State Services Commission
ICT Branch

Privacy Impact Assessment of the All of Government Authentication Programme –Identity Verification Service

John Edwards
Barrister and Solicitor

1. Introduction and Overview

1.1. This is the latest in a series of privacy impact assessments that have been prepared in relation to elements of the State Services Commission's work on online authentication.

1.2. The first and second privacy impact assessments were prepared by Pacific Privacy Partners in 2003 and 2004. They are available on the e-government website at http://www.e.govt.nz/services/authentication/authent-pia-200312 and http://www.e.govt.nz/services/authentication/pia-200404.

1.3. Following the publication of those documents, the ICT Branch of SSC split the workstreams associated with online authentication into the Government Logon Service component, and the Identity Verification Service component. Separate reports on privacy impact have been commissioned for each component. A privacy impact assessment was completed for the Government Logon Service in June 2005 and is available at (http://www.e.govt.nz/services/authentication/gls-pia).

1.4. That document expressly excluded discussion of an Authentication Agency, or of issues of establishment, proof, or evidence of identity. Those issues become the focus of attention in this report. The terms of reference for this report are attached as appendix "A".

1.5. The identity verification service is concerned with establishing identity to the high level of confidence (equivalent to passport level) set out in the draft EOI Standard (available at www.dia.govt.nz).

1.6. This paper should be read in conjunction with the privacy impact assessment prepared for the government logon service. The Authentication Service consists of two services, the GLS, and the IVS. This paper does not repeat all the process descriptions of how the GLS works, although this is required for a full understanding of the IVS.

1.7. This report is intended to be an independent and objective review of the privacy implications of the identity verification service, and its role in online authentication. As Pacific Privacy Partners noted in their reports, there are privacy positive and negative features about any proposal to authenticate identity. The greater security afforded can serve a privacy interest as it will provide a greater level of protection for individuals wishing to conduct online transactions. Also, the policy settings under which the project has been undertaken ensure that many of the risks to privacy are minimised. For example, nothing in the proposal gives rise to concerns about the expanded use of unique identifiers. New collections of personal information are avoided or kept to a minimum. These features have been developed in a privacy sensitive way, no doubt in response to

issues raised in the earlier reports. It is apparent from the latest iteration of the design specifications that the issues that have been raised in earlier reports have been taken seriously, and lead to novel approaches to striking the balance between the core needs of an authentication service, and of the individual privacy interest of the population as a whole.

1.8. There remain a number of issues to be addressed in the more advanced design stages of the IVS. For example the threshold for, and mechanism of effecting dual or multiple identities/credentials within the system is an important area of exception to the predominant business rules, and one which is of considerable significance from a privacy perspective. That issue also leads to a discussion of the "one person-one credential rule" which was a key concern identified in the earlier privacy impact assessments.

1.9. Other features which warrant close examination include the reliance for adherence to the Cabinet principles, and the preservation of privacy on policy instruments, and a plethora of documents such as standards, which do not uphold individual rights in a mandatory way. Again, the monitoring and enforcement of these instruments is a matter of current study, and as such the privacy implications of important aspects of the project are contingent on decisions which are still to come, and therefore remain subject to some conjecture. As is discussed in greater detail below, to be effective in addressing privacy concerns, standards and e-GIF policies need to be mandatory. To be effective, they need to be monitored, and service agencies need to be audited for compliance. Sanctions need to be added. If policies and standards that are identified in this report as contributing positively to privacy are not being adhered to by service agencies, then the IVS should not allow its service to be used by those agencies.

1.10. With the IVS approach being unique in the world, there is also the possibility of new threats, particularly in relation to the creation of a "virtual identity card" whereby the identity verification credential could become a de facto instrument of identification in the community. At this stage such speculation cannot make a very useful contribution to the discussion, in that the nature and likelihood of any privacy threat is contingent on technology and policy changes and is too remote from the current design parameters to be a concern warranting detailed analysis and regulation.

1.11. As with the earlier privacy impact assessment, the process of developing the identity verification service is ongoing. Further policy decisions are to be taken as standards documents are developed, and the systems needed to support the business models are decided on, vendors selected, and so on. A number of decisions will need to be made as to the shape of the legislation (if any) and other administrative and accountability instruments needed to support the policy. The privacy implications of the various options need to be analysed at each stage of design and implementation.

