commitment is made to the scheme, a detailed analysis of the role of the photo/biometric should be carried out, addressing the reasonable doubts about the accuracy and reliability of face recognition technology and the practical difficulties that will arise. (3.75)

Recommendation 11. There should be a clear commitment that the scheme will not develop to involve any other biometric without separate legislative authorisation following a full privacy impact assessment. (3.76)

Recommendation 12. The authorising legislation should clearly specify limits on the scope of the authentication scheme. (3.78)

Recommendation 13. The authorising legislation should reserve the Credential serial number for use only by the Authentication Agency for internal administrative purposes. (3.80)

Recommendation 14. The authorising legislation should proscribe the use of any Credential confirmation notice or administrative reference number issued by the Authentication Agency by other organisations as an identifier. (3.82)

Recommendation 15. Before any further commitment is made to the scheme, analysis of all the possible points of failure, and how they will be addressed, should be carried out. (3.86)

Recommendation 16. The authorising legislation should clearly establish the Authentication Agency as an independent function with appropriate status, structure and accountability. (3.92)

Recommendation 17. Further privacy impact assessment should be undertaken once the details of the proposed funding model are clear, and design work has progressed. (3.94)

Recommendation 18. Public presentation of the scheme needs to be careful in explaining the issue of compliance with privacy laws, and what this means. (3.103)

Recommendation 19. Legislation should clarify the application of the Unique Identifier Principle (UIP – Principle 12) of the Privacy Act to the various identifiers and numbers involved in the scheme. Existing issues about the application of the UIP should be resolved at the same time, after consultation with the Privacy Commissioner. (3.132)

Recommendation 20. Consideration should be given to varying the design such that the use of the same Key with different agencies would result in the issue of a different Key Serial Number. (3.151)

Recommendation 21. A comprehensive and continuing security review and risk assessment should be undertaken to address the many security issues as yet unresolved. (3.158)

Recommendation 22. Legislation should amend the Privacy Act to grant all Credential Holders, wherever they are located, the same rights under that Act. (3.159)

Recommendation 23. Legislation should specify any additional grounds for withholding Authentication Agency information in response to access requests needed

to ensure adequate security, and to protect the privacy interests of third parties. (3.161)

Recommendation 24. The authorising legislation should set the parameters for retention of various categories of data held in connection with the scheme. (3.173)

Recommendation 25. The authorising legislation should set out a detailed regime for use and disclosure of personal information held in connection with the scheme, dealing with:

- The distinction between use and disclosure in this context.
- Limits on who can access information, for what purposes, in what circumstances and subject to what conditions.
- Specific limits and conditions in relation to different categories of data, such as registration information, transaction information, and revocation/suspension data.
- A distinction between uses and disclosures directly associated with the operation of the scheme (including investigation of suspected ID fraud or theft) and those for other secondary purposes unrelated to the scheme. (3.188)

Recommendation 26. The authorising legislation should clearly prescribe relevant information exchanges as 'authorised information matching programmes' for the purposes of the Privacy Act, Part 10. It may also be desirable to impose additional controls on some of the information exchanges involved, and to expressly prohibit certain other exchanges. The Privacy Commissioner should be consulted about the appropriate level of control. (3.199)

Recommendation 27. An express decision should be made as to the extent to which outsourcing of any information handling involved in the scheme will be allowed. Legislation should ensure that individuals' rights and accountability are not lost or compromised as a result of any such outsourcing. (3.205)

Recommendation 28. Apart from the specific recommendations outlined in this section, agencies involved in the scheme will need to ensure that they comply with the Information Privacy Principles (or equivalent rules under Codes of Practice), taking account of the issues raised above under each Principle. (3.208)

Recommendation 29. Agencies involved in the scheme must be required to have appropriate internal complaint handling; dispute resolution and internal audit processes, and to enter into protocols with other parties to ensure complaints do not fall between gaps. (3.210)

Recommendation 30. Authorising legislation should ensure that an independent review body has the necessary powers to provide coverage of all participants in the authentication scheme, and to perform both complaint adjudication and proactive monitoring roles. (3.223)

Recommendation 31. The authorising legislation should provide for appropriate criminal offences and penalties over and above the civil penalty regime under the Privacy Act. (3.225)

Recommendation 32. The authorising legislation should provide for a continuing staff training and education function, to extend to training of all participants in the authentication scheme. (3.226)

Recommendation 33. There should be clearly defined responsibility for a public communications strategy, to include publication of the justification for and merits of the scheme, its design specifications and this Privacy Impact Assessment, before a final decision is made to proceed, and continuing public education programme during implementation and operation. (3.229)

Recommendation 34. The authorising legislation should provide for ongoing independent monitoring and for periodic independent review of the scheme, and for a clear consultation and public decision-making process for any subsequent significant changes. (3.233)

Recommendation 35. If the centralised model is pursued, the statutory framework should cover the following (this list picks up and expands on the specific recommendations already made):

- Authentication Agency functions – preferably not including the technical standard setting for acceptable Keys, or the provision of the technical infrastructure of a common login site, which should be undertaken separately.
- Authentication Agency Registrar & staff – independence, accountability, reporting, resources.
- Liability – clear allocation of responsibility between agencies (including AA, SAs, Organisational TRs and KPs), and clear specification of liability of individual Trusted Referees and Credential Holders.
- Trusted Referees – criteria, functions (and liability)
- Key Providers – criteria for participation, role, conditions (eg: required infrastructure, security etc).
- Unique Identifiers – clarification of the effect of the UI principle in the Privacy Act, and specification of appropriate controls on the use of the Credential, ID data, Key Serial Numbers and other identifiers involved in the scheme.
- Information Matching – designation of information exchanges involved in the scheme as authorised information matching programmes for the purposes of the Privacy Act.
- Criminal penalties – specification of criminal offences as a deterrent against abuse of the authentication system and of appropriate penalties
- Limited data – specification of what data items can be collected and stored in the central database
- Access, Use & Disclosure limits – specification of which agencies can obtain what data for what purposes, including where appropriate limits on the existing powers of other agencies.
- Data retention – specification of periods of retention for data collected for both registration and transactions, balancing operational requirements with privacy
- Auditing of all participants – by appropriate independent auditors at all relevant stages and processes
- Review Body – location, powers and resources. (4.20)

AUTHENTICATION FOR E-GOVERNMENT

Privacy Impact Assessment Report

CONTENTS

Introduction

Privacy Impact Assessment

1.0 A Privacy Impact Assessment seeks to systematically appraise the privacy implications of a new proposal or existing system. The technique of privacy impact assessment (PIA) is relatively new but has quickly become established as a valuable tool, drawing on the experience of environmental impact assessment.

1.1 The Office of the New Zealand Privacy Commissioner has been a pioneer in the use of PIAs[1], and in October 2002 published a Handbook, giving guidance on the use of the technique[2].

1.2 PIAs are now a legal requirement for US federal agencies[3] and in several Canadian jurisdictions[4], and are recommended by most Privacy or Data Protection Commissioners, and by government central agencies, including the UK Cabinet Office[5].

1.3 Reflecting government recognition of privacy as a key issue in relation to any authentication initiative, the E-government Unit (EGU) of the State Services Commission (SSC) carried out a preliminary Privacy Impact Assessment, in-house, and published a report in March 2003.[6]

1.4 In July, the EGU invited tenders for an external Privacy Impact Assessment. The terms of reference required a PIA prepared in conformity with the OPC Handbook, together with privacy analysis support to the Project Team

1.5 A contract was awarded in August to Pacific Privacy Consulting, with Xamax Consultancy as a sub-contractor. A brief profile of the consultants is at Appendix 1.

1.6 Work commenced in early September with a round of face-to-face meetings, and a partial draft PIA was circulated to the Project Reference Group, Steering Committee and Office of the Privacy Commissioner in October. Further meetings in November led to a revised full draft, submitted on 26 November. After receiving feedback and making further changes, this final report was submitted on [8 December].

---

[1] OPC has documented 12 PIAs since 1997, including PIAs of the photo driver licence proposal, insurance claims register and Health Intranet, and Justice Data Warehouse – Paper for PIA Workshop, Auckland, September 2003.
[2] OPC 2002 Privacy Impact Assessment Handbook
[3] US E-Government Act 2002, Public Law No: 107-347.
[4] Particularly Alberta and Ontario and, more recently the federal government. More PIAs have been carried out in Canada than anywhere else, but examples are also documented in Australia, Hong Kong and the USA as well as in New Zealand. (Auckland Workshop paper)
[5] Cabinet Office, 2002, Privacy and Data-sharing: The way forward for public services.
[6] http://www.e-government.govt.nz/docs/authent-pia-prelim/index.html

Project history

1.7 In April 2002 the government agreed to a two-stage approach to develop electronic authentication of people who undertake online transactions with the New Zealand government.

1.8 The E-government Unit of the State Services Commission (SSC) developed a conceptual model and identified a number of options, which were opened to public consultation in early 2003.

1.9 In June 2003, the government agreed to an all-of-government approach with centralised authentication functions and limited information exchange. Funding was provided for design and scoping work, and for the preparation of a business case, to be reported in early 2004 for a decision on implementation, legislation and funding.[7]

1.10 The government noted that the public consultation on the options indicated a preference for a model that gives precedence to security and privacy. Reflecting this, there is a Privacy Protection Policy Principle:

- Ensuring that the proposed approach protects privacy appropriately;

and two particularly relevant Design Assumptions:

- The public should be able to choose whether or not to access services that require authentication over the Internet (the 'opt-in' policy principle).
- The all-of-government model does *not* require national ID cards, digital certificates or the exchange of biometric data at the time of transaction (consistent with authentication principles such as technology neutral, affordability and acceptability)[8]

Project justification

1.11 Improved (consistent) authentication for on-line transactions is seen as a key enabler for e-government. E-government is all about government agencies working together to use technology so that they can better provide individuals and businesses with government services and information[9].

1.12 E-government initiatives are set in the context of 71% of New Zealanders having used the Internet within the last month, and 40% having used e-government services in the last year[10].

1.13 However, another survey has showed that only 31% of New Zealanders feel it is safe to provide personal information to government over the Internet[11].

---

[7] SSC, Design of online authentication for government: summary of recommended approach, July 2003
[8] Policy Principle and Design Assumptions from the Blueprint, July 2003
[9] FAQs about e-government, at http://www.e-government.govt.nz/programme/faqs.asp#a1 (accessed 20 October)
[10] GO 2002 International Survey, Taylor Nelson Sofres. 1000 New Zealanders interviewed in October 2002. The 71% finding was the highest in any of the 31 countries surveyed. Some agencies questioned the accuracy of these findings during consultations.
[11] GO 2002 International Survey

1.14 There are two broad categories of risk which authentication systems seek to address. These are:

- risks associated with malicious use of erroneous identities (encompassing identity fraud and identity theft), and
- risks associated with mistaken use or non-use of identities (encompassing both erroneous matches, and inability to match, both of which can lead either to unwarranted duplication of services, failure to deliver appropriate services, or direct privacy breaches through the provision of personal information to the wrong person).

1.15 The incidence and scale of both types of risk are notoriously hard to measure, and justifications for actions to address them are often based on assertions rather than quantifiable evidence. These issues are considered further in the privacy analysis.

1.16 The EGU has undertaken background work on trust levels required by government agencies for on-line transactions. The Business Case for the Authentication project summarised findings from a review of government on-line services in July 2002. 58% of services did not require users to identify themselves, 22% required identification but not verification, and 11% both identification and verification. (The balance of 9% were assessed as allowing pseudonymous use)[12].

1.17 The services requiring authentication (identification and/or verification) included both high volume transactions such as student loan applications and payment of child support, and more specialised low volume transactions such as certain licence applications.

1.18 It is important to recognise that no identification or authentication system for an entire population can be 100% perfect. Professionals in the field, including those responsible for current NZ government identity services, and those operating authentication systems in a variety of service agencies, accept that no system can be made completely foolproof, irrespective of budget or technology. The probability of a certain level of error, and of deliberate fraud, must be factored in to the business case for any system. Given this reality, the continued use of language such as 'proof' or 'proving' (which suggests infallibility and certainty) should be avoided[13]. Any authentication scheme is a risk management exercise – the aim is to keep the incidence of error and vulnerability to fraud or other abuse to acceptable levels, in the context of particular processes.

[12] Online Authentication Business Case, Final version, May 2003. The four Trust levels used were based on work of the UK Office of the e-Envoy, and the assessment was made by the E-government unit based on observation/testing of nearly 1400 services available through various government web sites, confirmed by the various service agencies,.

[13] The adoption of the term Evidence of Identity (EOI) in the NZ government is more accurate and far preferable to the term Proof of Identity (POI) still used in Australia and elsewhere.

Existing authentication initiatives

1.19 The PIA brief did not extend to a comprehensive review of existing or planned authentication initiatives in NZ government[14]. The following summaries are based on selective interviews with some agencies.

1.20 The Ministry of Health (MOH) is involved in several low volume pilot authentication projects, most of which involve health care professionals rather than patients. Authentication of roles is the main objective in these projects and for most of the immediately foreseeable applications in health care. A Health Network Code of Practice has been developed as a platform for secure collection, access and exchange of electronic health information, and digital certificates have been chosen as the authentication mechanism within the Health Sector.

1.21 Jointly with the Accident Compensation Corporation (ACC) the MOH is processing on-line claims (ACC45 submissions). The MOH and the ACC also have a joint Privacy Authentication and Security (PAS) initiative which is currently addressing at a policy level authentication and identification needs within the health care and funding system. Both agencies will be reviewing the all-of-government scheme against the PAS framework to ensure it meets their needs.

1.22 The MOH has not been closely involved to date in the cross-agency Evidence of Identity (EOI) work. Authentication for individual patients would need to encompass minors. Privacy is the key driver for security in the health care field, and in many applications medical secrecy provisions will be a stronger driver than the *Privacy Act*. In the health field, the *Health Information Privacy Rules* in the *Health Information Privacy Code 1994* substitute for the default *Information Privacy Principles*.

1.23 The Inland Revenue Department (IRD) and Ministry of Social Development (MSD) are jointly involved in the administration of student loans, and are currently experimenting with telephone access to information using voice recognition and passwords to authenticate callers. MSD has two web-based authentication systems – VoS for Education providers, and SAO (Student Apply Online) for initial application for student loans. However, MSD still requires sighting of EOI documents before processing student loan applications. MSD are also considering the potential for work/income transactions to be carried out on-line, which would require authentication. Most Social Security clients do not have easy access to computers, so this client group are a relatively low priority for on-line services. In the short term, MSD is more likely to develop on-line transactions with contracted service providers.

1.24 While IRD has for some time been investigating authentication options for all its clients, including the more than 5 million individual taxpayers, its main effort and priority relates to authentication of tax professionals and employers. Most current applications requiring authentication rely on User Codes and passwords, which IRD has been advised will provide adequate security for at least another two years. Individuals calling the IRD call centre are authenticated, where necessary, by

[14] The government has requested that all government departments and agencies liaise with the E-government Unit of SSC on any potential or existing developments that involve electronic authentication.

challenge-response questioning, and only a limited range of transactions are allowed by phone.

1.25 The Identity Services Division (ISD) of the Department of Internal Affairs (DIA) encompasses the registration of births deaths and marriages, administration of citizenship records, and issue and control of NZ passports. There is potential for numerous on-line transactions in these areas – many of them subject to the information-matching provisions of the Privacy Act, but few that require authentication of individuals. There are no immediate plans to introduce on-line services that would require ISD operating units to make use of an all-of-government authentication scheme. On-line access to the register of births, which is a publicly available, is under consideration[15].

1.26 Land Information New Zealand (LINZ) is one of the most advanced users of electronic transactions, through its Land*online* database. Registered users (mainly land professionals) have enquiry access and can lodge title dealings and survey information. They are authenticated by digital certificates[16] which are required to be held by each specified individual, with LINZ acting as the Registration Authority checking applicants proof [17]of identity.

1.27 Another user of digital certificates for authentication is the Ministry of Education (MOE), which employs the technology for the submission of data returns by tertiary education institutions.

1.28 The Independent Quality Assurance (IQA) consultants have found that currently there is a range of key technologies in use or being considered for use by NZ government agencies. These include:

- User ID and password
- PKI Digital Certificates with or without hardware tokens
- One-time password tokens
- ID and password plus cellphones texting one-time passwords, and
- Voice recognition of Ids plus PINs

IQA conclude ' … we see that the system will need to support multiple key technologies ..'[18]

1.29 The PIA consultants' conclusions regarding the position of other agencies are included in the *Summary and Conclusions* section at the end of this report.

Public reaction to date

1.30 There has been relatively little public comment to date on the Authentication proposal.

---

[15] Given that this information is publicly available, it should in theory not require any identification or authentication. However, it is being approached cautiously, as it has implications for the security of other areas of government (including potentially the all-of-government authentication scheme) that rely on birth records as EOI.

[16] See http://www.landonline.govt.nz/registereduser/digitalcerts.htm

[17] See footnote 14 concerning use of terms 'proof' and 'evidence'

[18] IQA Papers

1.31 Public consultation in early 2003; the Cabinet decision in June and the release of the Blueprint in July were reported in national media[19]. Whilst mostly factual, these reports emphasised the significance of privacy and security concerns in the government's choice of approach. The New Zealand Herald articles reported concerns expressed by the Citizens Advice Bureau and a security specialist which touched on privacy related issues, but no major concerns were expressed specifically on privacy. This contrasts with experience in Australia, the UK and the US where privacy and consumer groups have been very vocal and critical of Identity/Authentication proposals, and this has been widely reported.

1.32 The EGU undertook a formal consultation process in March & April 2003, inviting comments on a consultation document and holding 30 consultation sessions in five locations, involving the voluntary sector and local communities as well as government, business and educational institutions. Overall, the feedback indicated a strong preference for an option that, amongst other features, involves a limited degree of information sharing; requires a minimum of information to be provided at registration, and gives preference to security and privacy[20]. Other relevant feedback included a desire for clear accountability and availability of recourse in the event of security breaches, and for controls over how information is held and shared. Questions were also asked about whether the potential for identity fraud is escalated with moving to an online environment, and whether authentication solutions can adequately address any increased risk.

1.33 As the statutory spokesperson for the public interest in privacy[21], the Privacy Commissioner issued a media release in March welcoming the privacy enhancing design principles and assumptions in the government's proposal, but cautioning on a number of issues. These included ensuring that the opt-in basis was implemented in the form of real choice; retaining the option of anonymous transactions wherever possible; only authenticating to the level necessary for transactions, and avoiding the introduction of national identity cards 'by stealth'. The Commissioner emphasised the need for a detailed and thorough Privacy Impact Assessment.

1.34 Experience elsewhere suggests that the relatively low level of public concern expressed to date cannot be taken as a reliable indication that major privacy and security issues could not arise publicly as the scheme progresses. No matter how open the process and how many opportunities are given for input, the triggers for community concern are unpredictable. Any one of more of the privacy issues identified in this report could suddenly attract considerable attention and controversy, particularly as the way the scheme would work in practice becomes clearer.

Overseas experience

1.35 Most other countries are at various stages of considering authentication initiatives to facilitate e-government, alongside e-business. As a result, there is a large body of reports and papers available. The Authentication project team visited various

[19] New Zealand Herald 11 and 15 July 2003; Computerworld on line, 13 March, 3 July 2003; scoop.co.nz 1 July 2003;
[20] Online Authentication: Summary Report on Consultation Feedback from Agencies and Public Representatives, July 2003
[21] Privacy Act 1993, s.13 – various relevant functions

federal and local government agencies in Australia during August 2002, and in Singapore, the United Kingdom, Ireland and Canada in October 2002. Their reports of these visits are available on the SSC website.[22]

1.36 The findings from these visits underpinned the recommended approach adopted by the government in 2003 – emphasising a relatively low technology solution proportional to the identified need and with limited ambitions – thereby hopefully avoiding some of the costly mistakes made elsewhere. The experience of digital certificate based schemes in both Australia and the US has fallen well short of expectations[23].

1.37 Since these visits, the situation in most countries has developed further, with some initiatives progressing, others ending for a variety of reasons, and new ones emerging.

1.38 A recently completed report[24] for the Australian federal government sets out a *Framework* for Authentication and a number of *Implementation Strategies* which will be of interest. A *Privacy Impact Assessment* was undertaken as part of the project. Although not yet public, SSC may be able to obtain a copy through inter-governmental channels.

1.39 Private sector authentication initiatives[25] are also relevant, as are the issues of inter-operability and mutual recognition. This Privacy Impact Assessment draws on the consultants' knowledge and experience of authentication studies and initiatives in several jurisdictions, in both the public and private sectors[26].

[22] http://www.e-government.govt.nz/docs/authent-research-2002/index.html

[23] The uptake of digital certificates under the Australian government Gatekeeper framework has been low, and there has been a recent highly critical report by the US General Accounting Office on the planned e-Authentication Gateway (September 2003).

[24] Australian Government Authentication Initiative Final Report, August 2003, commissioned by the Information Management Strategy Committee and managed by the National Office for the Information Economy (NOIE). An earlier discussion paper, National Authentication Technology Framework (NATF) Consultation, issued in May 2003, is available at http://www.noie.gov.au/projects/confidence/Improving/authentication.htm

[25] such as the banking industry's Identrus scheme – see http://www.identrus.com/

[26] The consultants have undertaken directly relevant consultancy assignments for the Hong Kong Immigration Department; the Australian National Office for the Information Economy; Australian Health Network/Healthexchange; the Toronto Management Board Secretariat and several private sector PKI Certification/Registration Authorities. In an advocacy role they have closely followed and commented on numerous other authentication and identification initiatives. They have also conducted numerous other PIAs – see Appendix 1.

Proposed authentication system

2.0 This section of the PIA report describes the system to the level of detail required in order for readers to understand the subsequent privacy analysis. It is in the PIA consultant's own language, drawing on a wide range of sources. It has been reviewed in several drafts by the Project Team to try to ensure that it is an accurate reflection of their intentions. The diagrams at Appendix 3 may assist readers to understand the proposed scheme.

2.1 The design parameters are still evolving – they have changed significantly even in the 3 months since the commencement of this PIA. Clearly the findings and conclusions of the PIA may change as the design is progressively confirmed and/or changed. It is noted that the Independent Quality Assurance is also qualified in respect of design elements that are still evolving; and lack of detail on governance, and post-implementation change and quality management.[27] The Office of the Privacy Commissioner has indicated that provision should be made by SSC for further independent Privacy Impact Assessment of any significant design or governance changes after the date of this report.

2.2 terms in bold are defined in the Glossary in the Business Process Design (BPD) document[28] or other project documentation. The use of the term 'client' in relation to registration risks confusion with its use to signify customers of service agencies. In this PIA the terms **applicant**, **Credential holder** and **client** have been used to distinguish individuals in these three roles (except where quoting directly from other documents). A Glossary of Acronyms and terms is included at Appendix 2.

Introduction

2.3 The project is for centralised national **authentication** of identity of natural persons. Authentication of other assertions (and of identity of legal entities such as companies) is left to individual agencies and organisations in particular contexts.

2.4 The scheme will be available[29] to all natural persons, including overseas residents and visitors, who meet the following criteria:

- who have the capacity to agree to the terms and conditions that are ultimately prescribed for the scheme;
- who wish (or need) to use on-line services provided by a specified and limited range of NZ organisations (initially public sector[30]); and
- who can meet Evidence of Identity requirements.

Provision for parental consent means that minors would be eligible for ID credentials.

2.5 An individual's interactions with the scheme would involve the following four settings:

[27] IQA paper.
[28] Authentication for e-government: Business Process Design, v 0.7, 1 November 2003.
[29] The Government has declared that the scheme is to be optional rather than obligatory, although that effectively means obligatory for anyone wishing to, or required to, perform certain transactions online rather than over the counter or by phone.
[30] Conveniently defined recently in Public Finance (State Sector Management) Bill 2003 – includes all central government departments, crown entities, and local government.

- Registration with an Authentication Agency
- First Time Service Registration with a Service Agency
- Requesting services from a Service Agency
- Receipt of services (Service Delivery) – a result of successful authentication rather than part of it.

Each of these is discussed in turn, although the last two are combined.

Registration with Authentication Agency

2.6 It is expected that the Authentication Agency will be a discrete statutory authority, which may be located within an existing agency or Ministry.

2.7 Individuals will not have to justify their desire to register – they may choose to do so to 'protect' their name even if not intending to use on-line services themselves, although registering for a Credential requires the applicant to obtain a Key, even if they never use the Key.

Application for an ID Credential

2.8 Registration (Application for an ID Credential) involves presenting evidence of identity (**EOI**) to the **Authentication Agency (AA)**.

2.9 Application via online or offline form – individual provides:

- identity or ID data (see paragraph 2.25):
- administrative data, including:
    - contact details (phone and/or address – more than just email);
    - a photograph of acceptable quality[31], and
    - details of one or more trusted referees, including at least one individual who can vouch for the applicant, and in some cases organisations with which details can be verified (probably chosen from a list of 'acceptable' (trusted) organisations/databases) to supplement those with which mandatory checks will be carried out).

2.10 The photograph will be scanned and stored as a digital representation (a form of biometric). It will not be possible to reconstitute a photograph from the biometric, but the photograph itself will also be stored indefinitely for subsequent use, as described below, in the registration process.

Application processed and identity established (to satisfaction of AA).

2.11 Initial stages of registration could be done remotely (by post, or potentially on-line). (The current proposal is for a face to face encounter with a representative or agent of the AA (not just a Trusted Referee – see below) to be required at least once, but typically later in the process.)

2.12 The scope for use of agents has yet to be resolved - criteria will be developed for accreditation of agents by the AA – agents could be either SAs or specialist

[31] Criteria would be set as for passport photographs. Authentication Agency 'shopfronts' may be able to take photographs as a separate service.

intermediaries. The Project team does not see this role as being too widely dispersed, as strict standards would apply, and there may also be significant infrastructure costs.

Notify applicant of receipt

2.13 Applicants would be given the option to receive notification of the receipt of their application, including an application number. This would allow applicants to check the status and progress of their application on-line.

Validate data

2.14 The AA will carry out two levels of checks – 'simple validation' at submission (eg: checks for completion of mandatory fields), then 'basic data processing' (eg: dates out of range; obvious misspellings etc, and checks for duplicates).

Notify applicant of result

2.15 The applicant will be notified if their application fails initial processing.

Establish applicant identity

2.16 Criteria for acceptable Evidence of Identity (EOI) are yet to be finalised, but thinking to date can be seen in the parallel work of the cross-agency EOI Project.

2.17 The Draft EOI framework has five separate objectives – to ascertain:

- A. identity exists;
- B. living identity;
- C. client (applicant) links to identity;
- D. client (applicant) is sole claimant of identity, and
- E. client (applicant) uses the identity in the community

Confirmation of identity by third party trusted referees (TR)

2.18 Confirmation of identity would involve both checks against other databases (primary records) and confirmation by individuals with personal knowledge of the applicant[32].

2.19 Most of the checks against primary records would be mandatory – carried out automatically by the AA – eg: – with the Register of Births for a test of Objective A and the Register of Deaths as part of a test of Objective B. It is possible that other checks could be made with organisations nominated by the applicant (probably from a shortlist of 'acceptable' organisations such as the IRD or Dept of Labour[33]). A visual comparison of the applicant's photo with the person presenting at the AA shop front (see below) would test for both Objectives B & C.

2.20 Confirmation by an individual by a Trusted Referee with knowledge of the applicant and 'vouching for' them is considered necessary to satisfy tests for objectives C & E. Any other individual holding an ID Credential could act as a Trusted Referee[34], provided they were not living at the same address; not a close

[32] Trusted Referees Discussion Paper v 1.0 29 October 2003

[33] Consideration was given to checking private sector databases but there are a range of potential difficulties – see Trusted Referees Discussion Paper v 0.2 8 October 2003, para 25

[34] It is recognised that there would initially need to be a 'bootstrapping' arrangement to create a critical mass of Credential holders who could then act as referees (see Business Process Design v 0.73 November 2003

relative or partner of the applicant; were over 18 and had known the applicant for at least 12 months[35]. The AA would only be able to verify the TR's age (which would be part of their ID data in their Credential) – the other criteria would be satisfied through a statutory declaration by the Referee, backed up by statutory penalties.[36]

2.21 It is recognised that an exception process would be needed for applicants unable to find an appropriate referee – this would probably involve additional checks against other primary records[37]. There may also need to be the option to use Kaumatua, and other culturally specific alternatives, and in exceptional cases provision for individual Trusted Referees who do not themselves hold an Identity Credential.[38]

2.22 The 'vouching for' may not be at point of application – it could be at any time up to creation of the Credential. Individual TRs 'vouching for' an applicant would normally be expected to do so on-line, being presented with an image of the photograph supplied by the applicant[39]. No face-to-face encounter will be required with the individual trusted referee, although a face-to-face encounter with an agent of the AA is considered necessary for other reasons (see below).

2.23 The AA itself would carry out the remaining Test D (sole claimant of identity) by matching both the identity data and the photo biometric. Test D is critical both to ensure the identity has not been claimed before and to prevent multiple registrations by the same person. The photo biometric match would be a one-to-many match which is a much more difficult technical exercise that one-to-one matching. It remains to be specified how rejections would be handled, but this is likely to involve the manual comparison of the original photographic images, which requires that these photographs be stored indefinitely.

If applicable, Notify applicant of failure

2.24 Given that this would amount to an at least temporary denial of identity, with potentially highly significant consequences, there will need to be clear advice and procedures to individuals whose applications fail one or more of the tests. These have yet to be specified.

AA creates an ID credential

2.25 Once the applicant has satisfied the AA as to their identity, a minimum data set (the basis of an **ID credential**) is then recorded by AA. This is a set of verified facts (**ID data**), comprising:

- client's names – including **verified name**(s) (for which the applicant has provided EOI) and **non-verified name**(s) such as aliases and nicknames[40], as well as names created by administrative error;
- client's gender; and

[35] In addition, GCSB is understood to have suggested that only New Zealand citizens should be allowed to act as Trusted Referees.
[36] Trusted Referees Discussion Paper v 1.0 29 October 2003
[37] Eg: Citizenship Certificates or overseas primary records
[38] These criteria are modelled on similar criteria already used for Passport applications.
[39] This assumes that the TR will check their e-mail regularly – which may not be the case for many ordinary adults who are to be accepted as TRs.
[40] It is not clear whether only names declared by the applicant will be recorded, or also other names 'found' by the AA in the course of its checks

- client's date and place of birth.

2.26 It is known that even in a population the size of NZ there will be duplicates with the same name, gender and date and place of birth, and that this is even more likely with overseas populations who may want to access some on-line NZ government services[41]. The biometric of the photograph becomes an important tiebreaker in the case of duplicate ID Credentials[42].

2.27 While the scheme only allows for one ID Credential per individual, ID data will accommodate alternative names, and the AA will not seek to specify which of the verified names (for which an applicant has provided adequate EOI) has primacy. In other words, the scheme does not set out to create an 'official name' for each individual, although for those supplying only one verified name, this will be the effect.

2.28 ID data will not include business or professional roles – this is being left to SAs. The project team see this as an important part of the commitment to minimum information exchange – the AA does not need to know about an individual's roles or relationships with any particular SA, although the audit trail of SA's initial validation and subsequent use of Keys will in fact mean that that the AA unavoidably holds quite a lot of information about a person's relationships with government.

2.29 The current view is that the AA will not become involved in recording linkages between individuals (also including parentage, guardianship, powers of attorney). As in offline transactions, it will be left to SAs to establish separately that a particular person has the authority to act for another in particular contexts (there may be a separate case for a central register but this function is not considered appropriate for the AA).

2.30 The AA customer record will also include administrative data, including the photograph (image and biometric); contact details provided by the applicant, and internally generated data such as date of Credential issue and expiry[43]; the identity of the Trusted Referee(s) and date and time of verification with them, and audit trails..

2.31 The AA record for each ID Credential will also be assigned a unique customer or credential **number** (likely to be sequential) for internal administrative use. There is no need for the Credential number to be known to anyone outside the AA.[44]

Once Customer record created, client[45] is notified

2.32 Once a Credential has been created, a **Credential confirmation** notice will be sent to the Credential holder. This will confirm that a customer record has been

[41] Biometrics Discussion Paper v 0.3 9 October 2003, para 29
[42] It has been suggested that a fourth data item – mother's name – would ensure almost no chance of duplication at least within the New Zealand population. This data item is already used by the NZ Birth, Death and Marriages registration process.
[43] This assumes Credentials will have a finite life – there are a range of justifications for this
[44] Even the Credential holder does not need to know the number and the security risk of letting them know will need to be balanced against their 'default' right under the Privacy Act to access that information on request – see under IPP 6 below.
[45] Note that at this point, an applicant has become a client of the AA.

created, along with explanation of how to obtain a **Key** if not already acquired (see below) and how to apply to associate the Key with the Credential.

2.33 No detail is provided yet of what form the confirmation will take or what information it will contain and/or display, although it is expected to be in writing (letter, fax or e-mail) and will need to contain a number or reference (possibly the original application number but not the Credential number, which is reserved for internal AA use). Although it is not intended that it contain any of the ID Credential data, it is difficult to see how it could avoid including at least a name, together with contact details.[46]

Client obtains a Key from an approved Key provider.

2.34 A Key is the means by which a user of on-line services (client) will authenticate themselves to a Service Agency. This authentication may involve authorising the release of ID Credential data by the AA, or provision of a valid and current Key may suffice, depending on the criteria set by the SA, including level of trust required for the particular transaction (see paragraphs 2.57 & 2.79-2.80).

2.35 Keys could be issued by the AA[47] or by another accredited Key provider, or alternatively an individual may already have a Key issued by another agency which meets the required standard. Key providers may include some SAs but may also include private sector organisations.

2.36 Acquisition of a Key will not necessarily follow the creation of a customer record – individuals will often obtain a Key first[48] and then apply to the AA for an ID Credential, so that their Key can be associated with the customer record (see below) at the same time.

2.37 It is expected that most SAs will only need Keys to be a simple username/password pair, but some will require 'stronger' authentication than the typing of a password can provide, in particular in the form of a digital signature generated by use of a private key, whose public key is attested to in a digital certificate issued by a certification authority

2.38 It is proposed that technical standards will be issued for Keys acceptable to the AA (eg: length and format of usernames/passwords, strength of digital key pairs).

2.39 There is no detail yet on what other standards should apply to Key-issuing. These are likely to be specified through the E-government Interoperability framework (e-GIF)[49], and if Key Providers wish their keys to be accepted for government use they will have to meet the minimum standards.

[46] Postal or email address only – if delivered by phone or fax the confirmation need not contain the number.
[47] For convenience, AA shopfronts (as agents for the separate AA function as a Key Provider) may be able to issue a Key at the same time as processing an application for an ID credential..
[48] As illustrated in the Powerpoint Presentation, Process Design Consultation, October 2003, slide 17
[49] http://www.e-government.govt.nz/interoperability/index.asp

2.40 If the Key is to be a username/password pair, the Key provider (which may be the AA) may initially issue an **enablement code** allowing the user to then select their own Key (ie: **username and password**).

2.41 Holders will be able to have multiple Keys, including one or more username/password pairs, and/or one or more digital certificates/key pairs. Keys must necessarily be unique within a domain, i.e. within the set of Keys issued by each particular Key Provider. They will never be re-issued. In the case of username-password pairs, a username can be issued by a Key Provider to one person only. Hence the second John.Smith who presents at each particular KP will not be able to use John.Smith with that KP. The Key serial number will also be unique (if only because it will contain a unique identifier for the KP). Users will encounter the same problem experienced with free email systems such as Hotmail or Yahoo mail where individuals find they have to add characters/numbers if they wish to include their real name eg: John.Smith43[50].

2.42 Holders may choose multiple Keys to perform business or professional roles (but see the discussion in the Privacy Analysis below), but also to create different superficial persona – they will not have to justify their choice. This will theoretically allow individuals to continue to use a name or label by which they are already known to an SA even if that is not the same name that they use in other relationships with government[51] (although all their alternate names will need to be held by the AA as part of their unique AA credential, and may be revealed to SAs, depending on the business rules relevant to the particular transaction).

2.43 The options for delivery of enablement codes and/or Keys are still under discussion. Options include physical collection (from Key provider or agents); or despatch of codes/Key to a known location – either physical (in which case a postal address will be required), or other (eg: an SMS to a cellphone, in which case a phone number will be required). It is possible that some Keys may include a physical component such as a token, but criteria for acceptable Key specifications have yet to be developed.[52]

2.44 On issue, a Key is an independent set of data with no related ID Credential stored at the AA. It may be linked by the Key Provider to an *individual* (ie: natural person) holder, but the holder could also be a role, or even an organisation. A Key that is not associated with an ID Credential may still be used for authentication in other settings or contexts, or if separately accepted by an SA.

2.45 If the AA is to be a Key Provider, this function will be entirely separate from the issuing of ID Credentials[53]. Linkages between data held for the two functions will

[50] The only way of avoiding this might be for KPs to create separate 'domains' which seems unlikely.
[51] Assuming this is lawful – there may be some constraints on individuals ability to use pseudonyms in certain government transactions.
[52] This would be a significant issue if Key Providers issued cards or other devices containing identifying particulars – see under Analysis below.
[53] If the same agency housed both the AA and a KP function, a range of shared services would be acceptable – mainly corporate services but even some operational support, providing the data and processes were quarantined.

only be made in the same way as they would for Keys issued by other (non-AA) Key Providers (see below).

Associating Keys to Customer records – activation of Credential

2.46 Individuals would be required to appear in person at an AA (or agent's) shop front to have a Key associated with their ID Credential. Arrangements for the housebound or others unable to readily access a shop front are under consideration.

2.47 The applicant would present evidence that a Customer record had been created – typically the confirmation notice issued by the AA.

2.48 The AA shop front (or agent) uses the number or reference on the notice[54] to call up the customer record (this requires an on-line connection but need not be in real-time – individuals could pre-book an interview time).

Verify client matches photo

2.49 Shop front personnel would make a visual comparison between the person presenting and the photo image on the customer record[55]. Assuming a match, they would proceed to the next step.

Request Key and confirm acceptable

2.50 The shopfront personnel will ask the individual to use the Key which they wish to be associated with their Credential. This will not involve the individual in revealing their Key, (which may be a username/password pair or a digital Key on some electronic storage medium) to the shopfront personnel, but will require an on-line connection to all Key Providers[56]. It is envisaged that the person would typically enter their Key into a secure web-site belonging to their Key Provider, in a private environment[57]. The Key Provider would return to the AA shopfront or agent confirmation that the Key is valid and current, along with the serial number of the Key. This will be a unique number[58] assigned by the Key Provider according to specifications issued by the government[59]. The Key serial number would include characters identifying the Key Provider and possibly date and time of issue of the Key.

[54] Potentially, the record could be found by searching on Identity details if necessary, eg: where individuals 'lost' their confirmation notice.
[55] The shopfront may offer a photo-taking service but a registration application must have been processed, and an ID Credential created, before a Key can be associated with it.
[56] In order to provide this functionality, which will also be required by all SAs seeking to use the system, it appears that a sophisticated infrastructure will be required, providing common interfaces and connections equivalent to the present credit/debit card authorisation networks. Recent design documentation refers to this as a Centralised Authentication Hub or Common Logon Site. The viability of this infrastructure model has been reviewed by the IQA consultants. Source: IQA paper.
[57] For example, a private room could be used for this purpose to reduce the likelihood of 'overlooking' or 'skimming' such as has been a problem with Bank automated teller machines.
[58] Unique across all Key Providers
[59] probably not by the AA.

2.51 The individual would also at this point physically sign to acknowledge and accept[60] the terms and conditions associated with the use of the all-of-government authentication solution[61].

AA recording of Keys

2.52 The AA will add to the customer record the **serial number** of each Key associated with an ID Credential. This is for consistent administration – given the variety of different Key types that will be accommodated, and means that the AA does not need to record the actual Key (which would compromise security even more[62]).

2.53 The provisional design assumes that Keys will have limited life, in recognition of rapidly changing technology and the likelihood of the appearance of new types of Keys in the medium term. It is assumed that on expiry a new Key would be issued, rather than extending the life of the original, so that a new Key Serial Number would be issued. Key-holders would receive warning of expiry and could use an about-to-expire or recently-expired Key to associate a new one with the same Credential (expired Keys could only be used for this purpose for a limited period). For a Key which was lost or compromised, or which had expired for longer than the 'grace' period, Holders would have to go through the same process of applying to have a replacement Key associated with their ID credential as for first time association.[63]

2.54 Once a record is created, and a Key is associated with the Credential, the Key Serial Number will be retained indefinitely. It may become non-active (as a result of a Key being withdrawn (**suspended**) or **revoked** for various reasons including death) but is never re-used, and is retained for archival and non-repudiation purposes.

2.55 There will be a range of circumstances where knowledge of data items from a particular individual's ID Credential – particularly their names – and of any associated Keys will present a particular security risk. Special arrangements for 'protected identities' are under consideration[64].

2.56 While the above steps have been presented sequentially, they may well occur in a different order or even simultaneously. The critical point is that all of the following steps have to have been completed before a Credential is created:

- Completed application received and processed

[60] Acceptance of terms and conditions does not necessarily signify consent, if consent means free and informed. We all routinely sign so-called consents when in reality we are simply acknowledging that the service we want is offered on a take-it or leave-it basis, with no genuine choice other than to walk away.

[61] Legal advice is that a physical signature is required for liability reasons (although allocation of liability is yet to be resolved).

[62] See under IPP 5 – Security in the analysis section for privacy and security concerns about a centralised record of all associated Keys.

[63] This is a design issue with major implications for privacy and security, and the PIA can only be provisional on this matter until the process is confirmed

[64] It is envisaged that protected persons such as individuals on witness protection programmes will receive a new and separate ID Credential. Any links between the old and new Credential would be held separately and securely. Issues of how this separation would work in the context of a range of transactions, including taxation, superannuation, benefits, and court appearances, remain to be resolved, although there are existing precedents.

- Identity details and photograph verified with trusted referees
- Photograph matched with other photographs held by AA to ensure no duplication
- Photograph matched with individual at shopfront
- Terms and conditions signed by same individual at shopfront
- Valid and current Key presented by same individual at shopfront and associated with a Credential

Use of AA by SAs

2.57 The Authentication scheme is based on an analysis of levels of trust, and two of the Cabinet approved principles – the fit for purpose policy principle and the risk-based approach implementation principle – mean that SAs should only require users of on-line transactions to authenticate themselves where this is necessary. It remains to be decided if there will be mandatory criteria, or some process of approval, for agencies to meet before they can seek to use the proposed Authentication system.

2.58 The following part of the project description applies to those SAs that can justify authentication to a level that requires access to the AA system.

First time service registration (FTSR)

Presentation of a Key

2.59 The individual presents at a Service Agency (either on-line and/or in other ways) Through a channel provided by the SA (normally on-line[65]), the individual presents their Key to their Key Provider. The Key Provider returns the Key serial number to the SA (thereby confirming that the Key is valid and current) for subsequent use as described below.

Application for registration

2.60 An individual applies to an SA to become an *on-line* client, and will have to complete an SA registration process (Note this is not the same as registering as a client of the agency, for which separate processes will usually continue to apply[66]).

2.61 While presentation of a Key before registration may be appropriate in some circumstances (eg: where an SA wants to pre-populate a form), in other cases, these two steps may be reversed.

Request verified information

2.62 The client then authorises the AA to release ID data to the SA. This is known as a **Request for Verified Information or RVI**. process The model assumes that this can only be initiated by the SA, and requires express authorisation by the client,

[65] See paragraph 2.50above and footnote 56 for discussion of the major infrastructure that will be required to facilitate validation of Keys by SAs.

[66] The SA will typically require additional information concerning eligibility. But as SAs move increasingly to an on-line service delivery model, these two steps may merge ie: someone will become a client by applying on-line, and never have any other contact with the SA.

although there will presumably be some public interest overrides for investigations, law enforcement etc[67].

2.63 The SA would provide the client with an RVI number, which will conform to standards set by the AA, and which must be unique[68]. It may include a date-time stamp, and must serve to identify the SA issuing it, so as to allow its use as described below.

2.64 The client then accesses the AA web site and enters the RVI number, and again uses their Key. This authorises the AA, if the Key is valid and current (there is a simultaneous on-line check with the relevant Key Provider for this[69]), to send ID data to the specified SA (identified from the RVI number).

2.65 The model provides for the client to activate the RVI at different times – it could be at the time of application for service/transaction, or it could be at a later time – the SA may for instance send the RVI Number to the client by post or email. Alternatively, the client-AA session could be enabled from within the session with the SA, providing in effect a single seamless transaction. It is currently envisaged that there would be a Common Logon Site (CLS) through which all the related transactions are performed[70].

2.66 The AA will return to the SA the RVI number together with the ID data requested, and authorised for release by the client.

2.67 The design provides for the individuals with more than one registered verified name to specify which name(s) may be released to the SA. However, an SA's business rules or criteria may mean that it is a condition of service that clients authorise the release of all verified names, and all aliases (eg: as a barrier to 'double dipping'). It may be that not all SAs would require date and place of birth or gender, in which case release of these data items could also be optional.

2.68 The receipt by an SA of a client's ID data will normally be by an automated link to the AA in response to a specific RVI. Some SAs may hold the same (partial or complete) details in their own records, but will not get copies of whole sets of AA credentials or be allowed to routinely perform matches for other reasons. The only permitted operational[71] purpose of access will be to receive ID data relevant to the requested transaction[72].

---

[67] Access without the authority of the Credential holder would be another process – reserving the RVI process for the 'authorised' operation described here.

[68] The RVI number may be delivered by using a world wide web URL.

[69] There is no need for the AA to record suspension or revocation of Keys – it will instead check the status of the Key with the Key Provider on each occasion of an RVI.