Critical assumptions

1.12. As noted in the privacy impact report on the GLS, the process of privacy impact assessment involves an assessment of a given policy or technological initiative based on its features as known at a given moment in time. In addition, many of the privacy risks identified are contingent on the occurrence of a number of other events, such as institutional or policy changes affecting how personal information might be used.

1.13. There are some difficulties in conducting an assessment that will remain current as processes evolve and develop, and technology enables further functions and enhancements. Given that privacy impact assessment is a predictive process, a certain level of speculation is a necessary in order to anticipate privacy threats, and recommend mitigation strategies. However, a balance must be struck as to the level of speculation that is legitimate, and useful in contributing to the current development. At a certain point, predicted threats may be too remote from the current design and intention, and too contingent on a number of significant scope changes to merit serious analysis at the outset of the project.

1.14. One of the methods available to assist balancing these sometimes competing objectives is to state a number of critical assumptions, representing the central features of the proposal that have been used to inform the process of privacy impact assessment. The implication is that the privacy impact report will remain current for as long as these central features remain. This is a check on the effect of the evolving nature of the design, in that not just any development will materially alter the parameters to require fresh privacy impact analysis. There remains a role for speculation as to contingent effects on privacy, and as such, the following list does not completely remove the need in this report to consider the effect of expansion of the scheme, notwithstanding that expansions would be outside the currently defined parameters of the project.

1.15. Recording assumptions is particularly important in relation to a project like the IVS, because many of the assurances as to privacy protection depend on adherence to non-statutory instruments which have not yet been finalised and accepted. The business process remain at quite a high level with design parameters, and supporting IT architecture still to be finalised. The following assumptions are critical to the conclusions and recommendations in this report;

- There will be ongoing across government adherence to the Cabinet principles specified in paragraph 3.20.
- The voluntary basis of scheme will be underpinned by service agencies being obliged to continue to provide alternative offline means of establishment of identity.

- The use of the IVS and IVC is limited to individuals transacting with Government Agencies (G2P). Private sector agencies will not be able to allow users to use their IVC to verify their identity online.
- Agencies will adhere to the EOI standard, and will not require establishment and verification of identity to a level higher than the identity risks associated with the service they are offering.
- The IVC will not centralise the collection of personal information to any extent that is greater at present.
- The photo biometric will not be used for "one to many" matches with the any government photo biometric database.
- The service will not result in the creation of any new unique identifiers capable of being used by two or more agencies in breach of information privacy principle 12.
- Further operational policy documents and interagency instruments such as memoranda of understanding and standards are still being finalised or yet to be developed, but will be reviewed by the program for their impact (if any) on privacy as they are produced, and in any case will be in place prior to the implementation of the IVS.

1.16. One of the deficiencies that has been identified with this approach to privacy impact assessment is that the proposal under assessment is seen in an artificially constrained context. That is, so much of the risk is ruled out by adherence to a number of "givens" that the assessment may give a false sense of security. If any of the assumptions prove incorrect or insufficiently durable, the process of privacy impact assessment will seem, in retrospect, to have been valueless.

1.17. A related constraint is the project orientation, or the different expectations of the process of PIA for different stakeholders. To be of value to business analysts and system architects, a privacy impact report must identify practical issues arising from given design parameters. Speculation about what could be added to the design parameters is of limited value in assisting those involved in the project to minimise privacy risks. Privacy advocates however have a broader interest, not just in the narrow system characteristics, but in the broader policy implications of such a project. Those concerns transcend the "merely" technical, and include concerns about the potential misuse or now unanticipated expansion of the architecture in privacy adverse ways. Two examples illustrate the different approaches. Various processes of privacy impact assessment have highlighted concerns associated with the potential for using the system to aggregate previously disaggregated data held by a number of different agencies. These concerns have been taken into account by the systems designers in a way which considerably reduces the risk that the IVS will enhance that aggregation. Technical solutions have been designed (namely the use of modified identity verification credentials specific to each service agency) to address the privacy risk.

1.18. However a considerable risk from a privacy policy perspective is the extent to which the IVC becomes ubiquitous, and therefore universal. The risk here is that the IVC could become the basis for a compulsory document of identity, and that with all the architecture in place, and considerable uptake of the service by the population, it would be a small leap for a future government to make a new instrument, and use of the system compulsory. Those risks are outside the scope of those involved in the detailed system design to influence.