[70] The Independent Quality Assurance consultants for the Project have reached the tentative conclusion that this model is workable, although it recommends further evaluation by technical experts - see Hunter Group, Review of Business Process Design – Interim Report 2, 31 October 2003.

[71] Meaning for the purposes of the authentication scheme. As already noted, there will be a range of other public policy purposes for which AA data can be accessed, and the limits of this will need to be expressly set.

[72] The SA will not receive separate confirmation that the the client's Key is associated with a particular Credential – if it is, then the SA will receive the relevant ID data; if not, no data will be provided and the SA will have to either take this up with the client, or simply decline to deal with them.

2.69 The AA will always notify the client that information has been released in response to a valid RVI – this may be during the transaction session or, more likely, by email or post to the client[73].

Linking Key with SA Client Records

2.70 On receipt of a positive response from the AA to an RVI, the SA will then link the client's Key with a client record – by recording the Key serial number (received from the Key Provider) against their own customer name/**service reference number**, but only where necessary (ie: where verification of identity is justified for the specific on-line transaction).

2.71 The use made of the authentication result will depend on an SA's business rules. An SA will typically require at least the name by which they know the client (in their own records) to match the name (or one of the alternate names) included in the ID Credential. They may also require a match on place and date of birth and/or gender.

2.72 No other information held by the AA will be made available to the SA (ie: no contact details, and neither the image nor the biometric of the registration photograph).

2.73 If an individual registering for on-line transactions is not already a client of the SA, the SA may need to collect other particulars (**service delivery information**) as part of their FTSR process. In some cases, there will be an element of additional identity and attribute verification in this process – going beyond what the AA is able to provide. This is a matter for the SA and their own business processes.

2.74 Some SAs may also wish to confirm the identity of minors, or others 'without capacity' who do not themselves hold an ID Credential[74]. Confirmation of identity of such people will continue to be the responsibility of SAs using other processes.

2.75 Depending on the SA rules, clients may be able to associate more than one Key with their customer record if they wish or need to do so.

2.76 The SA may record specific customer roles, rights or responsibilities alongside the customer's Key Serial Number(s)

2.77 Some SAs will (some already do) require digital certificates – hopefully because they can justify a higher level of security[75] (eg: already required by LandonLine; Ministry of Education for some teachers, Ministry of Health for some health care providers). In such cases persons may not have a choice – use of a digital certificate may be mandatory (although they may hold other Keys for use in other roles).

---

[73] An 'out-of-band' notice is considered preferable for security reasons. While the contact details given on the original application may be out-of-date, the AA could invite updating. However, this would have implications for the value of the AA customer records as a population register – see Privacy Analysis.

[74] The design allows for minors to hold ID Credentials, where appropriate with parental consent, but it is unlikely that many minors will voluntarily apply to Credentials unless one or more SAs promote registration.

[75] The issue of whether there should be mandatory criteria for use of stronger authentication such as digital certificates is under consideration.

2.78 SAs have no need to record actual Keys, and to do so would create a security risk[76]. The business process design for the authentication scheme provides no opportunity for the capture of Key details by either the AA itself or SAs. .

Requesting Services from a Service Agency and Receiving Services (Service Delivery)

2.79 Once a client is registered with an SA to use a Key for online transactions, most SAs should only need to ensure that on each occasion of use, the Key in question is still valid and current. This will be done by the client using their Key in a session with the relevant Key Provider, generally facilitated through the proposed Common Logon Site. If the Key is valid and current, the KP would return the Key Serial Number to the SA, allowing it to locate the relevant client record.

2.80 However, some SAs may wish to repeat a more detailed Identity verification at the time of each and every request for service. This could be achieved through the same RVI process as will be used for First Time Service Registration.

Funding/charging

2.81 It is not yet clear what the financial arrangements will be. If SAs are charged for their use of the Authentication system, the pattern of use could be quite different from that which would emerge if the system was to be provided free of charge to users, and the costs covered centrally. Similarly, uptake and use of the system will be affected by any cost to Credential- or Key-holders. Since the pattern of use affects the privacy implications, no final assessment of the privacy impact will be possible until the funding arrangements have been clarified.

Other options

2.82 The Project Team have considered the other options that are available if for whatever reason the centralised Authentication scheme proposed is not adopted. Two principal alternatives have been identified.

2.83 Status Quo. This model assumes that online Authentication will continue to develop on an individual agency basis. Growth of online Authentication would be on the basis of 'as and when' specific Service Agencies find an appropriate service that can be offered online and which requires authentication, and a business case supports such a development.

2.84 Standards only. This model assumes that online Authentication will continue to develop on an individual agency basis. However, this growth would be required to use a consistent approach (set of standards), for example as to what is Identity, that would be generated/imposed/maintained etc centrally. Otherwise, the approach is similar to the Status Quo option – such services would appear on the basis of 'as and when' specific Service Agencies can justify them.

[76] In the case of digital signatures, SAs may record a client's public key.

2.85 Other options such as a more centralised and comprehensive model involving identity cards and the central storage of more data were considered and rejected at an earlier stage.

2.86 During consultation, it was observed77 that since SAs will have to maintain separate Evidence of Identity (EOI) processes for off-line clients, and to deal with exceptions and system failures, there may be limited value in the AA system, at least in terms of savings. The scheme design encourages direct liaison between SA and Key Providers for many service delivery transactions, without any interaction with the AA. If minimum EOI standards are set centrally, as seems likely through other initiatives78, and if Key Providers require EOI to those standards to meet the needs of other clients, then the value added by the AA and its accompanying infrastructure comes into question.

2.87 These observations have more do with the business case for the proposed scheme than the privacy impact, but they are relevant to the balance that will ultimately need to be struck between positive and negative features in deciding whether to proceed, as well as to the likely uptake and usage of the system if it proceeds.

[77] Discussions with Office of the Privacy Commissioner
[78] Eg. EOI cross-agency working group chaired by DIA.

Privacy Analysis and Risk Assessment

Scope

3.0 A Privacy Impact Assessment of the authentication scheme cannot be confined solely to the role of the proposed new Authentication Agency (AA), or even to the interaction between the AA and other agencies. A full PIA for this scheme must necessarily look also at the proposed use of the Keys and ID data by Service Agencies (SAs), as this is where many of the significant privacy impacts will arise. However, the brief for this PIA, and the timescale, have allowed only a relatively superficial review of likely uses – it has only been possible, for instance, to interview a few SAs about their possible uses of the scheme.

3.1 It is also clear that many SAs are not able or willing to commit themselves at this stage – they will only make decisions about the utility of the scheme to their operations once the design has progressed, and in particular until uncertainties about liability have been resolved. It seems likely that some agencies will not commit themselves to use of the scheme until they are able to see how it operates in practice. It has therefore been necessary to speculate about other possible uses, based on overseas experience and knowledge of typical government and business needs.

Alternatives

3.2 It is not the function of *this* Privacy Impact Assessment to canvass all possible alternative ways of achieving the government's objectives[79]. These alternatives may be more or less privacy intrusive. As noted earlier, the EGU considered a number of options, and Cabinet approved the current approach based partly on consideration of privacy concerns. There is some further discussion of the alternatives that remain open under 'Other Options' above (paragraphs 122-127).

3.3 Where an alternative is obviously available which could be accommodated within the current approach and design, and which is preferable from a privacy perspective, then it is mentioned in the analysis below. Where an alternative approach could resolve a major privacy issue it is also mentioned, such as under the *One individual, one credential* and *Biometrics* headings. But this report does *not* go back to first principles and look at all alternatives. This remains an option for the government, in light of both this Assessment and the Business Case.

[79] A PIA could have this objective – see for instance the PIA carried out as part of the Australian Government's review of Authentication options – National Office of the Information Economy, Australian Government Authentication Initiative Final Report, August 2003 – not yet publicly available.

General Issues

Issues arising from overall system design

Authentication both a positive and a negative for privacy

3.4 A national identity authentication scheme for on-line transactions would be both privacy enhancing and privacy diminishing. It could be a powerful tool to ensure both security and quality of personal information – directly contributing to compliance with IPPs 5 & 8, and indirectly to the other IPPs. On the other hand, the scheme will be perceived by some as introducing a significant infrastructure of surveillance, potentially facilitating the sharing and matching of personal information held for different purposes.

3.5 The scheme is also inherently privacy intrusive in requiring a level of identity verification that is unfamiliar to many New Zealanders[80]. The potential extent of popular resistance to being asked, or in many cases required[81] to register should not be underestimated, and this will be compounded by the need, in the current design, for renewal of registration many times during an individual's lifetime. The extent to which the public may be prepared to accept this will depend on whether they can be persuaded:

- that better authentication is necessary for on-line transactions with government;
- that the benefits outweigh the immediately identifiable privacy costs, and
- that there are sufficient protections in place to ensure that the costs to privacy do not increase in future as a result of scope- or function-creep.

3.6 A similar benefit:cost case will need to be made in relation to financial and other costs, but these lie outside the scope of this report.

Project justification - Identity fraud and Identity theft

3.7 One of the justifications for this, and all, authentication and identification schemes is the alleged problem of identity fraud and identity theft. A recent US Federal Trade Commission report has estimated that 1 in 8 Americans has been the victim of identity theft in the last five years[82]. A recent Australian Government report identifies 'new generation fraud' – involving technology, e-commerce and identity, and asserts "The type of fraud of most concern is internet fraud or cyberfraud."[83]

3.8 Despite claims that ID fraud and theft are major and growing problems, there is a dearth of evidence – reasons for this include the reluctance of organisations to admit to security breaches[84], and the reluctance of government agencies to share information

[80] NZ Passport holders will be familiar with a similar EOI requirement, but few other relationships with government require the same processes and level of evidence.
[81] See below for discussion of why registration will effectively be mandatory for many individuals playing organisational roles.
[82] Reported at CNN.com 4 September 2003 - http://www.cnn.com/2003/TECH/ptech/09/04/id.crime/index.html (accessed 19 October 2003)
[83] The Changing Nature of Fraud in Australia, July 2003, at http://law.gov.au/agd/Department/Publications/publications/Fraud.htm (accessed 20 October 2003)
[84] The Australian government report estimates that two thirds of fraud offences in the private sector are not reported

about the alleged problem. A new Australian report[85], based on responses from 120 organisations, estimates the cost of ID fraud in Australia in 2001-02 as AU$1.1 billion, although 57% of this was the resource cost of preventative measures, with only AU$420 million of actual financial losses. This compares with previous estimates of AU$2-4.5 billion. There is also some empirical evidence from the US and UK[86], although as the SIRCA report notes, figures on growth of ID fraud may partly reflect improved awareness and reporting.

3.9 There is some confusion and duplication in the use of the terms identity theft and identity fraud, not only in this project[87] but worldwide. The EGU has touched on this issue[88], reporting that the US government has defined identity theft as actual or attempted fraudulent use of identification information of another person, with the intent to obtain [benefit]. The UK government has proposed that the very act of using a false identity would be a criminal offence without the need to prove any criminal intent or conspiracy.

3.10 While relevant NZ criminal law currently focuses on property offences, the authentication project has a legal opinion to confirm that the Criminal Law covers the concept of identity fraud, specifically in an online environment. The EGU paper defines Identity fraud as occurring when someone uses a means of identification of another person or a fictitious person. This is however too broad a definition to be useful as it would catch both authorised actions on another person's behalf, and legitimate pseudonymous transactions.

3.11 Without going into greater detail, it is clear that both the definitions and the scale of the alleged problems are uncertain. This is not to deny that a real problem exists, merely that if significant costs (financial, privacy or other) are to be incurred to address the problem, it is desirable that there be greater certainty and more evidence as to the benefits, as well as a clear demonstration that the remedies proposed will actually work.

3.12 As well as limiting deliberate identity fraud and theft, a centralised all-of-government authentication system should have advantages in terms of limiting unauthorised access to information and consequential access to services by persons that are not eligible. But it also raises the stakes in terms of the consequences of such unauthorised access. There have been frequent anecdotal accounts of the cost to individuals of identity denial resulting from someone else having committed identity theft, particularly in the US[89].

---

[85] Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent SIRCA 02—2003 for Steering Committee on Proof of Identity, chaired by AUSTRAC, November 2003 – available through Standards Australia

[86] In the US, for example, the passage of the Identity Theft Assumption and Deterrence Act of 1998 (18 U.S.C. 1028) was founded upon the results of an investigation by the US GAO on the Cost of Identity Fraud released earlier that year (GAO, 1998). Comparative research has also been conducted within the United Kingdom (Cabinet Office, 2002). (Source: SIRCA report – see footnote 66)

[87] Biometrics Discussion Paper, v 0.3 9 October 2003, 3.3.2 & 3.3.3 paras 31 & 32 – appears to suggest that fraud is where the perpetrator aims to create multiple identities whereas theft is a single masquerade.

[88] On-line Authentication: Security, e-government unit, March 2003, Section 3 – Identity Fraud

[89] and also popular illustration in films such as *Gattaca*, *Minority Report* and *Catch me if you can.*

3.13 The EGU paper accepts that:

> "Online authentication is seen as having great potential for successfully reducing identity fraud, if implemented properly. Online authentication, implemented poorly, could exacerbate the growing problem of identity fraud."[90]

Related implications are explored further under *Issues arising from failed transactions* below.

Project justification – more accurate authentication of identity assertions

3.14 Apart from protecting against malicious actions such as identity fraud and theft, the other main justification for better authentication of identity assertions is the benefits of more accurate use of identifiers. The direct value of the authentication scheme is to ensure that information only goes to the 'right' person, but this is only an intermediate objective – the ultimate benefits include ensuring that individuals shoulder all of their obligations (taxation, payment of fines etc); seeking to deliver all services to which individuals are entitled; and ensuring that individuals do not receive services to which they are not entitled, or duplicate benefits (not all such results would necessarily involve deliberate fraud).

3.15 As with identity crime, there is a dearth of evidence of the potential scale and value of these benefits. Again, it is desirable that this evidence be produced and quantified to set against the disbenefits, including financial costs, of the authentication scheme.

Project justification – updating existing processes

3.16 Some agencies have suggested that the scheme should be seen merely as a technological updating of existing processes, with no new functions. We accept that identification is an existing issue for most agencies, and that concerns about identity fraud and theft, and the benefits of 'correct' identification, apply equally in off-line transactions, where authentication is also constantly under review. But the new scheme will do much more than simply replicate existing processes in the online environment. It represents a significant shift to greater centralisation, common infrastructure and cross-agency information exchange.

Recommendation 1. A clear articulation of the justification for the scheme, and a quantified analysis of the underlying problems it addresses, are necessary in order that the business case for the scheme can be assessed alongside the privacy impact.

One individual, one credential?

3.17 Many of the negative privacy consequences of the proposal (explained further below) stem from the initial policy choice, currently built into the design, to only allow one credential or record to be created and held by the Authentication Agency for each natural person. This is based on a conceptual model, consistent with the general NZ government approach to EOI which does not distinguish between entities and identities.

[90] On-line Authentication: Security, e-government unit, March 2003, Section 3 – Identity Fraud

3.18 We suggest that an alternative conceptual model is preferable, and reflects more accurately the way in which identity operates in the real world[91]. Whilst each individual (entity) has only one physical existence, most of us have more than one identity, if identity is defined as a particular presentation of a person, especially a role that a person adopts. While there may be some statutory constraints on what identifier an individual may use for some purposes (citizenship, taxation etc)[92], it is possible in many jurisdictions, including New Zealand, for individuals to legitimately use different names (such as birth or married names) for a wide range of different purposes.[93] Significantly, it appears that in most common law jurisdictions, the validity or criminality of any act is unaffected by the use of a name – the law looks to a person (entity), whatever they may have been known as when performing that act.

3.19 Understandably, bureaucratic systems find it difficult to deal with multiple identities and identifiers, and there has always been pressure to standardise labels, and to seek to uniquely identify individuals. However, any scheme which pushes or pulls individuals towards such an outcome will be seen by some as undesirable.

3.20 At the most general level, any privacy analysis of a scheme that supports identification and authentication must start by asking if the scheme will have the effect of requiring individuals to have, and to present themselves using, a single official identity, thereby denying them the option of multiple identities. The capacity of this scheme to admit and deal with 'alternate names' and multiple roles, whilst desirable, will not in itself be a sufficient response if the scheme also insists on linking all alternate names and roles to a single official identifier.

3.21 The rationale for the scheme, as expressed in various documents, is "to ensure that people who choose to transact with government electronically *are who they say they are*." (emphasis added) and to "allow [both parties to] have confidence in the identity of the other party" [94] and the need for "individuals to prove who they are"[95]. More recent working documents claim "[because] there can only be one identity for one person"[96] and "This means providing evidence of your unique identity"[97]. There is a logical gap between first three and last two of these statements. Neither of three objectives quoted above require that each individual can have only *one* identity (or ID credential). It should arguably be a sufficient objective and practical outcome that the scheme establish that a person is who they claim to be – a goal which allows for multiple identities and identifiers, not just multiple roles using a single identifier.

---

[91] For a more detailed exposition of this model, see Clarke R. (1999) *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice*, at http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html#Id ; Clarke R. (2001) *Authentication: A Sufficiently Rich Model to Enable e-Business'* at http://www.anu.edu.au/people/Roger.Clarke/EC/AuthModel.html#HEI ; and Clarke R. (2003) *Authentication Re-visited: How Public Key Infrastructure Could Yet Prosper* at http://www.anu.edu.au/people/Roger.Clarke/EC/Bled03.html#HEI

[92] In New Zealand there are some clear constraints within particular government programmes – eg: the Ministry of Education requires a single verified name for all educational qualifications.

[93] See Clarke R. (1994) Human Identification in Information Systems at http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html

[94] Design of online authentication for government: summary of recommended approach – July 2003

[95] Blueprint: Authentication for e-government, July 2003, p3

[96] Key Provider Role, v.0.3 Oct 03, paragraph 10.

[97] Discussion Paper: Single or Multiple EOI processes 2.2 v0.2 6 October 2003 (para 3).

3.22 There may be a case to be made for why some government purposes require knowledge that claimed and supported identity A is actually the same natural person as claimed and supported identity B[98]. But this case is not made convincingly in any of the documentation[99]. It is strongly suggested that a more robust argument is made before the justification for the scheme is published.

3.23 Assuming such a case can be made, it does not necessarily follow that the scheme has to allow only one Credential per natural person. A viable alternative would be to allow an individual to hold multiple Credentials, whilst recording the links between them (not necessarily, and indeed preferably not, at the AA). Access to the linkage information could then be 'rationed' to only those government functions which could demonstrate a need for the extra information – most should be content to know that a client *is who they say they are*.

3.24 It could be argued that this alternative design, with linked multiple credentials, would not deliver any more real privacy to individuals, since all of the transactions relating to a single natural person could be brought together. However, such a rebuttal underestimates both the symbolic value of allowing multiple identities, and the practical protection afforded by putting barriers in the way of easy data sharing and matching, and by ensuring that linkages are held by different agencies in separate systems.

Recommendation 2. The conceptual basis of the scheme should be revisited with a view to allowing for registration of multiple identities, linked only where necessary and justified.

Confirmation vs release of information

3.25 The scheme has been designed around a model in which the AA simply releases information – ID data – to SAs in response to an RVI authorised by the Credential Holder. The SAs are left to make any decisions about authority or eligibility based on that information. Several parties, including the Office of the Privacy Commissioner, have suggested an alternative model in which the AA verifies information provided by an SA, without actually releasing any ID data to the SA. In this model, an SA would ask the AA if a client with a particular set of ID data (name, date and place of birth and/or gender) held a particular Key. The AA would simply confirm 'yes or no'. One privacy enhancing advantage of this model is that SAs would not find out what other names the individual had registered (for use with other agencies), and would not be told gender and date/place of birth unless they were relevant to the particular transaction.

3.26 The Project Team's response is that their preferred model leaves the decision-making authority (and presumably therefore any liability?) with the SAs, and also

[98] It is understood that the IQA consultants, who initially favoured the option of multiple credentials, are now inclined to support the single credential model, partly on the basis that it reduces the likelihood of undetected theft.

[99] Some of the project documentation states that prevention of 'double dipping' underlies the need for evidence of a 'unique' identity, but there is sufficient doubt about this asserted benefit to justify a request for a more detailed analysis.

allows them to pre-populate forms. Neither of these reasons seem persuasive. It seems doubtful that any SA will use the scheme unless the AA accepts at least shared liability for any errors arising from reliance on the ID data. And most SAs will already have any of the items of ID data which are relevant to them in their own customer records, alongside a Key serial number, giving them another source for pre-populating forms.

3.27 There are other arguments against the simple yes/no verification. Firstly it would lead to the AA compiling a central record, in its audit logs, of which names were used by which individuals in relation to each SA. The preferred model in the current design initially had no such record, as all names, and other ID data, would have been given to an SA in response to an RVI request.

3.28 However, partly in response to privacy concerns, the revised design allows for Credential holders to specify in an RVI which items of ID data they authorise the AA to release. This means that the AA's records will show which names are passed to which SAs.

3.29 A second argument is that a simple binary response by the AA would inevitably mean that ID credential checks would need to be made more often. Instead of the SA receiving all of the relevant data from the AA and then being able to engage with the client over any discrepancies (e.g. Rachael spelt Racheal etc) all the SA would be able to say to the Client is "sorry your transaction has been declined because the data you have provided was not able to be matched with the AA data". The SA would have no way of determining how big or small the discrepancy was and would have to reject the transaction. If the client realised the error was their own and tried again then the SA would have to do another check with the AA so the RVI process would need to be repeated again. The approach is less customer friendly and would require far more ID credential checks to be carried out in total, increasing the overall exposure of Credential Holders information.

3.30 Another argument in favour of the 'release of ID data' model may lie in the business needs of SAs. Some SAs may have a need to know all of a client's registered names to prevent duplication and potential 'double dipping'. If so, however, this argument has not been clearly articulated to date. If it is the only convincing reason for the proposed model this should be clearly stated. This would then have implications for presentation of the authentication scheme as a neutral resource.

3.31 The design of the scheme clearly seeks to avoid any suggestion that it is in any way an eligibility checking system. It does this by confining itself to storing only a very limited set of ID data, and no information about individuals' relationships with particular Service Agencies. In the proposed model, individual Service Agencies are responsible for making decisions about eligibility or liability, based on their own business rules and relevant statutory criteria, once they have verified an individual's identity with the AA.

3.32 However, if SA rules require Credential holders to authorise release of all registered names, then it has been suggested[100] that this clearly gives the AA database additional functionality – a role in eligibility checking - which should be recognised in public presentations of its character.

3.33 If on the other hand there are no SAs which would mount this argument in favour of releasing information, then serious consideration should be given to the alternative 'confirmation only' model.

Recommendation 3. Consideration should be given to varying the design so as to allow simple confirmation of the validity of a client name, rather than only release of all registered alternate names.

Freedom of choice and Universality – a population register?

3.34 One of the key assumptions in the recommended authentication model is an 'opt-in' principle' – that "members of the public should be able to choose whether or not they want to access services that require authentication over the Internet."[101] This has been translated into one of the Policy Principles for online authentication approved by Cabinet in April 2002.[102]

3.35 It is however difficult to see how the authentication system could sustain the opt-in principle even in the short term.

3.36 Firstly, given the officially sanctioned trend towards e-government, it is inevitable that many categories of government clients will come under significant pressure to transact on-line, and therefore to obtain an ID Credential to allow them to do so. Government agencies will increasingly offer incentives to convert to on-line transactions, and alternative service channels will become less available over time as the take up of on-line services increases. Even if the letter of the commitment is honoured, and alternative channels continue to be available, off-line users will increasingly be placed at a disadvantage, at least in terms of convenience if not cost. This is not to necessarily criticise such trends, which are in many cases inevitable, but merely to encourage public acknowledgement that they are likely, and have consequences for the opt-in principle.

3.37 One of the factors that will influence perceptions of whether the scheme is genuinely 'voluntary' will be the strategies adopted both by individual agencies and at an all-of-government level to promoting registration. If there is a pro-active campaign to get clients to apply for ID Credentials, then there will be a greater perception of it being a register than if the facility is simply advertised as an option, for individuals to take up if and when they find it convenient. This will in turn depend partly on the financial basis of the scheme – see under *Funding/charging* below. If specific levels of registration are required to make the scheme financially viable, there will be a temptation to pro-actively promote it.

[100] Discussions with the Office of the Privacy Commissioner
[101] Design of online authentication for government: summary of recommended approach – July 2003
[102] Reported in Blueprint: Authentication for e-government, July 2003, p5

3.38 Secondly, one large category of initial users could be individuals in business roles who are required by their employers to obtain an ID credential so as to perform their duties (see *Individuals not roles* below). Experience around the world is that businesses and other non-individual entities, rather than consumers or citizens, have been the early adopters of online transactions with government.

3.39 Thirdly, most individuals needing to perform the role of Trusted Referees would be required to obtain an ID Credential[103]. It is argued that this is necessary so that the whole registration process can usually be completed on-line and for systems integrity, but these are not convincing arguments. The Business Process Design now accepts that there will need to be an off-line component to the registration process, and an exception process for Trusted Referees who do not have ID Credentials, but the intention remains for most Referees to already have a Credential.

3.40 It is also suggested that requiring individual Trusted Referees to have a credential could encourage friends and relatives of the applicants to apply[104]. While the logic of this is not clear, it reflects the clear intention to encourage registration.

3.41 Another factor that would undermine the opt-in principle would be any arrangements for parents or guardians to conduct transactions on behalf of minors or other 'dependent' clients. The scheme will issue ID credentials to minors who can produce adequate EOI, and who have the capacity to accept the terms and conditions, and it is easy to see how pressure will grow for many SAs dealing with minors and other 'dependent' clients to be able to identify the clients themselves as well as persons acting on their behalf. The current design of the Authentication scheme deliberately tries to avoid any recording of 'relationships' between Credential holders – leaving any such linkage to SAs. But this is a limitation which is already coming under pressure[105], and seems unlikely to survive in the medium term.

3.42 The difficulty of dealing with parental relationships is similar, but even more complicated, for persons acting on behalf of institutionalised individuals, including those in prisons, psychiatric institutions and senile dementia wards. They tend to have a power relationship greater than parents and guardians *in loco parentis*, and they commonly act on behalf of multiple individuals rather than just one or two children.

3.43 Whether the AA database is seen as the foundation of a population register will also depend partly on the details the way in which contact details are treated. The AA will need applicants' contact details during the registration process, and the Business Process Design currently anticipates using contact details subsequently to send confirmation of each Request for Verified Information (RVI), as a security measure. This implies indefinite storage of at least one contact item (phone or fax number or e-mail or postal address) However, they would soon become out of date for many individuals, given the level of mobility of the NZ population, unless steps are taken to encourage notification of changes. Making this a legal requirement would be the only way of ensuring a reasonable level of currency).

---

[103] The Trusted Referee Discussion Paper (V.0.2 8 October) suggests that the AA would pre-populate a database with accredited individual trusted referees (paras 20-21).
[104] Trusted Referee Discussion Paper (V.0.2 8 October) para 22.
[105] See Legal Issues Paper *How will minors obtain an ID Credential and associated Key?* Version 0.6 28 October 2003 – discussion of need for parental consent.

3.44 To the extent that contact details are kept up to date, then the value of the database for other purposes, the likelihood of function creep and its likely perception as a population register would all increase. Some SAs have already expressed interest in being notified by the AA of any changes to a Credential Holder's ID data, or at least being told that there had been changes, so that they could themselves ask the client. If no such services are intended, it would be preferable to consciously delete all contact information within a short time after a Credential confirmation had been issued, although this would mean abandoning the confirmation of RVI as a security measure (see also under IPP 4 - Security and IPP9 - Data retention).

3.45 It seems likely that it will be suggested that the scheme could offer an optional 'change of address' service, on the basis that this be convenient for consumers and efficient for both government and business. Any such 'add on' would pose great practical difficulties while at the same time posing a major privacy risk. It is clear from experience of such schemes that many individuals do not have a single set of contact details suitable for all purposes. Attempts to cope with the diversity and complexity of individuals' circumstances would be fraught with difficulty. At the same time the attraction to many organisations of a central store of updated contact details would inevitably lead to major 'function creep', potentially compromising the core identity authentication purpose of the scheme.

3.46 For all of the above reasons, it is likely that the Authentication scheme could easily be seen as the foundation of a universal population register[106]. To the extent that this could be an undesirable barrier to acceptance, very clear limits would need to be placed on the scheme. Alternatively, the government could choose to promote the advantages of a population register and argue that they outweigh any privacy and other risks.

Individuals not roles

3.47 The current design excludes role-based identities from the authentication system. This has both pro- and anti-privacy consequences. On the positive side, it means that the AA need not hold any information centrally about individual's various business or organisational roles. But on the negative side, it means that where an organisation *requires* its employees (or equivalents such as office holders) to obtain a Key to act on behalf of the organisation, they must provide *personal* details to the AA, even though they may have chosen not obtain a key in their personal capacity. This clearly compromises the 'opt-in' principle.

3.48 The Project Team take the view that there are many organisational contexts in which SAs do not actually need to identify individuals – only to authenticate authority to perform a certain role (eg: lodging official returns, authorising payments etc). Where this is the case, SAs should ideally be able to insist on client organisations carrying responsibility for any actions of authorised representatives, without needing to know their specific identities.

[106] The fact that not all New Zealanders would be registered, and that the AA would also register some non-nationals would not stop the main part of the database from forming a partial population register.

3.49 But it may be that there is a category of services where the client is an organisation, but the SA needs for various reasons to have a record of the specific person who took the action (legal requirements for individual civil or criminal liability, audit trails etc). Should such circumstances exist, it would be necessary for the individual to establish their identity to AA standards, which means giving the same basic set of personal ID data – there is no provision for the AA to issue a Credential to an organisational role.

3.50 The person requiring a Key in an organisational capacity could register with an organisational role as an unverified alternate name[107] (if the AA allowed this[108]), and using their business address for contact purposes (a superficially privacy enhancing feature), but there would be no option for them but to give the same basic ID data as if they were registering for personal use. Any individual wanting separate Keys for personal and organisational use would have no choice but to have both Keys associated with the one Credential, issued to them as an identified individual[109].

3.51 It would be helpful if SAs could provide input on how many of their potential on-line services would require authentication of individuals, even where playing an organisational role, as opposed to authentication of roles alone. None of the SAs interviewed for this PIA have provided information that they have yet considered the proposal at this level of detail.

3.52 The scheme design assumes that it will be up to either client organisations or SAs to manage the relationship between individuals and roles. It may be that authentication of roles, with or without a link to identifiable individuals, is the biggest area of application at least in the short to medium term, but this scheme does not set out to meet that need.

3.53 A related issue that needs to be addressed is the potential for discrimination against employees who wish to exercise their right not to hold an ID Credential, but whose employer requires them to do so to perform a business role. It needs to be ascertained whether action against an employee for refusing to register with the AA (up to and including dismissal) would be lawful under both anti-discrimination and employment law.

3.54 This potential problem will be even greater for clubs and associations, which may find it advantageous to interact electronically with government agencies. Each new round of office-bearers would find themselves forced to register with the AA as an accidental by-product of volunteering. Voluntary organisations already have difficulty getting people to take on positions of responsibility, and this could be yet another deterrent.

---

[107] Eg: Treasurer of XYZ club, or finance manager of ABC Ltd, although there may be legal liability issues surrounding any attempt to use such aliases.

[108] There will need to be some limits on what unverified names Credential Holder's can register, if only to avoid obscenities, but there is currently no intention to prevent the registration of non-offensive aliases. The question of whether two Credential Holders would be allowed to register the same alias is one of many that remain to be decided.

[109] It was noted in consultation that employers are resisting a requirement to use individual employees Keys to transact on behalf of their employer.

Recommendation 4. There should be further analysis of the demand for authentication of roles as opposed to individuals.

Pseudonymity

3.55 It is generally accepted that there are a range of transactions for which identification is not routinely required – the 'trust levels' analysis used by the cross-agency EOI project include a category of 'pseudonymous'transactions, which do not require identification but do require a means of contacting the person concerned[110].

3.56 Unfortunately, this is a somewhat narrow conception of pseudonymity which has led the Project Team to provide only a limited range of options in the design. An identifier that can be linked to the underlying entity only with considerable difficulty is commonly called a pseudonym.[111] Most of the project documentation uses pseudonymous transactions as synonymous with role based authentication[112]. Authentication of roles, as explained above, is seen as something that SAs can and should perform for themselves, and is not within the scope of the proposed scheme, which could more accurately be described as authentication of identity than simply authentication.[113]

3.57 In contrast, a broader analysis would recognise the potential for individuals to operate pseudonymously using personal aliases that are distinct from any particular organisational role and affiliation. The constraints that the preferred design has imposed on individuals' choice in this respect has already been discussed under the *One Individual, One Credential* heading above.

3.58 Partly in response to this issue, the design has been refined to allow some selective disclosure of ID data, so that not all SAs need obtain all of a Credential Holder's registered names in response to an RVI in all circumstances. But the practical effect of this element of choice will depend on the business rules of the SAs. It is important that the statutory framework re-inforces the Privacy Act principle of necessity (see under Collection - IPP 1 below), such that SAs can only require individuals to authorise release of multiple names and aliases where they can demonstrate that it is necessary, not just convenient.

Recommendation 5. The authorising legislation should require that service agencies expressly justify any requirement for clients to authorise release of all alternate names.

Disincentives to multiple Keys

3.59 While the scheme design allows for a Credential holder to have multiple Keys associated with their Credential, the process involved in associating a Key means that

[110] Draft Evidence of Identity Framework, v 0.2 10 September 2003, p4.
[111] In Roger Clarke's model, psesudonyms are a sub-set of a wider class of 'nyms' – see Clarke 1999 at http://www.anu.edu.au/people/Roger.Clarke/DV/AnPs and http://www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html
[112] Although one Discussion paper – Delivering Authenticated Services Online, v.0.6 5 November 2003 – includes a more sophisticated analysis.
[113] The IQA consultants support this narrow interpretation of pseudonymity by stating "Keys could potentially be pseudonymous, ie not bound to any identity record at the AA" Source: IQA paper.

it will be easier for most individuals to make do with only one Key, using it even for unrelated transactions where it would be preferable, for both security and privacy reasons, to have separate Keys. Inertia and convenience will lead most individuals to settle for a single Key.

Recommendation 6. Publicity for the scheme should clearly outline the option of multiple keys and explain the privacy advantages.

Identity cards

3.60 The Summary of Recommended Approach[114] includes a key assumption endorsed by Cabinet, that "the model does not require a national identity card …". This could be seen as a misleading assurance if, in practice, either the Credential confirmation or a token issued by a KP containing an individual's Key come to be required to be produced in a wide range of circumstances.

3.61 One difficulty faced by this analysis is the uncertainty surrounding the likely range and take-up of Key types, and their provision by independent Key Providers. The flexibility of the scheme design in accepting a wide range of Keys is admirable in many respects. But is does mean that there is the potential for the emergence of Keys involving tokens, perhaps in the form of a card, as a significant component of the scheme. There are pressures for individuals to hold a documentary form of identification for a range of different purposes – these are currently met to varying degrees by passports, driver licences, health cards, credit and bank cards, the HANZ 18+ card etc. There will be obvious attractions to one or more 'issuers' of EOI to offer a multi-function card, perhaps including a Key which could then be associated with an individual's AA issued ID credential. [115]

3.62 One of the main reasons for resistance to an official Identity Card is the presentation of at least some ID data on the face of the card, which leads to demands for its production in more and more settings. This PIA is not the place to debate fully the pros and cons of Identity Cards. To satisfy the Cabinet requirement, the project design has carefully avoided the need for any card or token that includes ID data on its face. But the PIA must warn about the potential for Cards to emerge alongside the scheme.

3.63 The best way of dealing with fears that the authentication scheme may lead to an Identity card is for the authorising legislation to expressly rule it out, with statutory prohibition, or at least strict limitation, of physical cards or documents containing *both* an Individual's Credential confirmation number or Key Serial Numbers, *and* any of the ID data.

[114] Design of online authentication for government: summary of recommended approach – July 2003

[115] Both the Hong Kong government Smart Identity Card (SMARTIC), about to be rolled out, and the proposed Queensland government 'smart' driver licence provide multi-functionality, including the option of a digital signature/certificate. Both schemes have been/are controversial on privacy grounds, although the introduction of the Hong Kong SMARTIC has been made easier by the population's familiarity with an existing ID card. Recent proposals for an Identity Card in the UK are also very controversial.

Recommendation 7. The authorising legislation should prohibit the production of cards or documents containing both Credential confirmation numbers or Key Serial Numbers and any ID data.

Biometrics

3.64 The enhanced role of photographs in the design[116] raises several privacy issues. One of the initial design assumptions endorsed by Cabinet was that the model does not require "the exchange of biometric data at the time of transaction"[117] It is not clear whether this was intended to mean at the time of service delivery, or included the transactions involved in registration and association of Keys. The overall impression created, although perhaps not intended, may have been that biometrics would play little or no part in the scheme.

3.65 – Biometrics raise significant privacy concerns, not just because of the personal information they involve, but also because of the intrusiveness of collection. The NZ Customs Service, which is now chairing an inter-agency forum on biometrics, has issued a useful briefing paper which identifies the privacy implications[118]. There are also analyses of the issue, and recommendations, from various privacy regulators.[119]

3.66 A photographic image is a form of biometric, particularly where it is to be subjected to automated analysis such as face recognition software. The scheme will need to publicly acknowledge, and justify, the inclusion of biometric information.

3.67 Early versions of the design assumed that the photograph submitted by an applicant would be transformed into a biometric template, and that it would be possible to destroy the photograph after the registration process was completed. It would be impossible to re-construct a visual image from the template. This would be an admirable privacy-enhancing feature in that it would remove any possibility of subsequent pressure for use by other agencies, and would clearly demonstrate the limited value of the scheme as a population register.

3.68 A feature of the proposal that has recently emerged is the use of photographic images during the registration process for one-to-many matching, i.e. for identification rather than for identity authentication. The purpose of this would be to detect individuals seeking to register more than one identity. It is important to note that little evidence exists that one-to-many matching is a feasible technique, whether conducted manually or using so-called 'facial recognition' technology[120].

---

[116] There was little or no mention of a photograph in the early documentation, but it has emerged and become more significant as the design has evolved.
[117] Blueprint: Authentication for e-government, July 2003
[118] NZ Customs Service *Biometrics Briefing Paper*, June 2003. See also http://www.customs.govt.nz/about/news/biometrics+110903.asp.
[119] European Data Protection Commissioners – Article 29 Working Party Working Document on biometrics, adopted 1 August 2003 – see http://europa.eu.int/comm/internal_market/privacy/index_en.htm. The Australian Privacy Commissioner has also written on the subject – see http://www.privacy.gov.au/news/speeches/sp80notes.htm
[120] DIA claim high levels of success with face-recognition technology, including in one-to-many matching, but no detailed published evidence appears to be available. See also footnotes 120 & 121

3.69 If this approach were adopted, then the volumes are likely to be such that it would be necessary to automate the process. The automated matching can be performed using templates alone. Assuming manual checks will need to be performed in order to deal with the inevitable large numbers of false positive matches, access to the original full photographic image will be necessary. There may be other alternatives, e.g. to require all applicants to re-apply with another photograph and keep doing so until the resulting biometric does not match an existing record[121]. But not only would this be highly inconvenient, it could also embody an unwarranted assumption of fraudulent intent.

3.70 A current design assumption is that Credential holders would need to periodically renew their registration, with a new photograph. This requirement, which clearly adds significantly to the cost, intrusion and inconvenience to all registered individuals, would appear to rest partly on the known degradation in the reliability of facial recognition as people age; partly on the need for periodic 'proof of life'; and partly the need to combat the ever-increasing skills of hackers and forgers. The overall pros and cons of retaining photographs or biometrics derived from them have not been set out in detail.

Recommendation 8. Further consideration should be given to the overall costs and benefits of retaining the biometric template and/or the photographic image itself.

3.71 If the AA needs to retain the original photographic image indefinitely for the operation of the authentication scheme, the possibility of use by other agencies arises. A range of agencies could mount a case for clients to submit to a comparison of their current appearance with either the full digital image or the biometric template held by the Authentication Agency[122]. While this is not envisaged in the design, if it happened, it would clearly undermine the design assumption "no biometric data to be exchanged at the time of transaction". This is an area of potential function creep which will need to be addressed by both assurances and firm safeguards.

3.72 It is observed that there are strict limits on access to existing driver licence photos held by the LTSA, with even law enforcement agencies needing a warrant, and a purpose related to road traffic offences, to obtain access. (See discussion of access controls under IPPs 10 & 11 – Use and Disclosure, below).

Recommendation 9. The authorising legislation should expressly limit the purposes for which the photograph, digital image or biometric of the image can be used.

3.73 Reliance on face recognition technology to match photographic images raises the issue of the accuracy and reliability of the technology. There are very different opinions about this, and unfortunately little empirical evidence and few dispassionate commentaries. There is general agreement that one-to-one matching is significantly easier than one-to-many, but very different views as to such variables as the false

[121] See Biometrics Discussion Paper, v 0.3 9 October 2003, 3.6 para 39

[122] DIA notes that there has been no such pressure from other agencies for use of the photographs held in the Passport system, but we suggest that greater awareness of face recognition capability, and the perception that the AA is a common service for all-of-government would make such pressure much more likely in the future.

acceptance and false rejection rates, quality of image and conditions required, and decay of matching accuracy with elapsed time since the image was taken.

3.74 In some jurisdictions, face recognition technology has been embraced enthusiastically – trials are under way at Australian airports[123] and the NZ Passports processing system is at the leading edge of the technology – more than 2.5 million photographs have been digitally encoded based on the bone structure of the face, and are used to match against renewal applications, with high levels of accuracy claimed[124]. In contrast, some applications in the US have recently been abandoned, allegedly due to poor accuracy and limited effectiveness.[125] Despite doubts, it should be noted that New Zealand is playing a leading role in responding to a US government requirement for a biometric of a digital image for passport holders from 27 visa-waiver countries by October 2004.

3.75 Nevertheless, even small error rates would create significant difficulties with a large applicant population. There are also practical issues concerning individuals who for religious or other reasons wish to keep their face partially covered. The scheme needs to be able to respond convincingly to questions about how face recognition errors will be handled without either inconveniencing individuals, unreasonably discriminating against minorities or destroying trust and confidence in the system.

Recommendation 10. Before any further commitment is made to the scheme, a detailed analysis of the role of the photo/biometric should be carried out, addressing the reasonable doubts about the accuracy and reliability of face recognition technology and the practical difficulties that will arise.

3.76 Other biometrics, such as iris recognition or hand geometry may offer higher levels of accuracy than face recognition from photos, but are not yet as readily available or affordable, and have significant disadvantages in terms of acceptability, typically requiring a more intrusive scanning process. The project team are not currently considering the use of any biometric other than one based on photographic images. Any departure from this position would raise significant additional privacy issues.

Recommendation 11. There should be a clear commitment that the scheme will not develop to involve any other biometric without separate legislative authorisation following a full privacy impact assessment.

Government uses only?

3.77 The scheme has been variously described as 'authentication for e-government', and 'all of government authentication'. This may have been used as a re-assurance as to the limited scope of the proposal, and to differentiate it from agency-specific

[123] Trials of 'Smartgate' by Australian Customs at Sydney airport – although the government has claimed success for these trials, no results have been published and there has been critical media coverage.
[124] Interviews with DIA Identity Services Division personnel.
[125] eg: trials in the City of Tampa, Florida, and at Logan airport in Boston have reportedly been abandoned. See http://www.aclu.org/news/2001/n010302a.html and Sydney Morning Herald 23 August 2003 and http://www.usatoday.com/usatonline/20030902/5460651s.htm (both sites accessed 24 November 2003)

schemes. However, it seems clear that the scheme is likely to involve use by the private sector, at least for those functions which the private sector performs on behalf of government (eg financial transactions reporting (money laundering) and income reporting). There is also likely to be private sector involvement in the scheme through outsourcing – this is discussed separately below (paragraphs 3.200-3.205)

3.78 It is also very likely that private sector organisations will seek to take advantage of the new system to replace existing commonplace reliance on existing forms of government ID – drivers licence, passport etc. Project documentation to date has only hinted at private sector use – it needs to be more open and either accept that the scheme is likely to be used widely by the private sector, or specify limits and how they will be enforced. If private sector use is anticipated, the scheme should avoid using descriptions, or terms such as "All of government (AOG) ID credential" which could be seen as misleading.

Recommendation 12. The authorising legislation should clearly specify limits on the scope of the authentication scheme.

Other issues concerning identifiers

3.79 A privacy enhancing features of the current design is that it allows for individuals holding a username/password Key to choose their own username, which need not be unique. There will be some centrally set standards for username/password pairs, but provided these allow for individuals to use their 'common' name, the scheme will have avoided a major perceived failing of some identification systems which force users to add characters to their name to achieve uniqueness[126].

3.80 A possible adverse consequence could arise from the assignment of a unique Credential serial number to each ID Credential (which means each registered natural person); and a unique Key Serial Number to each Key. The scheme design seeks to minimise the risk of the ID Credential serial number becoming an identifier by reserving it for use within the Authentication Agency. Neither the individual nor any SA or KP will have any need to record the Credential serial number. It is very important that this feature be confirmed in the authorising legislation.

Recommendation 13. The authorising legislation should reserve the Credential serial number for use only by the Authentication Agency for internal administrative purposes.