1.19. To manage these tensions, or different expectations of the process of privacy impact assessment it has been agreed that this report should make recommendations intended to ensure that the broader policy concerns are not lost in the modular technical detail. A key part of this is to recommend that further privacy impact assessments are undertaken if any of the parameters described by the "critical assumptions" are to change, and to ensure that such concerns remain high in the IVS project planning consciousness by including privacy risks (in the broadest sense), in the project risk register documentation.

Recommendation 1

That further privacy impact assessments should be undertaken before:

- Any proposed amendments to the Cabinet principles specified in paragraph 3.20 are put to Cabinet.
- Any proposal to relax the requirement that service agencies are obliged to provide alternative offline means of establishment of identity are considered.
- Any expansion of the use of the IVS and IVC beyond individuals transacting with Government Agencies (G2P) is proposed.
- Any substantial amendments to the EOI standard or the requirement on agencies to comply with the standard are made.
- Any changes to the IVS or IVC that would lead to the greater central collection of personal information are proposed
- Photo biometrics are used for "one to many" matches with any government photo biometric database.
- Any exemptions from information privacy principle 12 are proposed to accommodate wider use of unique identifiers associated with the IVS.
- Operational documents supporting the IVS, such as access agreements, memoranda of understanding, standards and the like are put in place.

Recommendation 2

That the IVS maintain and regularly report to its governing body on a privacy risk register, such a register to include risks such as:

- That the proposed systems of monitoring and control of service agencies will not be adequate to ensure adherence to the EOI standard and other central controls such as e-GIF.

- Replacement of existing lower level authentication with high confidence requirements necessitating wider than currently anticipated use of the IVS & IVC.
- Weakening of alternative (ie non-IVS) forms of online or off line authentication.

Out of Scope

1.20. While Maori issues were an explicit part of the brief for review in the earlier privacy impact assessments, no separate consideration has been given to the position of tangata whenua, the Treaty of Waitangi, or different cultural practices relating to privacy in this report. Some of these issues have been canvassed in *Research of Issues for Māori relating to the Online Authentication Project*, a report for the State Services Commission 29 March 2004 Paua Interface Limited.

2. Methodology

2.1. The following sources of information have informed the preparation of this draft:

- All-of-government Authentication Programme Initial Implementation Phase Integrated Conceptual Design version 1.1 13 July 2005
- Identity Verification Service functions High-level design specifications version 1.4, 1 August 2005
- Draft Evidence of Identity Standard August 2005 Version 0.6
- Authentication: Is (Or, To What Extent Is) A Statutory Regime Required? Version 1.0 February 2004
- Online Authentication Review of Legal Issues Version 1.2 23 April 2004
- The two privacy impact assessment reports prepared by Pacific Privacy Consulting (referred to above), and the document entitled Authentication for e-government Review of Privacy Impact Assessment Recommendations (SSC response to Pacific Privacy Partners reports)
- Meetings with the Office of the Privacy Commissioner, State Services Commission and Department of Internal Affairs.
- Principles for Electronic Authentication - A Canadian Framework Industry Canada 2004
- Australian Government Information Management Office - AGAF guide to authorisation and access management 2005
- *Non-Intrusive Identity Management* Dr. Stefan Brands McGill School of Computer Science & Credentica March 23, 2004
- *Who Goes There?: Authentication Through the Lens of Privacy* Computer Science and Telecommunications Board National Academies Press (2003)
- Liberty Alliance, and Microsoft Passport materials
- *Privacy Impact Assessment Handbook* Office of the Privacy Commissioner
- Ministry of Justice contributions to the project team including references to international studies on electronic and digital signatures, authentication and encryption, and other matters relevant to different stages of the project design.
- Draft Guide to Authentication Standards for Online Services (SSC)
- Draft Authentication Key Strengths Standard (SSC)