3.81 In contrast, Key Serial Numbers will be exchanged between the AA, SAs and KPs. While it is understood that individual Key Holders will have no need to record, or even know, the serial number of their Key(s)[127], there is a risk that the Key Serial Number could become a de-facto personal identifier, unless organisations are specifically precluded from using it in this way[128]. For most individuals who will only

[126] Doubts have been raised about whether username/password systems can allow for identical usernames – this needs to be resolved before this can be promoted as a positive feature.
[127] The question of whether Credential Holders would be entitled to obtain the Key Serial Number(s) (and their Credential serial number) under the Access Principle of the Privacy Act is discussed below.
[128] See also paragraph 3.151 concerning the possibility of having multiple Key Serial Numbers for each Key.

ever hold one Key, the risk is greater, but even for those who hold multiple Keys, each one will uniquely identify the Holder. Allowing multiple Keys avoids a one-to-one link between Key and Credential, but does not address this problem. The Unique Identifier Principle (IPP12) in the Privacy Act, discussed below (see paragraphs 3.121-3.132), may serve to limit this risk, but for technical reasons is not currently a sufficient safeguard, and will require amendment to fulfil this role[129].

3.82 A similar risk arises from the issue of a Credential confirmation notice to each Credential Holder. Depending on what information this notice contains, it too could become a de facto ID document. If it is to be sent by different channels (post, email, SMS) at the Holder's choice, this risk will be lessened, as only a proportion of Holders will have a standardised written confirmation. It will nevertheless be necessary to proscribe the use of the confirmation notice or reference number as an Identifier, either directly in the legislation or by ensuring that Information Privacy Principle 12 applies to it.

Recommendation 14. The authorising legislation should proscribe the use of any Credential confirmation notice or administrative reference number issued by the Authentication Agency by other organisations as an identifier.

Issues arising from 'failed' transactions

3.83 It is inevitable that automated systems applying business rules will lead to rejection of some transactions, including applications for Credentials and Keys, attempts to associate a Key with a Credential, and subsequent authorisations of RVI. There will also be at least occasional technical failures. Mention has already been made of the unproven accuracy of face recognition technology, particularly in relation to one-to-many matches.

3.84 An important issue will be what the individuals affected by rejections or failures are told, and what opportunity they will be given to resolve the problems arising. This is partly a data quality issue (see under IPP 8), and partly one of use and disclosure (IPPs 10 & 11) if rejections lead to actions such as referral for investigation[130].

3.85 If individuals lose their only Key, they may have to re-present at an AA shopfront with evidence of having a Credential, in order to have their identity verified and a new Key associated with the Credential[131]. If they have also lost their Credential confirmation notice, the shopfront may be able to find the appropriate customer record by searching on ID data items[132]. A Credential holder who still has at least one associated Key will be able to associate other Keys more easily – although either a face to face encounter or a challenge-response process would probably be required.

---

[129] In the Australian federal Privacy scheme, there is both a general unique identifier principle and a specific set of controls on the use of the tax file number.

[130] There should be clear criteria for referral eg: will the AA be informed of any failed attempt to associate a new Key, or to authorise an RVI.

[131] Consideration is being given to a challenge-response process to avoid the need for this requirement

[132] The question of what access to the AA database the shopfronts would require has yet to be specified, and involves security considerations.

3.86 An acceptable set of rights and administrative remedies will be required to deal with errors and system failures. These should include reasons for decisions, in sufficient detail to enable the individual to understand them and work out what steps to take; a hold on administrative action; internal review and appeal rights to an external Review body; with the prospect of meaningful remedies, including payment of compensation for loss and damage including distress and inconvenience.

Recommendation 15. Before any further commitment is made to the scheme, analysis of all the possible points of failure, and how they will be addressed, should be carried out.

Issues arising from choice of agency to perform Authentication Agency role

3.87 The identity of the Authentication Agency will have a bearing on the nature and strength of some privacy issues.

3.88 Independence of the AA has already been recognised as very important, although it begs the question independence from what? – a host agency?, SAs?, the government of the day? etc. The perception will be different with different agencies under consideration – eg: the Births Deaths and Marriages (BDM) Registry (within Identity Services Division of DIA) has a clearly related purpose but there may be problems of perception given the openness of the births register (the opposite image from the high security required for authentication).

3.89 Passports (also within DIA ISD) is clearly a service delivery affecting only a sub-set of the population, as is driver licencing (LTSA). This could be seen as inappropriate linkage to 'end-uses' of the authentication system. Both could also be seen as having an unfortunate association with identity cards (drivers licences more so given their common usage in community as ID, and strong links to law enforcement in the context of road traffic offences). Other operational agencies would inevitably be seen as a self-interested end-users with negative associations – no amount of re-assurance would dispel the impression that authentication was assisting with their other functions.

3.90 A new agency entirely separate from any existing government entity would best satisfy the objective of independence, but has been ruled out as inconsistent with recent government policy on structure of government.[133]

3.91 The next best option is a statutory function with a separate independent 'registrar' within an existing agency (the BDM model). Arguments put in favour of locating the AA within the Identity Services Division of DIA[134], and the DIA responses, are convincing – this appears to be the best fit of any existing Department or agency. Notwithstanding the possible perceptions referred to above, public consultation in April 2003 identified DIA as an agency that the public *would* be comfortable to have as an Authentication Agency.

3.92 However, if the AA is to be located within DIA or any other agency, the authorising legislation should clearly specify the parameters that ensure

[133] See Review of the Centre papers on SSC website http://wwwssc.govt.nz
[134] Preliminary Authentication Agency Analysis v 0.4 18 August

independence, such as terms and appointment of a 'registrar', reporting – preferably directly to Parliament, etc. It would also be essential for staff of the AA, if they are employees of an agency with wider functions, to be subject to confidentiality provisions relating specifically to the AA functions. This would be to avoid any suggestion that 'wearing another hat' they could access or use AA data for other purposes.

Recommendation 16. The authorising legislation should clearly establish the Authentication Agency as an independent function with appropriate status, structure and accountability.

Issues arising from funding models

3.93 Funding arrangements for the authentication scheme have yet to be specified. Options clearly include central funding of the infrastructure and administration of the scheme, or a user-pays model, in which Service Agencies and/or individuals pay for their use of the system. To the extent that SAs have to pay for their use of the system, this could either be funded by additional resources or have to be met out of existing budgets or compensating savings elsewhere. If there is any suggestion of private sector contribution to funding (a partnership approach), the question would arise what would they gain in return. Given that the authentication scheme could be seen as 'critical infrastructure', it may be desirable to expressly rule out private sector funding.

3.94 While the funding arrangements have no direct implications for privacy, they will of course influence the uptake and usage of the scheme, thereby indirectly affecting the scope and universality of the system. A model which cost individuals little or nothing to obtain a Credential and associate a Key would encourage registration, while appropriate funding arrangements for SAs could encourage them to adopt the central all-of-government authentication system as a supplement or alternative to their own authentication initiatives.

Recommendation 17. Further privacy impact assessment should be undertaken once the details of the proposed funding model are clear and design work has progressed.

Privacy Act Compliance

Introduction

3.95 The purpose of this section of the PIA is not to identify in detail how the agencies involved would comply with their obligations under the Privacy Act, including the Information Privacy Principles (IPPs). It is to identify any broad areas of difficulty or special issues that might be encountered in so complying.

3.96 The Privacy Act primarily deals with 'information privacy'.[135] Other dimensions of privacy, such as privacy of the person (e.g. concerns about capture of biometrics including photographs), privacy of behaviour (e.g. tracking of people's activities across multiple walks of life), and privacy of communications – some of which have been discussed above - are not regulated by the Privacy Act[136]. This section accordingly only addresses those aspects of privacy that are currently subject to express statutory regulation. It also does not encompass any aspects of the common law that may be relevant, such as the law of breach of confidence and the tort of passing off.

3.97 Where possible, issues of compliance with the Privacy Act IPPs and other issues are dealt with separately for the AA and SAs. In some cases, compliance and other issues arise from the interface between the AA and an SA, and it is necessary to deal with these issues in an integrated way.

3.98 It should be noted that there are a number of ways in which conduct that is not in accordance with the IPPs can still be lawful. These include waivers granted by the Privacy Commissioner either under a Code of Practice (s.46) or under a specific authorisation (s.54) (Conditions apply to both); or specific statutory authority, which overrides some of the IPPs (s.7). Where a difficulty in otherwise complying with an IPP is identified below, the appropriateness and likelihood of one of these 'overrides' is discussed.

3.99 In the health field, the *Health Information Privacy Rules* (HIPRs) in the *Health Information Privacy Code 1994*[137] substitute for the default *Information Privacy Principles*. The brief for this PIA did not extent to reviewing how compliance with the Rules might differ from compliance with the Principles in relation to the use of authentication in health applications. This will be the responsibility of any health agency that is subject to the Rules.

3.100 Similarly, some businesses in the telecommunications industry are now subject to the *Telecommunications Information Privacy Code*, issued by the Privacy Commissioner in May 2003. For these businesses, the *Information Privacy Principles* are replaced by the *Telecommunications Information Privacy Rules* (TIPRs). While Service Agencies and the proposed Authentication Agency are not likely to be

[135] also known as data protection
[136] although the Privacy Commisisoner has some functions in relation to these wider issues – Privacy Act, s.13.
[137] As amended – there have been several amendments to the Code since it was first issued, most recently in 2000.

affected by this Code, some Key Providers may be[138]. Key providers may also be subject to relevant provisions in Telecommunications law, which will apply to the telecommunications businesses whose facilities will be used by the scheme.

3.101 It must be recognised that commitments to comply with Privacy Act[139] are not necessarily what they seem, as the IPPs (or HIPRs or TIPRs) can always be overridden by other statutory changes – in which case the action in question is still compliant with Privacy Act even though the practical effect is reversed.

3.102 The public is likely to assume that statements by Ministers and agencies that a new scheme will comply with privacy legislation means that the Principles will be applied; whereas what those statements may actually mean is that the scheme will take full advantage of the available exemptions and exceptions, and may even create new ones, which render the Principles irrelevant.

3.103 Public acceptance of the scheme may therefore be dependent upon carefully expressed statements, which avoid misleading the public about what protections do and do not apply.

Recommendation 18. Public presentation of the scheme needs to be careful in explaining the issue of compliance with privacy laws, and what this means.

Personal Information involved

3.104 The main category of persons about whom the AA will collect and hold personal information is individuals applying for an ID Credential (Registration). Personal information held will include the ID data, administration data (including contact details and the photograph and biometric template), the Credential Number and the Key serial numbers of any associated Keys. Further information will be held about the subsequent transactions of Credential holders.

3.105 Since any Credential Holder over 18 can act as a Trusted Referee, there is no need for the AA to pre-identify TRs as such, although the AA's records will show which Credential Holders have acted as TR for one or more other Holders.

3.106 The AA will of course also hold employee records and administrative records containing personal information, but in these respects the AA would be no different from other government agencies – all of which must comply with the Privacy Act in respect of such records. No further consideration is given in this PIA to such records.

Collection (IPPs 1-4)

Justification

3.107 The AA's collection of personal information about registrants will clearly be for a lawful purpose connected with a function or activity of the agency (IPP1(a))[140].

[138] Other Codes issued by the Commissioner deal with specific issues and should not be relevant to this scheme

[139] See Implementation Principle – Legal compliance

[140] It is assumed that the operation of the scheme is consistent with the Bill of Rights Act – at least one agency consulted asked this in the wider context of the constitutionality of the scheme.

Provided the collection of all items of personal information can be justified it will also comply with IPP 1(b) (necessary for that purpose).

3.108 It will however be necessary for the AA to justify the collection of all the types of information it requires for registration. The current scheme is likely to use the EOI framework being developed by an inter-agency committee[141], but as discussed above under the '*One Individual, One Credential*' heading, it has not yet been adequately demonstrated that that framework is soundly based conceptually, or that all of its elements are necessary.

3.109 The AA will collect personal information directly from individuals registering for the issue of an ID Credential (see project description above). Direct collection is the preferred option under IPP2.

3.110 Personal information about registrants will also be collected by the AA from third party trusted referees. Collection from third parties is an 'exception' to IPP 2 which is permitted under certain conditions - there will be multiple bases for this (eg: authorisation by individual (b); necessary for … (d); avoid prejudice to purpose (e)).

3.111 It is assumed that all SAs will also be able to justify the collection of personal information about clients registering for on-line transactions, and the collection of personal information about those clients from the AA, and from other Key Providers, both during First Time Service Registration, and during Service Delivery, satisfying both IPP1 and IPP2.

3.112 The draft EOI framework requires information sufficient to pass five tests (see paragraph 2.17). While the AA may need to apply all five tests (subject to the issue of multiple identities discussed above), SAs may *not* need to apply to tests of Objective A (identity not claimed before) and of E ('evidence of the use of the [claimed] identity in the community'), as they will often only need to satisfy themselves that the identity exists and that the client links to it (tests of Objectives B & C), which they should be able to do by checking the validity and currency of a Key presented by a registered client. This should result in SAs needing to collect relatively little personal information (in the form of EOI) for many transactions.

Notification

3.113 Where personal information is obtained directly from registrants, the AA will have the opportunity to meet its notification obligation under IPP 3, and should also take this opportunity to explain the role of the trusted referee and the information flows involved in the scheme.

3.114 A comprehensive 'package' of information to registrants may also serve to satisfy at least some of the IPP3 obligations of SAs in relation to their subsequent use of the scheme and of Identity keys.

3.115 Individuals will need to be reminded at appropriate points in the various transactions about what is happening to their personal information. This is particularly important in the context of a Common Logon Site, or of other

[141] Draft Principles for Evidence of Identity and Draft EOI framework, 10 September 2003

arrangements for seamless multiple transactions from within a single Internet session. The desire for 'efficiency' reasons to hide the actual nature of the transactions will need to be balanced against Privacy Act obligations to be transparent.

Other collection issues

3.116 The AA will keep records of transactions involving its records – notably of requests from SAs for verification. These will progressively accumulate into a very comprehensive database of some of the interactions with government of individual Key Holders[142], and with any private sector organisations which are authorised to use the services of the AA. This information about the subsequent transactions, even though it arises from an RVI authorised by an individual, is clearly not collected directly from the individual and is arguably not even collected from the SA – it is internally generated by the AA. The main implications of this data arise in relation to retention (IPP 9) and use and disclosure (IPPs 10 & 11), discussed below.

3.117 The AA should have no difficulty satisfying IPP 4 in relation to both registration and transaction information – collection by lawful means that are fair and do not unreasonably intrude; assuming the overall scheme justification is accepted, and provided there are clearly no less intrusive means of implementing it.

3.118 One specific collection issue relates to Māori stakeholders. The work programme's Tikanga strand has recognised a need to assess whether there is a widespread view that government agencies should not collect or store whakapapa and, if appropriate, ensuring that whakapapa is not included directly in the authentication model[143]. However, the requirements for evidence of identity (EOI) during registration, for example for Māori, will need to be culturally sensitive.

3.119 If any of the transactions between individuals and the other parties (AA, SAs or Key Providers) involved multiple on-line sessions, then the issues of 'cookies' arises. Many Internet users are suspicious of the use of cookies, which a web-site server places on a user's computer to allow sessions to be linked and previously collected or stored information to be retrieved for re-use. Some users deliberately block the placement of cookies on their computers, and for many users accessing the Internet from their place of work the cookies may be blocked by the corporate firewall. It is not yet clear if cookies would be required – there may be alternative ways of providing the required functionality with appropriate security (see under IPP 4 below). If cookies are to be required (and this can be justified in terms of IPP1), the AA will need to ensure that this is transparent to users, both in its privacy policy and in explanations to users who attempt to use the AA site with cookies disabled.

3.120 A further consideration in relation to cookies is that many circumstances would arise in which an individual would start a session on one workstation and complete it on another. Examples include; start at home but finish at work, start at work but finish at home, start in one workstation in an Internet café or library and finish on

[142] Although only at the level of contact with an agency, with no details of the service sought or provided. Nevertheless, it will often be possible to infer other information from the fact and timing of the contact.
[143] Authentication Project: Policy Work Programme (Phase 1) V.0.1 21 July 2003, paragraph 14.

another workstation in that or another Internet café or library. The design cannot therefore depend on cookies in order to enable continuation of a suspended session.

Unique Identifiers (IPP 12)

3.121 The Unique Identifier (UI) Principle (IPP12) is obviously directly relevant.

3.122 A threshold question is whether the ID Credential (the basic data set explained in the Project Description) is a UI as defined in the Act[144] While the combined effect of the data set is to 'uniquely identify' an individual (at least to a very high level of probability), the set contains the individual's name, which is expressly excluded from the definition of UI. The preferable meaning of this is that name alone cannot be a UI – but the ID Credential including a name can be and is a UI. The rest of this analysis proceeds on this assumption.

3.123 It is also arguable whether Keys themselves (eg: username/password pairs or digital certificates) will be UIs. While a Key associated with a Credential will 'uniquely identify' that individual Credential Holder in the sense that the Key Provider will have associated it with a specified person, it fails another part of the test in the definition – it need not uniquely identify the person *in relation to [the assigning] agency*[145] (*emphasis added*). Also, where a Key is issued by a third party Key Provider, it is not assigned 'for the purposes of the operations of [that] agency'[146] – rather it is assigned for the purpose of use with other agencies unrelated to the Key Provider.

3.124 However, the ID Credential serial number, and any serial numbers assigned to Keys in accordance with AA standards will, under the current design, all be 'unique identifiers' under the Privacy Act. The fact that an individual may have more than one Key and therefore more than one Key serial number will not prevent each one 'uniquely identifying' that individual.

3.125 The 1998 Review of the Privacy Act identified two issues in relation to the operation of IPP 12. The first is the meaning of 'assign' and the second is whether the Principle should apply to identifiers assigned by the private sector (it does at present).

3.126 The first issue raises some doubt about whether an ID Credential serial number or Key serial number would be a UI in the hands of *any* user which merely records that number, or only in the hands of a user which utilises the number to refer to an individual. It would be useful if this could be clarified in any amending legislation, preferably to ensure that the numbers are brought within the scope of IPP12 – see below for reasons why amendments will be required in any case in relation to this Principle.

3.127 The second issue is also relevant, as IPP 12(2) may interfere with the ability of the AA to lawfully record a Key issued by another Key Provider against an individual's Credential. The Privacy Commissioner recommended in 1998 that IPP

[144] PA s.2 Interpretation of 'Unique Identifier'
[145] Part (b) of the definition
[146] Part (a) of the definition

12(2) be limited to government-issued identifiers, with a specific discretion to be able to extend the controls to specific private sector identifiers through a Code of Practice if the need arose[147]. However, the design of this scheme intentionally uses a range of private sector issued Keys as identifiers, which may suggest that IPP 12 (suitably amended) should apply to both government-issued and private-issued Keys.

3.128 The intention of IPP 12 is precisely to limit the development and use of multi-function unique identifiers (UIs) without appropriate authority[148]. The AA should be able to meet this principle since its entire (statutory) purpose will be the assignment and management of identifiers; i.e. the scheme quite precisely sets out to stimulate the use of multi-function identifiers; but it will be expressly authorised by law. In particular a central mission of the AA should satisfy IPP 12(3) – reasonable steps to assign UIs only to individuals whose identity is clearly established. However, any breakdown in the scheme or administrative failure that resulted in incorrect assignment of Identity credentials or of Keys could demonstrate a breach of IPP 12(3).

3.129 Under the proposed design, the ID Credential number assigned and held by the AA is never recorded by any other agency. But both SAs and the AA will record the serial number assigned to a particular Key by the Key Provider.

3.130 The *use* of Key Serial Numbers by SAs will have to satisfy IPP12. The proposed model involves SAs assigning persons' Keys (issued by the Key Providers) to their own customers, presumably using Key Serial Numbers, which will be UIs.[149]. This would only be permitted by IPP 12(2) if the SAs were 'associated persons' under the Income Tax Act - they are not. Therefore, either specific statutory authority[150], or a Privacy Commissioner issued Code of Practice[151] or authorisation[152] will be required to override IPP 12(2).

3.131 It would be invidious to expect a Privacy Commissioner to be the instrument of relaxing the UI Principle in the context of a major national authentication scheme. Authorisation should therefore be given by means of express statutory provision. This clear need for amendment of the Privacy Act will however have to be publicly justified in terms of the commitment in the Legal Compliance Implementation Principle to 'comply with relevant law, including privacy .. law'[153].

---

[147] Necessary and Desirable, Review of the Privacy Act 1993, March 1998, Recommendation 28
[148] See discussion in Necessary and Desirable, Review of the Privacy Act 1993, March 1998, paragraphs 2.14.5-2.14.7
[149] Assuming association of a Key Serial Number with a client record *for the purposes of the SA (emphasis added)* is held to be an 'assignment' under IPP 12. Interpretation of this provision by the OPC to date has been that mere recording of another (first) agency's UI, or even its use only for the original purpose of its assignment, does not constitute assignment by the second agency. It could be argued that an SA would only be recording a Key Serial Number for the purposes for which that serial number had been assigned.
[150] thereby invoking s.7(4) – an action is not a breach of …[IPP 12] if that action is authorised by or under law.
[151] PA s.46
[152] PA s.54
[153] Blueprint: Authentication for e-government, July 2003, p6.

3.132 The 1998 Review of the Privacy Act recommended amendment of s.66 to make a wilful breach of IPP 12(2) an 'interference with privacy' irrespective of the absence of any harm or detriment[154]. On the assumption that statutory amendments will authorise the use of Key Serial Numbers by SAs which would otherwise breach IPP 12(2), it might be appropriate to revisit this recommendation, so that any wilful use by an organisation *not* expressly permitted to use Keys would be a breach, thereby invoking the civil law remedies under the Privacy Act.

Recommendation 19. Legislation should clarify the application of the Unique Identifier Principle (UIP- Principle 12) of the Privacy Act to the various identifiers and numbers involved in the scheme. Existing issues about the application of the UIP should be resolved at the same time, after consultation with the Privacy Commissioner.

Storage and security (IPP 5)

3.133 It has not been possible to make a sufficiently detailed assessment of security issues because the process design for the scheme is not yet sufficiently fully articulated, nor stable. In particular, the concept of a *Centralised Authentication Hub* or *common log-on site* (see paragraphs 2.50 and 2.65) has only been developed towards the end of this assessment, and this has major implications for security and privacy. It is not clear that risk assessments have been performed across the full range of circumstances that will arise, and hence it is not clear that the security requirements for communications between the parties and for stored data have been established. In these circumstances, the comments provided in this section are of necessity preliminary only. It is very important that all the as-yet-unresolved security matters be kept under review.

3.134 IPP 5 requires agencies to protect personal information against loss, unauthorised access etc, and other misuse with security safeguards that are reasonable in the circumstances. Security will of course also be required for other reasons such as to ensure the integrity, functionality and availability of the systems involved. Often, the level of security required for these other reasons is at least equivalent to, or exceeds, what is required to safeguard privacy. But this cannot be assumed, as in various circumstances, compliance with this privacy principle can require additional safeguards.

3.135 The NZ Government addresses the confidentiality, integrity and availability of all official information through the *Security in the Government Sector* policy. This includes *Minimum Standards for Internet Security in the NZ Government*. The EGU have issued more specific advice in *Online Authentication - Internet Security*

3.136 Guidance on security from a specific privacy perspective is available from the Australian Federal Privacy Commissioner[155]. This refers to three relevant NZ standards:

• AS/NZS ISO/IEC 17799:2001 Information technology - Code of practice for information security management

[154] Harm or detriment is usually required before a breach of an IPP becomes an actionable 'interference with privacy'. PA s. 66 (1)(b).

[155] http://www.privacy.gov.au/publications/IS6_01.html

• AS/NZS 7799.2:2000 (Previously known as 4444.2) Information security management - Specification for information security management systems
• AS/NZS 4360:1999 Risk management

3.137 Many other text-books and technical publications provide guidance on these matters.[156] In view of the extreme sensitivity of the operation of the scheme, and of the information stored and transmitted, it is essential that the highest information security standards be applied to the scheme's design, construction and operation. On the basis of the documents available during the period in which the PIA was conducted, it is far from clear that the project had met those expectations. As the relevant documents become available, it is vital that they be carefully assessed from both the security and privacy perspectives.

Security of information flows

3.138 The scheme design provides that all information exchanges between AA and SAs (and Trusted Referee agencies) would use the NZ government secure network (SEE), with server to server encryption. It is understood that exchanges between Key Providers and both the AA and SAs would be required to use similar security. However, it is not clear from the SEE site[157] what mechanism is used, or proposed to be used, to achieve server-to-server security. Hence it is not clear that this vital issue has yet been addressed within the proposed design. It is very important that all the as-yet-unresolved security matters be kept under review.

3.139 Internet transactions between individuals and Trusted Referees, the AA and SAs would utilise Secure Sockets Layer (SSL), which provides encryption of messages passing between the client software on the workstation (generally thought of as being a web-browser) and the servers running applications for the relevant agencies. The possibility of telephone transactions has been raised recently (see for example paragraph 2.59), and this would raise an entirely new set of security issues, which cannot be assessed either for security or privacy implications without further detail.

Security of information within workstations

3.140 Individuals will use workstations within agencies for some purposes, and for others will utilise workstations in their homes, their workplaces, and public places such as libraries and Internet cafes. Workstation operating systems and applications are inherently insecure, and despite this having finally become a matter for discussion in the media, and despite public undertakings recently given by some vendors, that situation is unlikely to change in the short-to-medium term.

3.141 It is therefore critical that the scheme's design include:
- in relation to the public use of workstations made available by agencies - risk assessment and risk management measures to address the security risks; and

[156] See in particular Clarke R. (2001) *Introduction to Information Security*, at http://www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html especially sections 2 and 3, and Appendices 1 and 3; and the many texts and leading articles identified in the Bibliography to that paper.
[157] at http://www.e-government.govt.nz/see/index.asp

- in relation to public use of other workstations, risk assessment - to the extent practicable risk management measures, and public warnings and advice about the risks involved and how to manage them.

It is not clear that this vital issue has yet been addressed within the proposed design. It is very important that all the as-yet-unresolved security matters be kept under review.

Security of information within servers

3.142 All agencies participating in the scheme, and to the extent that Key Providers are corporations private sector participants as well, will store a considerable amount of sensitive personal data. This data is attractive to both insiders and outsiders. There are various threats, including:

- accidental disclosure;
- intentional access by an authorised user, but for unauthorised purposes;
- intentional access by an unauthorised user, by means of an authorised username and password pair; and
- intentional access by an unauthorised user, by means of circumvention of the access control mechanism, e.g. physical or logical break-in / cracking / hacking.

3.143 All parties to the system need to implement appropriate measures to ensure that the data that they store is protected by security measures commensurate with the sensitivity of the data involved. SAs hold personal data of varying sensitivity. The AA would hold data of the most extreme sensitivity, including all name variants, recorded aliases and at least some kinds of contact information. The KPs would hold personal data of varying degrees of sensitivity, but also identification data associated with the Key which is of highly sensitive.

3.144 It is therefore critical that the scheme's design include:

- in respect of the AA, risk assessment and risk management measures to address the security risks; and
- in respect of SAs and KPs, guidance in relation to the risk assessment and risk management measures that are needed in order to address the security risks.

It is not clear that this vital issue has been adequately addressed within the proposed design. It is very important that the as-yet-unresolved security matters be kept under review.

Security of personal data stored by Trusted Referees

3.145 TRs may also hold data of considerable sensitivity. It is not clear that risk assessment has been performed, and that the security requirements for data storage by these parties have been established. The organisations and individuals would be highly diverse in their size, and in their professionalism in matters of data storage and data security. Moreover, many of them may prove to be difficult to influence in relation to their data practices.

Security of data used in discontinuous sessions

3.146 If, as proposed, the registration process can be discontinuous; ie: spread over time or over several on-line sessions, a security issue arises over authorising the applicant to return and pick up a partially completed process, which will inevitably include personal information lodged at a previous stage. The scheme proposes to address this issue partly through the use of additional 'shared secrets' eg: temporary

passwords or access codes issued to applicants to allow them to return and complete a process. However, shared secrets are a relatively low-security device, and a detailed analysis will be required of the threat that this might pose to the integrity of the system. This is one of many ways in which the scheme, unless very carefully designed, would be likely to contribute to the risk of identity fraud rather than reducing it.

Security of Keys stored by agencies

3.147 In the case of digital signature key pairs it is not necessary for the Key Provider to record the private key, and indeed essential that it does not for security reasons.

3.148 In the case of username/password, the Key Provider, unless they are also an SA conducting transactions with the Key holder, may not need to record the password, and might be satisfied with a hash (mathematical transformation) of it (see privacy analysis below). This protects against the risks of a workstation being used by an officer of the agency, or by a person who gains access to the stored password, in order to masquerade as the individual. (It does not protect against simulation by transmitting the hashed password in a stream of traffic purporting to come from a workstation).

3.149 Under the proposed scheme, the same Key is to be used for authorising the AA to release the holder's ID credential and as a log-on ID for Service agencies. This will inevitably give rise to security concerns as the Key Serial Number will need to be stored in multiple agencies and locations, thereby increasing its exposure and vulnerability. This is a serious privacy concern, because the Key Serial Number is at risk of becoming used as a general-purpose identifier, which would enable correlation of personal data from many sources.

3.150 A further vulnerability may exist. The design documents are far from clear as to the use of the Key Serial Number by the AA and by the SAs. There is a possibility that anyone gaining unauthorised access to another individual's Key Serial Number could use it as a means of masquerading as that person in relation to a range of government services. If such a vulnerability exists, then the impostor might also be able to authorise release of the 'real' person's ID Credential, potentially allowing the impostor to commit identity theft.

3.151 A comprehensive assessment of the privacy impact of this aspect of the design cannot yet be performed. It is critical that this matter be carefully re-assessed when the design is complete and stable. One possible solution would be to provide for the use of a Key to generate a different Key Serial Number for different agencies; ie: there would be multiple KSNs for each Key.

Recommendation 20. Consideration should be given to varying the design such that the use of the same Key with different agencies would result in the issue of a different Key Serial Number.

3.152 The design provides for Confirmation of a Request for Verified Information (RVI) to be sent to the Credential holder concerned by a separate channel from that used for the RVI transaction itself. This is a security measure in that it provides some

assurance that unauthorised RVIs will be detected, but it also requires contact details to be kept - see paragraph 3.43.

Security of personal data and Keys held by individuals

3.153 Individuals who participate in the scheme are required to store data. This includes one or more Keys.

3.154 The security considerations arising in relation to the storage of Keys depends on what kind of Key they are.

3.155 In the case of a Username and Password, the Username does not have to be kept secret, but the Password has to be, because capture of the Password combined with capture, interpolation or guessing of the Username is sufficient to enable a third party to masquerade as the individual.

3.156 The scheme envisages that individuals would be permitted to change Passwords to a string that they can remember, but there appears to be no requirement to avoid easily-discovered passwords, such as those uncovered through dictionary attacks. In any case, it is not clear to what extent the scheme will be able to impose standards on all Key Providers.

3.157 In the case of a digital signature regime, it is critical that the private key be only ever accessible by, and only ever able to be invoked by, the Key holder. This has implications for key-generation, for the storage location of the key, for the physical protections for the storage location and the key, and for the software protection for the key. The IQA Interim Report 2 acknowledges a further aspect of the risks involved: "In the event that the user has two or more keys, then their data at the AA and their SAs will be as secure as the security of their weakest key".

3.158 It is not clear that risk assessments of the various circumstances have been performed, and hence it is not clear that the security requirements for data storage by individuals have been established. Still less does it appear that the practicalities of large numbers of people possessing and protecting highly sensitive data have been appreciated and addressed. It is very important that all the as-yet-unresolved security matters be kept under review.

Recommendation 21. A comprehensive and continuing security review and risk assessment should be undertaken to address the many security issues as yet unresolved.

Access and Correction (IPPs 6 & 7)

3.159 It is assumed that the AA will either be subject to the Privacy Act or to equivalent access and correction rights[158]. The existing withholding grounds (Part IV) and procedural provisions (Part V) will presumably apply, and the former should accommodate all the countervailing public and private interests.

[158] The Privacy Act only allows requests for access or correction (information privacy requests) to be made by NZ citizens and permanent residents or by others while physically in New Zealand (Privacy Act s.34). To ensure equity, either the legislation authorising the scheme, or an amendment to the Privacy Act, should extend these rights to all Credential Holders, wherever they are located.

Recommendation 22. Legislation should amend the Privacy Act to grant all Credential Holders, wherever they are located, the same rights under that Act.

3.160 One issue that will need to be resolved is whether any part of the information held by the AA and/or SAs will be exempt from access on security grounds (eg: serial numbers). Ideally, the scheme should be completely transparent and allow individuals to know/see all numbers or labels assigned to them. While any withholding of information would inevitably fuel suspicion, there may be overriding security arguments for not disclosing some details (see under IPP 5). There are currently no grounds under ss.27-29 which would obviously meet this need, and it seems likely that express statutory authority (invoking s.7) would be required.[159]).

3.161 Another issue to be resolved is the appropriate balance between the privacy of Credential holders (or applicants) and of Trusted Referees in the event that a person making an access request wanted to know what had been said about them in the context of a declined application.[160]

Recommendation 23. Legislation should specify any additional grounds for withholding Authentication Agency information in response to access requests needed to ensure adequate security, and to protect the privacy interests of third parties.

Data quality (IPP 8)

3.162 Data quality will be a primary concern/function of the AA for operational reasons. While the AA should have no difficulty in showing that it is *attempting* to take reasonable steps to ensure accuracy etc, objectively achieving adequate data quality will be a major and continuing challenge.

3.163 One issue will be how the AA deals with unavailable or unknown identity facts – eg: birth dates/places, or with individuals who for various reasons are unable to produce EOI to meet the normal standards[161]. To what extent will the AA be given discretion to assign credentials on a 'best endeavours' or 'near enough' basis, and what are the implications of this for the integrity and security of the scheme overall?

3.164 Initial registration relies to a large extent on checks against other databases. The IQA consultants have identified as an issue the quality of the data in those databases, and the PIA consultant's own experience of matching programs suggests that there will be some significant problems arising from the use of data collected for one purpose in one context for an entirely different purpose/context.

3.165 The scheme will also have to be able to deal with changes to the items of ID data for a Credential holder. Individuals can lawfully adopt multiple names, and change not only their name(s) but also their gender, and both date and place of birth

[159] Privacy Act s.30 implies that a Privacy Commissioner Code of Practice or s.54 authorisation would not suffice.
[160] Exemptions (a) and (b) in s.29 are relevant, as may be s.27 (1)(c) if refusal of an application had led to law enforcement activity.
[161] For instance it is understood that the Department of Immigration has assigned common birth dates to some refugees. Many other people may have no documentary evidence of date or place of birth.

may need to be corrected on the production of new evidence. All such changes create difficulties for a scheme which presumes that each person has a unique and unchangeable set of ID data, and also opens up opportunities for illicit manipulation of the database in connection with Identity theft or fraud. The project will need to specify in some detail what rules it will apply to changes of ID data to provide re-assurance not only that genuine changes can be accommodated, but also that the risk of unauthorised changes can be managed.

3.166 Another data quality issue is the quality of photographic images and their use – despite the claims of technology providers, there is considerable doubt about the reliability and accuracy of face recognition systems. The government will have to show that the use of photographs in the proposed system can reach acceptable levels of accuracy and reliability, avoiding too many incorrect acceptances and erroneous rejections (false positives and negatives) (see discussion under *Biometrics* above).

3.167 Any automated system encounters issues around acceptable levels of data quality. At every stage of processing, there are likely to be criteria and thresholds of acceptability (for example, see data validation stage of Registration in the project description above). There is always a balance to be struck between setting criteria too tight, leading to rejections and inconvenience, and setting them too loose, compromising quality, integrity and security.

3.168 Accepting that automated systems applying business rules will lead to rejection of some transactions, including applications for Credentials and Keys, an important issue will be what the individuals concerned are told, and what opportunity they will be given to resolve the problem – perhaps by correcting or clarifying the information they have provided. (An associated issue of referral for investigation is discussed under the heading of the Use and Disclosure Principles) (See also discussion under *Issues arising from 'failed' transactions* above, and *Accountability mechanisms and safeguards* below.)

Data retention (IPP 9)

3.169 Data retention will be a significant privacy issue. The best privacy protection is often destruction of information, although this sometimes has to be balanced against the contribution that data retention can make to security. There is inevitable conflict between the tendency of historians to seek retention and accessibility of everything, and the privacy interest of individuals in suppression and destruction. The government agencies involved in the scheme will be bound by the *Archives Act 1957* – a preliminary appraisal is under way with National Archives assistance but is not yet available.

3.170 The AA would keep personal information collected for registration indefinitely. It is proposed that the data set forming the ID Credential, once recorded, would be permanent, to ensure uniqueness, and to ensure that any associated Key(s), once issued, are never assigned to another individual, and to ensure future non-repudiation of a 'past' identity, and of past transactions by a particular identity. A record could be 'de-activated' if Keys were revoked or otherwise withdrawn (due to death of holder, compromise etc), but would never be deleted.

3.171 The permanence of the AA records could contribute to fears of the surveillance and control implications of the scheme. While it would be easy to satisfy the letter of IPP 9 by specifying indefinite storage in the authorising statute; justifying the need for permanence, and balancing it with an appropriate range of safeguards, will be an important part of the communication strategy for the project.

3.172 Of particular concern is the retention of the transaction information. The record of checks against the AA database will build up into a comprehensive, if superficial, profile of an individual's on-line transactions[162]. While there is a case for retention of these records, in the form of a log or audit trail, for systems integrity and auditing purposes, there will inevitably be pressure for access to the data for a range of other purposes, including law enforcement, revenue protection etc (see below under IPP 11). The longer the data is retained the more that pressure will grow and the more likely it is that the data will be accessed for these secondary purposes. The scheme needs to specify, and justify, retention periods for transaction information.

3.173 A further practical issue is the extent to which records will be kept of partial or failed applications that do not result in the issue of a Credential, or the binding of a Key to a Credential. There will no doubt be arguments in favour of retention of all such information for security purposes – particularly for subsequent analysis of fraud attempt etc. On the other hand, such records could accumulate into quite detailed patterns of activity by particular individuals which, whilst of little or no value to the Authentication scheme, could be of intelligence value to other authorities. If records of incomplete transactions were to be retained, then there must be clear justification for it, and appropriate controls on access to them.

Recommendation 24. The authorising legislation should set the parameters for retention of various categories of data held in connection with the scheme.

Use and Disclosure (IPPs 10 & 11)

3.174 The project design and documentation to date emphasise the role of consent, and this could be the basis of compliance both by the AA and SAs with IPPs 10 (exception (b)) & 11 – (exception (d)) – 'authorised by the individual concerned'. However, great care should be taken to avoid the inappropriate use of the word 'consent' in circumstances where an individual has no real choice but to authorise a particular use or disclosure. See the discussion above about the credibility of the 'opt-in' principle under the heading '*Universality – a population register*?'.

3.175 It would be preferable for the basis of use and disclosure of personal information in the authentication scheme to be clearly set out in law as part of the authorising legislation. This would avoid any uncertainty about the way in which the various exceptions to IPPs 10 and 11 would be interpreted in relation to the scheme. This in turn would allow the scheme to be promoted publicly with firm and unequivocal assurances as to the way in which the scheme would operate, and equally importantly what would *not* be permitted.

3.176 It is important that the provisions authorising use of information are clear about when a use becomes a disclosure – releases of information should not escape controls

[162] See paragraph 3.116.

applying to inter-agency transfers just because they are to unrelated parts of the same agency (intra-agency) and therefore technically a 'use' rather than a 'disclosure'.

3.177 A detailed regime for use and disclosure in the statute authorising the scheme would effectively supercede IPPs 10 and 11[163]. There would be increased risk to public support for the scheme for every aspect of the new regime that is weaker than the existing one. The authorising legislation would need to ensure that a new use and disclosure regime, even if 'tougher' than the IPPs, did not have the effect of denying individuals access to the remedies available for 'interferences with privacy' under the Privacy Act.

Use and Disclosure of Registration information and of Credential data

3.178 There should be specific authority for all of the uses and disclosures of information necessary for the operation of the scheme (once they have all been identified). This authority would need to cover the information exchanges between the various participants – individuals; the AA; SAs; Key Providers, and Trusted Referees (including other databases (see under *Information Matching* below).

3.179 A strictly limited range of exceptions for other public interests (such as emergencies, law enforcement etc) should be specified, with appropriate safeguards. While these would provide for some of the interests allowed for in the exceptions to IPPs 10 & 11, they could do so in a much more rigorous and certain manner. All other uses and disclosures should be expressly prohibited. It is not acceptable in relation to this scheme for additional uses to be founded on an individual's consent where this is extracted effectively under duress, and is not free as well as informed. .

3.180 The possibility of criminal penalties for breaches of these rules should be considered[164] rather than simply civil remedies as in the Privacy Act, to reflect the importance of public confidence in the scheme – see paragraphs 3.224-3.225.

Use and Disclosure of revocation/suspension lists

3.181 This is a sub-set of the previous category – a form of operational use, but with external consequences. Presumably, any attempted use of the scheme by an SA which found that either the Credential or the Key in question was invalid would prompt some form of action or investigation[165]. Clear criteria and guidelines need to be established for any such action, given the potential consequences for individuals (including denial of identity; allegations of Identity fraud or theft, criminal investigation etc) (see also *Issues arising from 'failed' transactions* above).

3.182 As with transaction information (discussed below), there would also need to be clear and specific rules about access by third parties for purposes not directly associated with the operation of the authentication system, with very high standards of justification required.

[163] Privacy Act s.7
[164] The penalties applying to various Identity Services functions within DIA provide a precedent.
[165] It is intended that there be some tolerance built in to the system eg: for a limited number of attempts to enter a password.

Use and Disclosure of transaction information

3.183 There should be specific authority for the allowable uses of the AA's transaction records during their lifetime (see retention discussion under IPP 9) – uses/disclosures both by the AA itself, and the permitted circumstances, conditions and other safeguards for third party access (such as for law enforcement).

3.184 Another category of third party access that may need to be allowed, subject to conditions, may be access by SAs in relation to their own use of the scheme, such as for reconciliation of audit trails, or in relation to specific investigations – any such access should be restricted to transactions involving the SA in question, but even this should not be an unconditional right.

Use and Disclosure of information for law enforcement purposes

3.185 Distinctions need to be drawn firstly between law enforcement purposes connected with the operation of the authentication system (eg: investigation of identity theft or fraud) and other unrelated investigations; and secondly between purposes connected with specific investigations and speculative or intelligence purposes. Ideally there should be a hierarchy of access, with use or disclosure for investigation of abuse of the authentication being easier than for the other purposes, and intelligence uses being the most strictly controlled.

3.186 Assuming that the scheme will be governed by detailed statutory authority, a tiered approach to law enforcement access could be built in.

Use of information for statistical purposes

3.187 Cabinet has acknowledged, as one of the Māori issues raised during consultations, the need to explore the implications of protecting authentication data so that it cannot be used for statistical purposes (for example, to publicise Māori take-up of online authentication).

3.188 Use of information for statistical purposes, for most non-Māori, need not be a major privacy issue provided it involves the use of aggregate data, in such a way that information about identifiable individuals is not released (although it may be used in the course of analysis to link records). A minority of non-Māori are concerned about the 'autonomy' aspects of such uses, and together with Māori specific concerns this justifies a detailed consideration and specification of the statistical uses, if any, of AA data which will be allowed, and the controls that will apply to any such uses. Statistical expertise will be required for such a consideration.

Recommendation 25. The authorising legislation should set out a detailed regime for use and disclosure of personal information held in connection with the scheme, dealing with:

- ***The distinction between use and disclosure in this context.***
- ***Limits on who can access information, for what purposes, in what circumstances and subject to what conditions.***
- ***Specific limits and conditions in relation to different categories of data, such as registration information, transaction information, and revocation/suspension data.***

- ***A distinction between uses and disclosures directly associated with the operation of the scheme (including investigation of suspected ID fraud or theft) and those for other secondary purposes unrelated to the scheme.***

Information matching (Part 10)

3.189 The Information matching provisions of the Privacy Act (Part 10 and Schedules 3 & 4) do not automatically apply to all matching. Matching programmes have to be expressly prescribed (and the relevant provisions listed in Schedule 3) in order to come under Part 10.

3.190 On the face of it, the definition of information matching programme[166] also limits the coverage of Part 10 – some one-to-many verifications would not constitute matching programmes, and other many-to-many matches would not be covered because they would not be "for the purpose of producing or verifying information that *may* be used for the purpose of taking adverse action" (*emphasis added*).

3.191 But most of the provisions of Part 10 do not use the term 'information matching programme'. Instead, they apply to 'authorised information matching programme(s)'- a term which is separately defined without either of the two limiting conditions that apply to 'information matching programme'.

3.192 Many of the information exchanges involved in the operation of the proposed Authentication scheme fall outside the more limited definition, but could nonetheless be covered by Part 10 if they were 'authorised'.

3.193 For instance all of the following, if done in real time in relation to a particular individual, may be one-to-many; and would also not have any overt intention of taking adverse action[167]:

- checks between the AA and other databases as part of the processing of an application for a Credential;
- checks by an SA with Key Providers on the validity of a Key; and
- the RVI process whereby an SA accesses ID data for a client from the AA.

But they are all capable of being subject to Part 10 if an 'Information Matching Provision' in another law makes them into 'authorised information matching programmes'.

3.194 A government decision will be required as to whether any or all of the interactions involved in the operation of the Online Authentication system are prescribed as 'authorised information matching programmes' for the purposes of the Privacy Act. It seems likely that the government would wish to either bring them under the scope of Part 10, since this is expressly designed to offer additional privacy safeguards to deal with the perceived risks arising from matching; or alternatively provide similar but customized safeguards and oversight in other legislation.

3.195 It may be that as well as prescribing certain matching programmes for authorised but controlled operation under Part 10, or otherwise providing similar

[166] Privacy Act s.97

[167] Although almost any matching, even if it is primarily directed to positive outcomes, could nonetheless be seen as having adverse consequences, where, for instance, someone was found to be ineligible for a benefit or assistance.

safeguards; the government would also wish to expressly prohibit or proscribe certain other matching. For example, it may be important for public acceptability of the scheme to expressly rule out use of the transaction information as an intelligence database – for instance to draw links between transactions with other government agencies and tax liability. On the other hand, there may be some intelligence matching which would be seen as having a higher priority than the protection of privacy – such as in the context of terrorism.[168] If some such matching against the new records to be held by the AA are envisaged, they should at least be subject to the additional protections of Part 10, if not more specifically regulated.