Terms and Acronyms

2.2. For the purposes of this report, the following terms and acronyms are used.

Term	Description
CLS	The Common Logon Site, a website that provides the Internet facing front end of the GLS to service users
GLS	Government Logon System, a shared all-

	of-government service for logon management. Comprised of the CLS and KP.
Identity Verification Credential (IVC)	A set of data attributes which uniquely identifies an individual consisting of; name, sex, place of birth, date of birth, mother's birth name and IVCN.
Identity Verification Credential Number (IVCN)	A unique identifier permanently attached to the IVC
Integrated Authentication Service (IAS)	A common online front-end for service users and service agencies to conveniently access back end services, GLS and IVS.
Key	A means of service users confirming their identity to access online services that is available only to that user. It could be as simple as a user name and password, or could be a token, digital certificate, etc.
Key Provider	Key Provider is a part of the GLS that provides keys to the user and provides for their on-going maintenance.
Key Serial Number (KSN)	The unique number assigned to a key by the key provider
Modified Identity Verification Credential Number (MIVCN)	A unique random number assigned to an IVCN that is sent to a service agency when verification is required for an online service. Each service agency will receive a different MIVCN.
Modified Key Serial Number (MKSN)	A unique, random number specific to the Service Agency generated by the GLS corresponding to the RKSN. It bears no resemblance to the KSN or RKSN, but is used by the Service Agency as the means of linking the key presented by the user at the GLS to the Service Agency's own user unique identifier.
Root Key Serial Number (RKSN)	The unique, random number associated with one or more KSNs that a Service User chooses to group together.
Service Agency (SA)	A government department or agency which provides an online service or services, and uses the GLS or IVS as the means of confirming the identity of service users.
Service User	A member of the public who uses the online service or services that are provided by Service Agencies.

3. Description of the Project and Information Flows

3.1. Service agencies offering online access to their services will be required to assess the level of identity risk associated with any given service, and on the basis of that assessment, decide on the level of confidence they require that a person seeking to conduct a transaction is who they say they are. That assessment will determine the extent of verification of identity a person must undergo in order to gain access to the service.

3.2. There will remain a number of ways by which a person can establish and verify their identity to service agencies for lower levels of risk. The IVS will be used only for the highest level of risk/confidence, and will provide a level of security that is mandatory where the highest level of confidence is required for online transactions. Where a service agency identifies that it requires the highest level of confidence in identity, a service user will be able to provide that level of verification either by using the IVS, or by using some alternative offline system, such as presenting a passport or other such document of identity to the service agency.

3.3. A very limited number of services may require even more checks than the highest level of verification required in the standard, and will therefore design their own processes independent of the IVS or the EOI standard. For example, security and intelligence agencies may provide their own checks over and above those available via the IVS.

3.4. The assessment of risk, and the thresholds for requiring different levels of identity confidence, and verification are to be set out in standards, to which service agencies will be expected to adhere. One significant impediment to this process of impact assessment is that the audit and monitoring mechanisms to ensure meaningful compliance with the standards are yet to be designed.

3.5. If the service user requires a high level of identity verification for using online government services, he or she will be able to apply to the IVS for an identity verification credential, or use a passport level "offline" means of verifying identity in accordance with the EOI standard. It should be noted here that the business processes permit any person to apply to the IVS for an IVC, whether they require online access to services or not, although why anyone would apply for an IVC with no intention of or capacity to use it is not clear.

3.6. The applicant must provide the following personal information:

- Name(s), including registered name, and name changes where these have occurred.
- New Zealand passport number (if they have a passport).
- New Zealand citizenship number (if they are a citizen by grant).

- Trusted referee's name, contact details and email address. If the trusted referee does not have an IVC then they will need to include their passport number.
- Passport quality photo.
- Proof of use of the identity in the community.
- Guardianship or power of attorney details (if they are not applying for themselves).

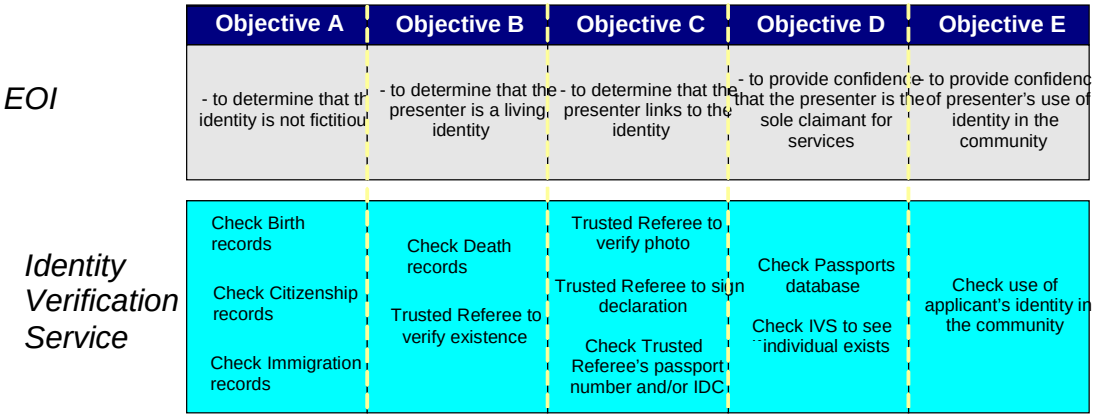
3.7. If the individual does not have a New Zealand passport or citizenship certificate then the following information is also requested:

- Marriage certificate number or marriage details (if applicable).
- Civil union certificate number or civil union details (if applicable).
- Citizenship status (if by birth and have no New Zealand passport or are not a New Zealand citizen).
- Residency number (if applicable).
- Non-New Zealand passport number and country of origin.
- Birth certificate number or birth certificate details.
- Guardianship or power of attorney details (if applicable).

3.8. The IVS then undertakes checks against the databases administered by the Department of Internal Affairs (the IVS will have access to the Birth Register, the Death Register, Marriage and Civil Union Registers and Citizenship Register as an authorised information matching programme regulated under Part 10 of the Privacy Act) and undertakes any other necessary checking (such as with the referee). The seven stages of verification are linked to the five EOI Objectives (listed as A – E below);

- IVS checks application information quality.
- Trusted referee verifies individual's photo.
- IVS determines individual's identity exists (A).
- IVS determines individual's identity is living (B).
- IVS determines individual belongs to identity (C).
- IVS checks individual is sole claimant to identity (D).
- IVS checks individual's use of identity in community (E).

3.9. The following table, taken from the High Level Design Document, illustrates the steps the IVS will take to achieve each of the EOI objectives.



3.10. In addition, Objective D will be checked by means of a biometric derived from the photograph submitted by the individual against the photographs retained in the IVS database. It should be noted however that there remains some debate about the readiness of this "one to many" biometric checking technology, and as such, at the date of this assessment, this function is not proposed for the initial roll out of the IVS. Any further developments in respect of any biometrics to be associated with the IVC should be subjected to further privacy impact assessment, including reliability tests, and the business process consequent upon a "match". Records of false positive and (if possible false negative matches) should be retained for an extended assessment period prior to any formal implementation to assist in evaluating the reliability of the technology.

3.11. Once the identity has been established, an identity verification credential is created. This credential is a composite of data items. At the time of writing it is anticipated that the IVC will comprise:

- names[1]
- sex
- date of birth
- place of birth
- mother's birth name.
- a unique identity verification credential number

3.12. Key features of the IVC are:

- There is only one type, and strength of IVC, and only one issuing agency.
- On its own, an IVC has no independent function. It's utility comes with its association with a key. It is in a sense misleading to refer to the IVC as a

[1] Including the name(s) shown on an official record such as a statutory declaration, previous names, aliases and names created by administrative error.

tangible thing with inherent functions and values. The IVC is merely a collection of data. The sum of the data, rather than any individual part is what ensures it is unique, and relates only to one person.

- Unless exceptional circumstances are deemed to exist, as determined by DIA at the time of application, an individual will only have one IVC. Exceptional circumstances are those where by some legal authority requirement, a person is entitled to use a name for various official purposes usually requiring verification that is separate and distinct from their identity as recorded in official registers such as the register of births. An important area of work in relation to this feature remains to be completed. At present there is no clear criteria for who is entitled to qualify for what might be called "multiple identities", nor is there clarity as to precisely what this will mean, and how it will work. For example, people on witness protection are one category that might warrant special treatment, and one would expect undercover police officers, and intelligence personnel to be able to conceal their "true" identity. Other classes might also make a strong case, such as people who have domestic violence orders from the court, or those who have taken action under the Harassment Act. Once the eligibility criteria is established, the mechanism needs work. For example, will the system retain links between the known identities, or will they be regarded as different people to the IVS?
- Access to and use of the IVC will require a minimum of two factors of authentication, but not just any two factors will be sufficient. The Authentication Key Strengths Standard will specify the acceptable level of strength of the two factors. The standard will presumably have to be regularly revised to ensure the strength keeps pace with changing technologies. This will adhere to the Guide to Authentication Standards for Online Services currently under development.
- It is proposed that the IVC will expire every 5 years and on the individual's death.
- Each IVC will be version numbered in line with the EOI standard version numbering in order to be able to easily determine which version of the EOI standard an individual has been verified to. This will provide a "through life" record of the IVCs.
- IVCs will be created only by the IVS, but the IVS might permit other agencies with EOI processes appropriate for the highest level of identity-related risk category under the authentication standards to undertake parts or all of the EOI process on IVS's behalf to create an identity credential. These would be agencies that can demonstrate a sufficiently rigorous process of EOI. The obvious example would be the Permanent Residence process of New Zealand Immigration Service, in relation to individuals with foreign identity documents.
- An IVC can be issued to minors and people under the care of guardians and those with power of attorney. However, only the individual issued with the IVC will be able to use it i.e. the guardian or individual with the power of attorney must use their own IVC, not the IVC belonging to the individual that they are working on behalf of.