3.196 What should be avoided is leaving any information matching involving personal information held by the AA outside the scope of Part 10 and regulated only by the general IPPs. Matching of AA data should either be specifically authorised, or prohibited.

3.197 An important issue is whether any prescription (or conversely proscription) of specified information matching programmes should be part of the package of legislation enabling the AA and the Authentication scheme. If not, and it is left to separate legislation relating to SAs enacted on a different timetable and subject to future variation, that may fuel fears of function creep and/or loss of safeguards.

3.198 A specific requirement of any information matching programme prescribed for the purposes of the Privacy Act, bringing it under Part 10, is that any on-line transfers of information have to be expressly approved by the Privacy Commissioner.[169] Since nearly all of the information transfers in the authentication scheme are expressly designed to be on-line, approval by the Commissioner of any that fell within Part 10 could be assumed once the scheme was authorised by law[170].

3.199 If any of the interactions involved in the operation of the Online Authentication system are prescribed as 'authorised information matching programmes' for the purposes of the Privacy Act, resources and time would need to be allowed for the procedural requirements of Part 10 and the Information Matching Rules. If controls are introduced via separate legislation, there will still be a similar administrative cost.

Recommendation 26. The authorising legislation should clearly prescribe relevant information exchanges as 'authorised information matching programmes' for the purposes of the Privacy Act, Part 10. It may also be desirable to impose additional controls on some of the information exchanges involved, and to expressly prohibit certain other exchanges . The Privacy Commissioner should be consulted about the appropriate level of control.

Outsourcing

3.200 Outsourcing has always been a controversial subject from a privacy perspective. While compliance with privacy standards can be written into outsourcing contracts,

[168] There is however a widespread belief that terrorism prevention and detection is being used in many jurisdictions as a convenient but unjustified excuse for extensions of the powers of some law enforcement and intelligence agencies.
[169] Privacy Act, Fourth Schedule – Information Matching Rules – Rule 3.
[170] Although the Commissioner may well seek to impose conditions – Privacy Act, Fourth Schedule, Rule 3(2).

there is a widespread public perception, based partly on some well-publicised failures, that contracting out involves a loss of control and accountability. Individuals have certain rights when dealing with agencies, but those rights do not always extend to dealings between the individuals and the outsourced service providers. Most governments have acknowledged this issue by drawing the line at certain sensitive functions which they have required to be conducted 'in-house' by public servants.

3.201 A decision will be required as to whether the AA functions include ones which are so sensitive that they should not be performed by contractors. From a privacy perspective, such a decision would be appropriate, at least in respect of some aspects of the scheme.

3.202 An extra dimension to this issue is whether, even if outsourcing is considered appropriate and defensible in principle, it should nevertheless not be performed overseas – see the discussion below on cross border issues. In New Zealand, the Privacy Commissioner has found it necessary to issue a Code of Practice to specifically cover the overseas transfer implications of privatisation and subsequent contracting of government data processing services.[171]

3.203 It seems likely that the AA will use agents for some parts of the registration process – eg: application; trusted referee 'vouching', delivery of Credential confirmations. This gives rise to an issue of responsibility for compliance with Privacy Act IPPs, acceptance of liability etc. The AA will be presumably be responsible for accrediting agents and for monitoring and periodic review of standards, but it is essential that there should be no ambiguity or uncertainty about who is responsible and accountable. The scheme design and authorising legislation should ensure that individuals' rights in relation to access, correction and redress are not compromised by such outsourcing.

3.204 Key Providers will not be providing an AA service, but they will have to meet AA standards for their Keys to be accepted for use in the scheme, and their participation should be covered by some form of agreement or contract.

3.205 Contracts or agreements between all participants in the scheme will need to include express, and enforceable, provisions relating to responsibility for privacy, security and liability, including compliance with the Information Privacy Principles.

Recommendation 27. An express decision should be made as to the extent to which outsourcing of any information handling involved in the scheme will be allowed. Legislation should ensure that individuals' rights and accountability are not lost or compromised as a result of any such outsourcing.

Cross border issues – Transborder data flows

3.206 The issue of information transfers outside New Zealand will arise in both AA registration and SA use, in relation to persons seeking to transact from overseas, including overseas resident Trusted Referees.

[171] EDS Information Privacy Code 1997, expired 30 June 2003 (replaced with undertakings from the contractor).

3.207 While NZ agencies remain responsible for personal information they hold outside the country[172], there is otherwise no specific trans-border provision in the Privacy Act at present. One has been recommended by the Privacy Commissioner in order to achieve adequacy assessment by the European Union EU under their Data Protection laws[173], and it is understood that the Government has accepted in principle the need for such an amendment. If such a requirement is introduced it is likely to be similar to NPP9 in Australian Privacy Act 1988 – organisations must take reasonable steps to ensure that similar protection applies in any jurisdiction to which they transfer personal information. This can be satisfied (under the Australian principle) either by the consent of the individual concerned, by the existence of an equivalent law or other scheme in the destination jurisdiction; or by contract terms.

3.208 NZ agencies already have to comply with a similar though more limited requirement under IPP 5 in relation to security (IPP 5(b)), which is usually met by contract terms – eg: with outsourcing service providers – or by MoUs with foreign government agencies. The way in which the cross border transfer implications of contracted-out government data processing has already been mentioned under the Outsourcing heading above[174]. The Privacy Commissioner has also been consulted about other overseas transfers.

Recommendation 28. Apart from the specific recommendations outlined in this section, agencies involved in the scheme will need to ensure that they comply with the Information Privacy Principles (or equivalent rules under Codes of Practice), taking account of the issues raised above under each Principle.

Accountability mechanisms & safeguards

Internal complaint handling, dispute resolution and audit

3.209 Whatever arrangements are made for external oversight (see below), there would be an expectation that the agencies concerned would attempt to resolve complaints themselves at first instance (internal review).[175] To ensure that this was effective, protocols would be needed between SAs, the AA and KPs to clarify responsibility for handling complaints involving authentication. For instance, many complaints about eligibility for or denial of service by an SA may involve an element that relates to alleged errors in the transaction between the SA and the AA, and/or alleged errors in the original verification of identity by the AA. It would be important to ensure that such complaints did not fall between the gaps, with the SA, KP and AA all declining to accept responsibility. To guard against this possibility, an effective external review mechanism (see below) should have the power to rule on where responsibility lay.

3.210 The AA and SAs should be expected to include the operation of the Authentication system into their internal audit programs.

---

[172] Privacy Act s.10
[173] Necessary and Desirable, Review of the Privacy Act 1993, March 1998, Recommendation 35(a)
[174] see footnote 165
[175] The need for this is recognised by the Project Team – see paper *Identification of a Review Body* version 1.1 31 October 2003, paragraph 24.

Recommendation 29. Agencies involved in the scheme must be required to have appropriate internal complaint handling; dispute resolution and internal audit processes, and to enter into protocols with other parties to ensure complaints do not fall between gaps.

External audit and review

3.211 Existing review mechanisms including the Privacy Commissioner and the Ombudsmen will apply unless excluded by statute[176]. Many complaints about operations of AA are likely to fall within the Privacy Act jurisdiction[177]. However, because of exemptions and exceptions in the Privacy Act not all errors or grievances arising from the operation of the scheme are guaranteed to be covered. Some work has been done on this but it is important that a detailed analysis be performed of all the possible grounds for complaint, and where necessary, gaps in the availability of remedies should be plugged.

3.212 The Project Team's work has emphasised the similarities between the functions of the Privacy Commissioner and the Ombudsmen in relation to complaints handling. There are however some important differences.

3.213 One important distinction is that the Ombudsmen can only make recommendations about changes in administration, whereas the Human Rights Review Tribunal can award damages for interferences with privacy[178] under the Privacy Act[179].

3.214 Complaints about the authentication scheme may involve the actions of Trusted Referees and of Key Providers. Many TRs will be individuals and at least some KPs are likely to be private sector organisations. Both individuals and private sector organisations can be agencies under the Privacy Act, under the jurisdiction of the PC but they would not be within the Chief Ombudsman's jurisdiction, which is confined to the public sector. The Project Team consider that the AA would take responsibility for actions of private sector participants which related to the scheme, but this is not as reliable as ensuring that they are directly accountable to an external review body.

3.215 The Privacy Commissioner has somewhat wider functions in relation to promotion of awareness of privacy in specific contexts, rather than just awareness of complaint rights. If the Ombudsmen were to perform the role of Review Body, they would need additional functions in this area.

---

[176] The Project Team has also identified the Human Rights Commission jurisdiction. While important, this is not considered further in this paper, although some of the findings may be relevant.

[177] See paper *Identification of a Review Body* version 1.1 31 October 2003. The table at paragraph 22 of that paper underestimates the categories of complaint which would involve an Information Privacy Principle or Information Matching Provision.

[178] Interferences with privacy are breaches either of any of the IPPs, of provisions of a Public Register Code of Practice issued under s.63, or of the Information Matching provisions (Part X); which have an adverse effect on an individual (Privacy Act s.66)

[179] Privacy Act s.88

3.216 There is obvious potential for complaints about the actions of the AA, and of SAs and KPs in relation to their use of the AA, to fall between jurisdictions. The Privacy Act provides for referral of complaints from the Privacy Commissioner to the Ombudsmen[180], but a Protocol would be needed between the Privacy Commissioner and the Chief Ombudsman to clarify criteria for deciding jurisdiction.

3.217 While the Ombudsmen do not have a general pro-active auditing role, the Privacy Commissioner can undertake audits on request[181]; has a specific role of monitoring the use of unique identifiers[182], and has a significant program of pro-active monitoring of information matching, for which is has recruited staff with specific skills. The Auditor-General could conduct performance audits of Authentication Agency processes but would have no particular reason to give this area priority in the allocation of scarce resources, and might also face jurisdictional barriers in auditing processes involving individual Trusted Referees and private sector Key Providers. For these reasons the operation of a centralised all-of-government authentication scheme needs to be subject to regular independent external audit.

A new Review Body?

3.218 A new separate review body would have several advantages. It could assist in re-assuring the public that comprehensive oversight and remedies were being provided. It would provide a single clearly identifiable point to which complaints about any aspect of the Authentication system could be taken – it should not be left to the aggrieved citizens to have to decide which jurisdiction their complaint fell under[183]. Provision could also be made for financial compensation for non-privacy errors that resulted in significant harm or inconvenience. A separate body could also be given a pro-active audit role across all aspects of the authentication system. Finally, a specialised agency could develop expertise in the technical issues involved in the authentication scheme.

3.219 Against these advantages must be balanced a range of other factors including cost[184], agencies having to learn a new set of processes, and the fact that there would still be the potential for overlap at the margins, eg: where complaints involved actions of Service Agencies which were still subject to the Privacy Commissioner and Ombudsmen jurisdictions. A separate body would also differentiate electronic transactions, when the same accountabilities and processes should arguably apply whatever channels a person is using. Also, the creation of a wholly new body would run counter to government policy as expressed through the Review of the Centre[185].

---

[180] Privacy Act s.72

[181] Privacy Act s.13(1)(b)

[182] Privacy Act s.13(1)(c)

[183] Both the Privacy Commissioner and the Ombudsmen can require a complainant to have first taken an issue up with the agency concerned. This could generally apply to complaints about the authenticaton scheme, with complaints going first to the AA, and SA or a KP as appropriate, but only where responsibility was clear. It seems likely that in at least some situations it will not be clear which agency is responsible and one or more agencies must be prepared to take on a clearing house role. A new Review Body could readily perform this role.

[184] Estimated by the Project team to be significantly higher than the marginal costs of absorbing functions into existing agencies.

[185] see f/n 129

3.220 A hybrid approach would involve the creation of a new Authentication Review Body role, with clear jurisdiction over all participants in the Authentication system, and a customised set of functions, but to give this role to one of the existing external review bodies[186].

3.221 Several factors would suggest that this might be best placed in the Office of the Privacy Commissioner:

- The specific existing functions of monitoring the use of Unique Identifiers and Information Matching, directly relevant to this scheme, and for which it has recruited specific skills.
- The estimation (of this consultant) that most complaints about authentication will involve an Information Privacy Principle or Information Matching issue under the Privacy Act;
- The breadth of the Privacy Commissioner's jurisdiction covering public and private sector organisations and individuals, and
- The wider range of existing functions, covering all the likely requirements of a Authentication Review Body role.

3.222 If this solution was adopted, there would clearly still need to be protocols for referral of complaints to and from the Ombudsmen as appropriate.

3.223 Whatever decision is made about the location of the Review functions, it is desirable that this itself is reviewed within a set period after the scheme commences operation, in light of experience.

Recommendation 30. Authorising legislation should ensure that an independent review body has the necessary powers to provide coverage of all participants in the authentication scheme, and to perform both complaint adjudication and proactive monitoring roles.

Offences and penalties

3.224 The 'default' regime under the Privacy Act is for civil penalties in the form of potential awards of compensation by the Human Rights Review Tribunal. Several agencies consulted, including the Office of the Privacy Commissioner, have expressed the view that this would not provide an adequate deterrent against intentional abuse of of the authentication system. It would seem appropriate for there to be criminal penalties attaching to at least some such abuses. It may be that certain abuses would already be criminal offences under the general criminal law or computer crime legislation[187]. If not, or if the specification of those offences do not adequately cover the risks in the authentication system, then appropriate offences should be provided in the authorising legislation.

3.225 One specific abuse would be coercing an individual to make an information privacy (access) request under the Privacy Act with a view to fraudulent use of the

[186] At least one agency consulted raised the issue of liability in relation to the Review Body role, and in particular the different status of government departments, Crown entities (such as the Privacy Commissioner) and Officers of Parliament (the Ombudsmen).
[187] The new section 252 of the Crimes Act, which took effect from 1 October 2003, may be relevant

information obtained. This should be a criminal offence, as already recommended by the Privacy Commissioner[188].

Recommendation 31. The authorising legislation should provide for appropriate criminal offences and penalties over and above the civil penalty regime under the Privacy Act.

Staff training

3.226 There is no point in putting in place elaborate safeguards and accountability mechanisms if the employees concerned are not adequately trained to understand the risks and implement the safeguards. The legislation establishing the Authentication Agency should expressly provide for this as a function, and adequate resources must be provided to allow both initial and continuing training. The Authentication Agency should been given some responsibility for training employees of other participants in the authentication system (SA and KP employees and both organisational and individual TRs) in their specific responsibilities in relation to the operation of the system.

Recommendation 32. The authorising legislation should provide for a continuing staff training and education function, to extend to training of all participants in the authentication scheme.

Communications strategy

3.227 There will of course be a need for general community education about the new authentication scheme, and presumably one or more specific campaigns to promote registration. As part of any communication or advertising, the privacy implications need to be addressed, and not merely by way of token re-assurance. The specific privacy issues highlighted in this report should be expressly addressed and an explanation given as to how the scheme will deal with them. Misleading assurances about the effect of Privacy law need to be avoided.

3.228 The communications strategy for the scheme is already under way, and includes the public consultation in early 2003, subsequent announcements and public availability of some of the project documentation. The strategy will next need to deal with the decision making process of deciding if, and if so how, the scheme is to be implemented. A Cabinet decision is expected in March 2004. This Privacy Impact Assessment, together with the detailed Business Process Design and the Business Case should be made publicly available for comment and consideration before that decision.

3.229 Experience elsewhere has been that Privacy Impact Assessments, even where commissioned, have been kept from the public until after critical decisions have been made, fuelling suspicions about motives and function creep. Far better to expose the analysis of all benefits and costs, both financial and intangible, as early as possible so that a mature debate can be held about the overall public interest.

[188] Privacy Commissioner (1998) Necessary and Desirable: Privacy Act 1993 Review, paragraphs 12.18.6-12.18.18.

Recommendation 33. There should be clearly defined responsibility for a public communications strategy, to include publication of the justification for and merits of the scheme, its design specifications and this Privacy Impact Assessment, before a final decision is made to proceed, and continuing public education programme during implementation and operation.

Monitoring, Reporting and Periodic Review

3.230 The all-of-government authentication scheme is sufficiently important, as a piece of public infrastructure likely to directly affect a major and ever-growing section of the New Zealand population, to warrant close monitoring and periodic review.

3.231 The routine monitoring should be performed by someone independent of the scheme's operation (including the review body(ies), whose performance also needs to be monitored). This monitoring may be appropriately performed by the Controller and Auditor-General, perhaps on a specific reference, as well as in pursuance of his existing functions.

3.232 The legislation authorising the scheme should also provide for an appropriate mechanism to review any major changes to the scheme, such as additional functionality for the AA, increased information storage or exchange, or greater access to data for previously unauthorised purposes, whether or not those changes require legislative amendments[189].

3.233 The legislation should also stipulate at least an initial review after the scheme has been in operation for a number of years, to independently examine whether the scheme has met its objectives and honoured its commitments. Subsequent periodic reviews may also be desirable, to ensure that scope- and function-creep do not take place unnoticed or unremarked.

Recommendation 34. ***The authorising legislation should provide for ongoing independent monitoring and for periodic independent review of the scheme, and for a clear consultation and public decision making process for any subsequent significant changes.***

[189] Even if changes require legislative amendments, it may not be enough to rely on normal parliamentary processes – significant changes should be examined by a review committee representing a range of interests before the amendments are introduced.

Summary and Conclusions

Findings

4.0 It has proved difficult to assess the privacy implications of the proposed scheme due to the fluid state of the design. Many critical elements of the design remain to be fully articulated or are subject to change. This is not intended as a criticism – it is in fact commendable that a Privacy Impact Assessment has been commissioned before the design has been finalised. The lack of a stable design does however mean that the findings can only be provisional and to some extent speculative. To the extent that this leads to expressions of concern about privacy and security issues, this should be regarded positively in that this allows further decisions to be taken in full knowledge of the possible privacy and security implications, and hopefully for the design to be adapted to maximise privacy and security.

4.1 The NZ Government's approach to Online authentication seeks to minimise the adverse privacy consequences, while offering some advantages. Compared to many initiatives in other jurisdictions, the approach seeks to provide a pragmatic low-technology solution to a problem which is recognised, but not yet fully articulated or quantified. If it can hold to the foundation principles laid down by the government at the outset, it may be able to avoid the creation of an infrastructure for comprehensive surveillance of the general population that is a characteristic of the over-ambitious and costly solutions under consideration elsewhere.

4.2 Some features of the proposed scheme are particularly commendable from a privacy perspective, if they can be maintained. The limited information to be held by the AA; the requirement for Credential Holders to expressly authorise each release of ID data through the RVI process and, as far as it goes, the provision for alternate names are all privacy positive.

4.3 If carefully designed, and properly authorised by law, the proposed system should be able to operate consistently with the Privacy Act 1993, including its provisions relating to unique identifiers and information matching. Monitoring and review arrangements are proposed which should ensure continued attention to compliance with privacy principles and appropriate redress for individuals adversely affected by errors or misuse, but only if they are carried through in the authorising legislation.

4.4 However, mere compliance with privacy law does not in itself address all privacy concerns. In terms of the underlying concerns clearly identified in early consultations, some adverse privacy consequences are unavoidable, and will need to be balanced against the other advantages of the proposed system.

4.5 There are also significant doubts about whether the system as currently proposed *can* conform to the foundation principles, and avoid a progressive 'creep' in both scope and function that would significantly increase the risks to individuals' privacy.

4.6 The risks fall into a number of broad categories, some of which are inter-related:

4.7 The 'opt-in' principle, that participation be a matter of choice for individuals, is threatened in a number of ways, and it is doubtful if it can realistically be delivered in a meaningful way.

4.8 The likely attraction of the scheme to a wide range of government agencies, for authentication of both clients and employees, will almost certainly mean that a very large majority of the adult population will find it necessary to enrol.

4.9 The proposed use of digitally encoded photographs and face recognition analysis (biometrics) moves the scheme significantly towards an intrusive high tech solution that arguably already involves a departure from one of the design assumptions[190].

4.10 There will inevitably be pressures for the use of information stored for a specific limited purpose under the scheme (including biometrics, contact details and transaction information) for other government purposes. Unless expressly prohibited, some of these secondary uses would already be authorised by law and thereby also compliant with the Privacy Act.

4.11 There will inevitably be strong pressure for use of the scheme by the private sector, both for the various roles private sector organisations play on behalf of government, and for their own independent purposes.

4.12 While the legitimate role of pseudonymous transactions has been recognised, the scheme itself does not provide for them – leaving it to service agencies to provide for a limited role based authentication. This is disappointing, although typical of authentication frameworks in most jurisdictions. Providing more comprehensively for pseudonymous transactions as a positive privacy enhancing feature would require a significant re-think of the conceptual model.

4.13 All of these factors in combination build up to a system which looks very much like the foundation of a national population register, with all of the potential of such a register for secondary uses and subsequent extensions, including developments currently rejected such as the issue of identity cards. This perception must be managed, and will only be overcome by strong and deeply entrenched legislative safeguards.

4.14 Data quality issues are very significant and cannot be treated as minor technicalities to be resolved later. The implications of errors in the operation of the scheme are potentially very serious, and the frequency of errors, and the way in which individuals concerned are then treated, are critical factors in the public acceptability of the scheme. The risks have not so far been well articulated or quantified, which is necessary before any overall public interest balance can be struck.

4.15 Similarly, data security issues are fundamental to the acceptability of the scheme – not just for privacy reasons. Many of the questions that need to be asked about security remain unanswered. In some cases this is because the answers will depend on the detailed design and technical solutions to be adopted, which have not yet been decided. At this stage, it is therefore not possible to say if the scheme will even be

[190] Depending on how the 'no biometric exchange' assumption is interpreted – see paragraph 3.64.

able to meet the standards required both to comply with the Security Principle in the Privacy Act, and for operational acceptability.

4.16 Overall, dealing effectively with privacy concerns inevitably limits some of the efficiency and convenience gains that could otherwise flow from an authentication scheme that paid no attention to those concerns. A trade-off is involved. It may be that adoption of all the recommended privacy protection measures would cripple the business case for the scheme. Ultimately, risk analysis and/or political judgements will balance the strength of the privacy risks and concerns, and whether the public interest and private benefits of the scheme outweigh some or all of those concerns. This judgement will determine which if any of the recommendations in this report are accepted and implemented.

Position of other government agencies

4.17 The general impression gained by the PIA consultants from discussion with other agencies is that they are following the progress of the SSC authentication initiative with interest but at this stage without any firm commitment or great enthusiasm. Most see the all-of-government scheme as potentially offering a means of authenticating the identity of individuals which would sit alongside other in-house or bilateral arrangements, which will continue to be developed, especially for transactions with legal entities and professionals, which are seen as the major growth area for on-line transactions and e-government in the short to medium term.

4.18 Some agencies see a need for additional Evidence of Identity over and above that proposed for the scheme. While the scheme design anticipates this being a matter for individual Service Agencies, there are suggestions from some agencies that they would like to see the central scheme itself store and provide more personal information – both more detailed ID data and other attributes. There is also some interest in the potential of the proposed database of digital photographs or images. Reservations about the utility and value of the scheme centre around unresolved liability issues.

4.19 The reaction of other agencies, in the PIA consultant's view, provides some support for concerns about potential scope- and function-creep, although it probably has even greater implications for the business case.

Authorising legislation

4.20 The public will only be able to have confidence in the scheme itself, and in assurances and commitments concerning its limits, if detailed and specific legislation is passed to set up the Authentication Agency and govern the operation of the scheme.

Recommendation 35. If the centralised model is pursued, the statutory framework should cover the following (this list picks up and expands on the specific recommendations already made):

- ***Authentication Agency functions – preferably not including the technical standard setting for acceptable Keys, or the provision of the technical infrastructure of a common login site, which should be undertaken separately.***

- ***Authentication Agency Registrar & staff – independence, accountability, reporting, resources.***
- ***Liability – clear allocation of responsibility between agencies (including AA, SAs, Organisational TRs and KPs), and clear specification of liability of individual Trusted Referees and Credential Holders.***
- ***Trusted Referees – criteria, functions (and liability)***
- ***Key Providers – criteria for participation, role, conditions (eg: required infrastructure, security etc).***
- ***Unique Identifiers – clarification of the effect of the UI principle in the Privacy Act, and specification of appropriate controls on the use of the Credential, ID data, Key Serial Numbers and other identifiers involved in the scheme.***
- ***Information Matching – designation of information exchanges involved in the scheme as authorised information matching programmes for the purposes of the Privacy Act.***
- ***Criminal penalties – specification of criminal offences as a deterrent against abuse of the authentication system and of appropriate penalties***
- ***Limited data – specification of what data items can be collected and stored in the central database***
- ***Access, Use & Disclosure limits – specification of which agencies can obtain what data for what purposes, including where appropriate limits on the existing powers of other agencies.***
- ***Data retention – specification of periods of retention for data collected for both registration and transactions, balancing operational requirements with privacy***
- ***Auditing of all participants – by appropriate independent auditors at all relevant stages and processes***
- ***Review Body – location, powers and resources***

Use of this report

4.21 As discussed earlier, Privacy Impact Assessments are intended to be public documents, providing a basis for informed debate about the benefits and costs of new initiatives. It is strongly recommended that this PIA Report be published as soon as possible, and in particular in time to allow for feedback before any decision is made as to implementation of the proposed authentication scheme.

4.22 Given that the scheme design is still evolving and not stable, there will be a need to update or revise the PIA to review changes. Changes may well answer some of the unresolved questions, but may also raise significant new issues, or alter the significance of issues already identified.

Appendices

Appendix 1: Consultants profile:

Pacific Privacy Consulting - Nigel Waters – Principal

Nigel Waters has been an independent privacy consultant since 1997, working for Australian and overseas clients in both the private and public sectors, including conducting a number of Privacy Impact Assessments.

He was Deputy Australian Federal Privacy Commissioner between 1989 and 1997, and Assistant UK Data Protection Registrar, 1985-88.

He has participated in OECD and Council of Europe data protection expert groups, and in many of the conferences and working parties of International Data Protection Commissioners.

He is a founder member, and currently Convenor of the Australian Privacy Charter Council, and Associate Editor of *Privacy Law and Policy Reporter.*

He has Masters degrees from the University of Cambridge (Geography); the University of Pennsylvania (City & Regional Planning), and the University of Technology, Sydney (Journalism). He is currently a Visiting Fellow at the University of New South Wales.

Nigel is the author of numerous submissions, reports, conference papers and articles on data protection and privacy.

Project Partners – Xamax Consultancy - Roger Clarke – Principal

Roger is a leading international expert in e-business and information infrastructure.

He has conducted numerous consultancy assignments for public and private sector clients in the areas of authentication, both on- and off-line, privacy and e-government.

He is currently Visiting Professor at the University of New South Wales and the University of Hong Kong and has had a distinguished academic career at the Australian National University.

Roger has published widely in the areas of privacy, surveillance, information infrastructure, e-government and e-business and maintains a world-renowned resource Website on these areas.

He holds Commerce degrees from UNSW. and a doctorate from the ANU, and is a Fellow of the Australian Computing Society.

Relevant assignments - Pacific Privacy Consulting

Client: **Privacy Commissioner of Victoria**
Nature of Assignment: Development of a Privacy Audit methodology and Manual
Date: April-June 2003

Client: **New Zealand Department of Justice/Privacy Commissioner (sub-contracted by DY Consulting, Wellington)**
Nature of Assignment: Review of Complaints handling
Date: September-November 2002

Client: **Victorian Electoral Commission**
Nature of Assignment: Development of Privacy Management Plan
Date: April-September 2002

Client: **NSW Office of State Revenue**
Nature of Assignment: Review of Privacy Management Plan
Date: April-July 2002, and June 2003

Client: **Parliament of Victoria, Scrutiny of Acts & Regulations Committee**
Nature of Assignment: Report and draft Code of Conduct for Victorian Members of Parliament
Date: April–December 2001

Client: **Privacy Commissioner for Personal Data, Hong Kong**
Nature of Assignment: Paper and draft Code of Practice on Workplace Surveillance
Date: January-April 2001

Client: **NSW Fire Brigades** *(sub-contracted to Xamax Pty Ltd)*
Nature of Assignment: Development of Data Management Plan under the Privacy and Personal Information Protection Act 1998 (NSW)

Client: **Immigration Department, Hong Kong SAR**
Nature of Assignment: Privacy Impact Assessment for proposed HKSAR Identity Card
Date: September 2000

Client: **NSW State Superannuation**
Nature of Assignment: Development of a Data Management Plan under the Privacy and Personal Information Protection Act 1998 (NSW)
Date: March – July 2000

Client: **eSign Australia (now VeriSign)**
Nature of Assignment: Advice on public key infrastructure products and privacy policy
Date: March 2000

Client: **Privacy Commissioner of New Zealand**
Nature of Assignment: Issues Paper on Telecommunications Privacy
Date: March-May 2000

Client: **Land Victoria**
Nature of Assignment: Preparation of Data Management Plan
Date: October 1999-May 2000

Client: **Privacy Commissioner for Personal Data, Hong Kong**
Nature of assignment: A review of the value of notification provisions in data protection laws, and subsequently business planning for introduction of a register (latter task as sub-contractor to PricewaterhouseCoopers).
Date: March-May 1998, and January-May 2000

Client: **National Computer Board, Singapore**
Nature of Assignment: Risk Assessment - review of adequacy of privacy protection in Singapore in the context of possible data transfer restrictions from other jurisdictions.
Date: November 1998 - July 1999.

Client: **Zergo Asia Pacific Pty Ltd (became Baltimore, now SecureNet)**
Nature of Assignment: Advice on public key infrastructure products and privacy policy.
Date: November 1998 - April 1999.

Client: **Commonwealth Office of Government Information Technology**
Assignment: Review proposal for a government public key infrastructure (Project Gatekeeper) and comment on privacy implications
Date: April 1998

Relevant assignments - Xamax Consultancy

Agencies of National Governments

- **National Office for the Information Economy**, Canberra, 2003
  Requirements analysis and conceptual design for the government's authentication framework, including Privacy Impact Assessment

- **Ontario Management Board Secretariat**, Toronto, 2001
  Analysis of privacy implications of alternative authentication schemes

- **Hong Kong Immigration Department**, Hong Kong, 2000
  Privacy Impact Assessment for the proposed HKSAR chip-based ID-card

- **National Office for the Information Economy**, Canberra, 2000
  Analysis of accreditation requirements for Registration Authorities (RAs)

- **Department of Health and Aged Care**, Canberra, 2000-2002
  Conception and assistance with design of electronic consent mechanisms

- **Industry Canada**, Ottawa, 1999
  Presentations to the Privacy Working Group, the Public Key Working Group, and a Privacy Panel at the Technology in Government Conference

- **Ontario Management Board Secretariat**, Toronto, 1999

Review of privacy impact assessment guidelines

- **Australian National Audit Office**, Canberra, 1998

Assistance in relation to the planning of a privacy audit

- **Centrelink**, Canberra, 1997-98

Privacy strategy for smart card implementations

- **Single Entry Point Task Force / Business Entry Point Management Branch**,
  Department of Workplace Relations and Small Business, Canberra, 1997-98

Privacy aspects of single entry point and single registration process, Requirements analysis for a universal business identifier, Privacy strategy

Agencies of State Governments

- **N.S.W. Health Commission**, 1998

Privacy strategy relating to the Patient Data Linkage project

- **Victorian Dept of the Premier and Cabinet, Multimedia Vic.,** 1995-97

Privacy and user authentication issues in electronic services delivery

Privacy strategy for smart cards

- **Australian Capital Territory, Department of Urban Services**, 1994

Privacy and user authentication issues in ESD

Private Sector Corporations

- **Standard Transactions**, British Virgin Islands, 2002

Requirements analysis and preliminary design of a privacy-sensitive e-authentication scheme for agents, corporations and private clients

- **Nuix**, Sydney, 2000-

Privacy analysis and strategy for the company's eCommerce platform and email-archive forensic analysis applications

- **Healthexchange**, Sydney, 2000

Privacy aspects of the company's new Certification Authority business

- **Card Technologies Australia**, Sydney, 1993-94

Privacy strategy for multi-function smart cards

- **Health Communications Network**, Canberra, 1993

Privacy principles and guidelines for electronic health care services

Appendix 2

Glossary (modified from Business Process Design)[191]

Term/Acronym	Meaning
Administrative Data	Data or information contained on an ID credential used for administration purposes only.
Attribute	An individual piece of information.
Audit trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time.
Authenticate	To give legal validity to, to render valid, to establish the validity of.
Authenticated individual	A person who has successfully met the requirements of the authentication registration process and been issued an ID credential.
Authentication Agency (AA)	The government agency or agencies responsible for (i) verifying the **identity** of the registering **person** and (ii) establishing an ID credential for that person to use when accessing government services online. The Authentication Agency is not necessarily the same as the agency providing the service - the **service agency**.
Authentication session	The period of time commencing after both parties have accepted each others ID credential and ending when one of the parties terminated the session.
BDM	An acronym for Births, Deaths and Marriages. Births, Deaths and Marriages: part of the Department of Internal Affairs.
Client or Individual	A **person** seeking to access a government service online (but see paragraph 2.2).
Credential ID Credential	A recorded set of identity data, or attributes, provided by a living person and verified by the Authentication Agency using a process to establish identity. The ID Credential created by the Authentication Agency is an electronic record containing verified identity data.
ID Credential Number	A unique number used by the Authentication Agency to identify and administer **ID Credentials.** For internal use at the Authentication Agency only.
Data	Information provided by a person to an **Authentication Agency** or a **Service Agency OR** by a **Service Agency** or **Authentication Agency** to a person
Evidence of Identity	See **Identification**
Government Agency	A blanket term that includes departments, Crown entities, and any organisation within the State sector. **Service agencies** and **Authentication Agency** are government agencies.

[191] The Glossary from the Business Process Design v.1.0 has been edited to conform to the way terms have been used in this PIA. Some terms have been omitted, others modified, where they have either not been used, or used differently, in the PIA. Where they have been used differently, this is explained in the PIA.

Term/Acronym	Meaning
ID Data	A single piece of information, that when combined with other ID Data uniquely describes/defines a **person.**
Identification	The process of associating identity data with a particular **person**.
Identification Evidence of Identity (EOI)	A process whereby a real-world entity is recognised, and its 'identity' established.
Identity Data	Refer to ID Data.
Identity fraud	To use the identity of a **person** without their express consent, for a purpose that the person is not aware of, and/or does not approve of. Generally for an illegal activity.
Identity theft	A particular type of **identity fraud**, accomplished by 'hijacking' of a genuine identity. By gaining access to the identity, the offender is able to impersonate the owner and conduct business as them, usually for the purposes of committing fraud
Identity information	That set of detailed information that together uniquely describes/defines a **person**
Key	The technology that allows the Client to unlock and provide the information on their ID Credential to a Service Agency
Key Linking	Part of the First Time Service Registration process of associating a **Key** to a Client record maintained by a **Service Agency**.
Key Provider (KP)	An agent or agencies authorised to issue accredited Keys to a Client.
Key Serial number (KSN)	A generated, sequential number used to uniquely identify a specific Key.
Legal Liability	The phrase that summarises where the responsibility will lie if/when failures/frauds in the system occur
Non-repudiation	The inability of a person or agency to legally repudiate (deny) its participation with an action or a piece of information
Person	An individual human being; man, woman, or child.
Personal Information	Information about an identifiable **individual (see Privacy Act)**.
Privacy Impact Assessment (PIA)	A formal process to identify and assess privacy implications – in this case of an online authentication solution for government.
Pseudonym	An arbitrary name chosen by an individual to identify themselves, e.g. a username.
Registration	The process of establishing an **identity** of a **person** as a prequisite to being issued an ID Credential to enable **authentication**.
Repudiation	The rejection or renunciation of a duty or obligation – usually arising from a disputed transaction
Request Verified Information (RVI)	A process used to allow the Client to authorise release of ID Credential data from the Authentication Agency to a Service Agency.
Review Body	An independent agency that acts as an authentication watchdog; a body that **individuals** can ask to intervene in the event that they believe they have been incorrectly treated or adversely affected by a decision made by an agency as part of the authentication process.
Revocation list ID Credential	The register of **ID credentials** that have been suspended, withdrawn or cancelled/revoked.

Term/Acronym	Meaning
Revocation List	A list of ID credentials held by the Authentication Agency comprising ID credentials that are no longer valid. A reason for each ID credential being on the list is retained by the Authentication Agency.
Service Agency (SA)	**Government agency** responsible for delivering an **e-service** – not the **Authentication Agency**
Service-delivery information	Additional information (beyond that contained in an ID credential) required by a **person** so that they can access a specific **e-service**.
Service reference number	Customer reference number held by **Service Agency** (e.g. IRD number).
SIGS	Security In the Government Sector manual – the minimum standards for Government security. [http://www.security.govt.nz/sigs/index.html]
Trusted Referee (TR)	A person: i. that confirms data about a person is accurate; and ii. that confirms that the stated data belongs to that person. iii. that can be held accountable for provision of any information that is later found to be false or misleading. A third party, agreed in advance by both the authentication agency and the person, that verifies the identity of an individual during the stage that the individual's registration for authentication is taking place. Trusted Referees fall under two categories, these are: 1. **Trusted record:** A record of the Client's identity maintained by a trusted agency for the purposes of verifying aspects of the Client's identity (e.g. the Department of Internal Affairs, Births Register); and 2. **Individual with personal knowledge:** An individual who uses personal knowledge to verify information about the Client (e.g. close friend, employer, lawyer, doctor, landlord).

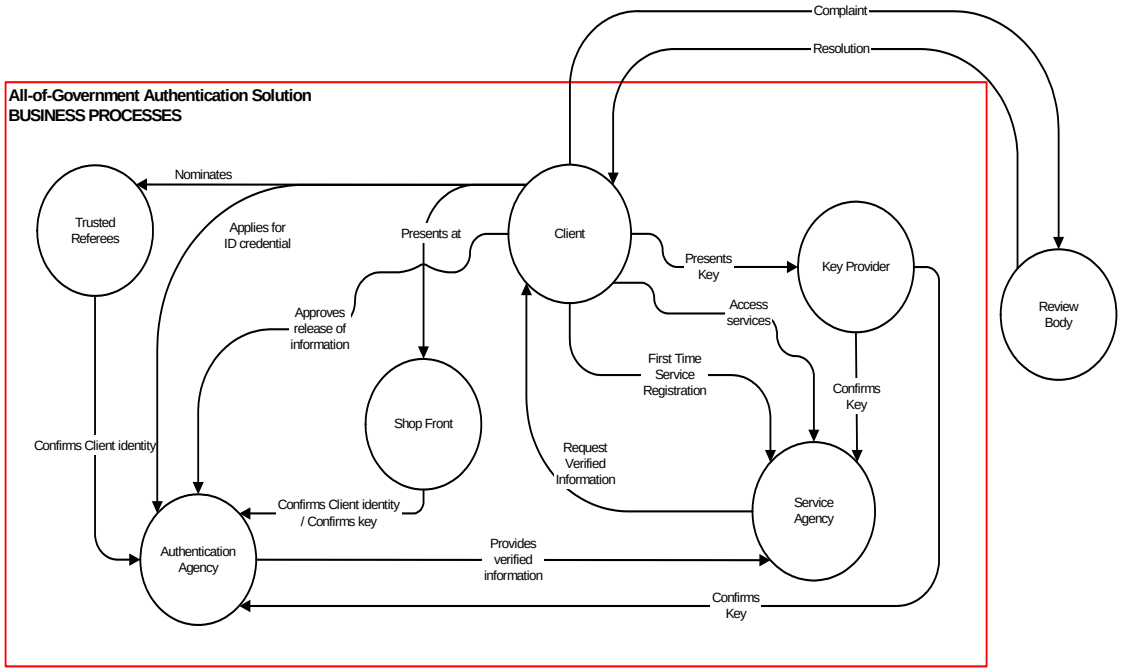
Appendix 3 – Diagrams of main relationships

(Source: Business Process Design v1.0)

For formal definitions of the actors refer to the Glossary – Appendic 2.

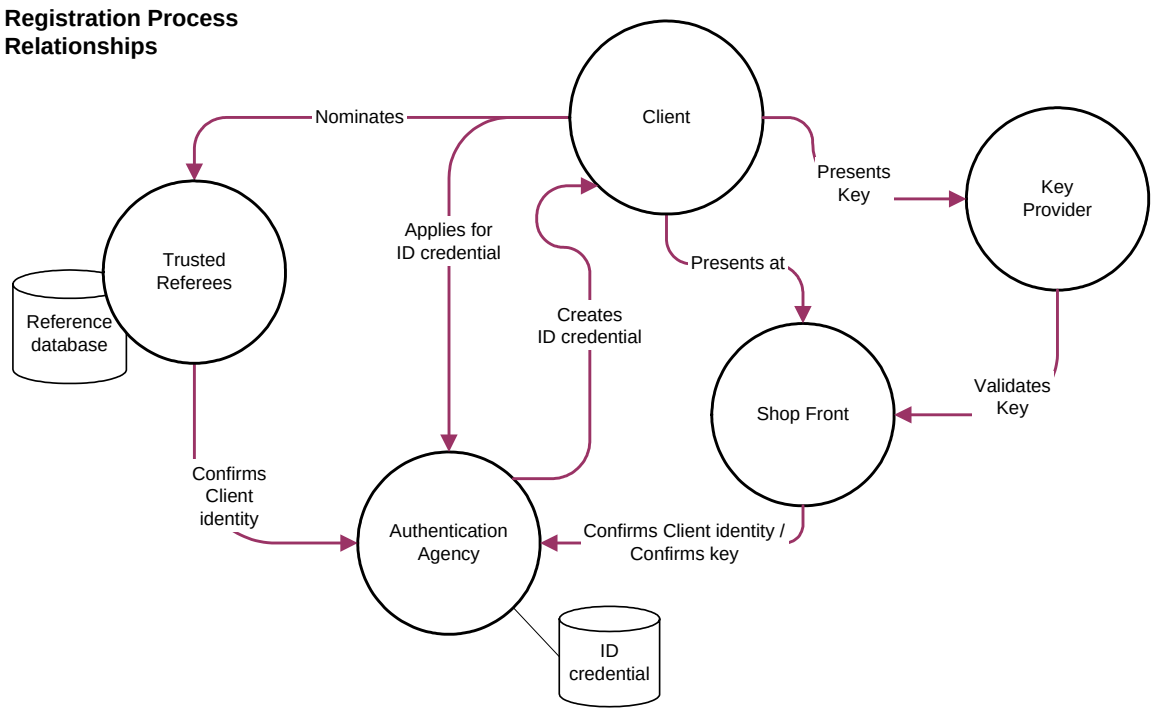
Appendix 3a The diagram below shows the relationship between the actors and provides an overall context of the proposed authentication solution.

Authentication Design
Relationship Bubble Diagram



Appendix 3 b

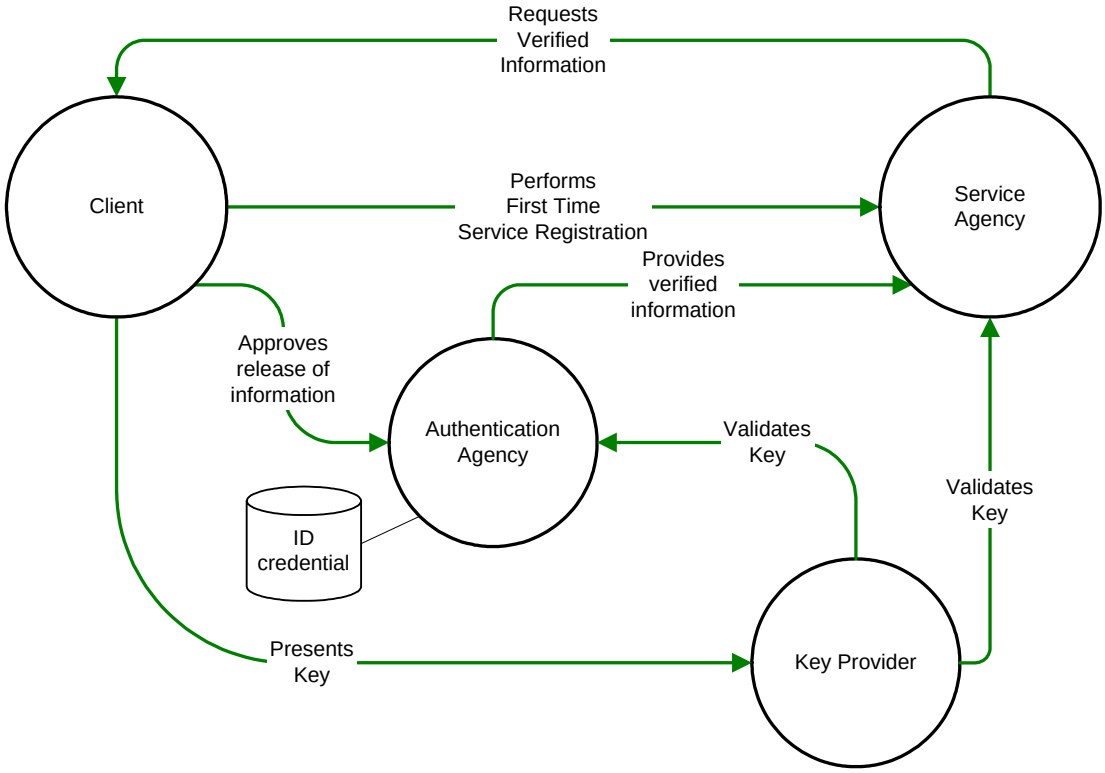
The diagram below summarises the role of the actors in the Registration process.



Appendix 3c

The diagram below summarises the role of the actors in the First Time Service Registration process.

First Time Service Registration Process Relationships



Appendix 3d

The diagram below summarises the relationship of the actors in the Request Service process.