3.13. It should also be noted that the IVS will only issue an IVC. It will not provide identity verification to a lower standard than the IVC. Therefore, all verification processes involving the IVS will result in an IVC. In theory, the

process to verify identity to a lower level of confidence commensurate with the identity risk represented by the service offered can be undertaken by individual service agencies, or any other organisation providing an identity service. Whether this will occur, or whether the IVS will "crowd out" lower levels of verification leading to a de facto standard of identity being the IVC for the full range of authentication levels and identity risks is one of the key unknowns, and one of the key risks associated with the project. The mitigation of this risk will be in the adherence to, and monitoring and auditing against, the standards and the Cabinet principles.

3.14. It is a legitimate response to this concern to note that the IVS is not responsible for the actions of the service agencies, which are themselves required to comply with the Privacy Act, and the Cabinet principles, and that remedies are available to aggrieved individuals who believe a service agency is using an unnecessarily high level of identity verification. In addition, the complexity, and likely cost of the higher level of verification should be a disincentive to unnecessary use of the IVS where a lower standard of authentication would suffice, as will the requirement that service agencies ensure alternative offline systems of authentication are also available (although this point is subject to the frailties of the voluntary system of standards discussed elsewhere in this report).

3.15. Once the identity has been verified, and an IVC created, an electronic record is created in the IVS database for the individual. The record will consist of:

- A unique identifier, the IVC Number (IVCN) for internal use within the IVS and linked to a table containing a cross reference to the modified form (MIVCN) for presentation to SAs.
- The individual's identity data attributes.
- The IVC's status such as *Active, Inactive, Suspended, Revoked.*
- The IVC's version number.
- IVC creation timestamp.
- Who created the IVC (person or system).
- A link to all the information gathered in establishing the individual's identity.

3.16. The next step is for the IVC to be associated with a key at the GLS. As mentioned above, the IVC can only be accessed via a high strength two factor key. To use the IVC for online transactions, the user will need a two factor key (something you have, and something you know, eg username & PIN and, for example an encrypted token). This is regardless of the level of security, risk or identity confidence assessed by the service agency.

3.17. Once linked to the key, the GLS assigns an IVS MKSN to the key, so that whenever that key is presented, the IVS will be able to confirm that the key

presenter has a verified identity. That message is transmitted to the service agency, together with selected components of the IVC and a MIVCN that is unique to that service agency.

3.18. The process of subsequent online verification of identity to service agencies is described in the High Level specification as follows;

> If the individual presents a valid key, of the appropriate strength and confidence level, to the GLS, which is then authenticated and confirmed to the IVS, then the individual is presented with the IVC information to be sent to the SA. The individual must select which of their legally recognised name(s) and personal details they wish to be released to the SA. The IVS will then incorporate these into the IVC, associate a Modified IVC number with the IVS data, and pass this information to the SA.

3.19. A useful table provided by the project team demonstrates the distribution of access to different items of information among the principal functions:

	Service User	Service Agency 1	Service Agency 2	GLS	IVS
Identity	*X*	*X*	*X*		*X*
Authentication Credential	*X*			*X*	
Key Serial Number				*X*	
Root Key Serial Number				*X*	
Modified Key Serial Number		*X*		*X*	*X*
Modified Key Serial Number 2			*X*	*X*	*X*
Identity verification credential	subset	subset			*X*
IVCN					*X*
MIVCN		*X*			*X*
MIVCN 2			*X*		*X*

3.20. This table shows the data items that any one actor will have at any one time.

3.21. The parameters for the system design have been set by Cabinet decisions. The summary (taken from the RFP) of the policy decisions taken for the Authentication project as a whole provide a helpful insight into the policy drivers affecting the technical solutions selected:

Key Policy Principles
The Government has agreed the following key policy principles for electronic authentication of individuals carrying out transactions with government agencies.

- Security - Suitable protection must be provided for information owned by both people and the Crown
- Acceptability - Ensuring that the proposed authentication approach is generally acceptable to potential users, taking into account the different needs of people and emerging industry standards, and avoids creating barriers
- Protection of privacy - Ensuring that the proposed authentication approach protects privacy appropriately
- All of government approach - Balancing public and agencies' concerns about independence with the benefits of standardisation while delivering a cost-effective solution.
- Fit for purpose - Avoiding over-engineering, recognising that the levels of authentication required for many Government to People transactions will be relatively low.
- Opt-in - Ensuring that members of the public retain the option of authenticating their identity and carrying out transactions offline and are not disadvantaged by doing so. However, it will not be possible for an individual to conduct secure online Government to People transactions without the use of the appropriate authentication process.

3.22. In addition, there are Implementation Principles that have been endorsed by Cabinet which forms the basis of the implementation of the conceptual design:

- User Focus- Ensuring the recommended solutions are as convenient, easy to use and non-intrusive as possible
- Enduring solution- Providing a solution that is enduring yet sufficiently flexible to accommodate change and a wide range of current and future transactions
- Affordability and reliability- Ensuring the recommended solutions are affordable and reliable for the public and government agencies
- Technology neutrality- Ensuring a range of technology options is considered, and as far as possible avoiding 'vendor capture'
- Risk-based approach- The solution must comply with relevant law, including privacy and human rights law
- Legal certainty- Relationships between the parties should be governed in a way that provides legal certainty
- Non-repudiation- The issue of non-repudiation must be considered for those transactions that require it, so that the risk of transacting parties later denying having participated in a transaction is minimised
- Functional equivalence- Authentication requirements should be similar to those that apply to existing transactions except where the online nature of the transaction significantly changes the level of risk

4. The Privacy Analysis

4.1. This part of the report consists of analysis of the project with reference to the information privacy principles. The information privacy principles are set out in full in Appendix 1 of this report.

4.2. As an introductory comment it should be noted that New Zealand has a fairly comprehensive regulatory framework for information privacy in the Privacy Act 1993. If this analysis were being undertaken in another jurisdiction, or in New Zealand in the absence of the Privacy Act it would be a subject of much greater concern. As it is, the Privacy Act gives people a right to complain to an independent statutory officer of any misuse of the IVC, or abuse of the scheme as a whole. If the complaints or concerns fall outside the area of concern of the Privacy Act (which is concerned only with information privacy), other agencies also have roles. For example the misuse or fraudulent use of an IVC might involve the criminal law, and be investigated by the Police. The Ombudsman and Auditor-General may have roles in reviewing complaints of unreasonable refusal to issue an IVC, or inadequate monitoring of adherence to standards and the like.

4.3. The presence of the Privacy Act will feature in any discussion of possible legislative responses to the authentication project. Legislation ought to be remedial, rather than (other than in exceptional cases) based on positions of principle. Therefore, legislation should only be recommended as a response to issues identified in this report to the extent that the Privacy Act, and other existing legislative constraints are inadequate.

4.4. Having said that, it is important also to note that the process of privacy impact assessment is not exclusively concerned with legal compliance. The regulatory model for privacy in New Zealand is based on very broad principles. Compliance in the sense of litigation risk management can be achieved relatively easily in most circumstances, however, compliance with the Privacy Act does not necessarily mean that the project does not involve some adverse privacy outcomes.

4.5. In addition, although the Privacy Act is technology neutral, aspects of the authentication project raise novel issues which might require fresh analysis. The following discussion is not therefore limited to privacy concerns measured against the yardstick of the information privacy principles.

4.6. One respect in which the Privacy Act is ill-equipped to address privacy issues arising from the project, and where the other elements of the regulatory framework are unable to fill the gap, is the availability of a remedy to users outside New Zealand. The protections of the Privacy Act, and the policies and standards identified in this report as important in mitigating privacy risk

should be available to, and enforceable by New Zealand citizens wherever they are in the world, in the same way that the Official Information Act and Privacy Act provides New Zealand citizens with rights to request information regardless of their domicile.

Recommendation 3

The Privacy Act should be amended to provide for its extraterritorial application for users of the IVS.

Collecting and obtaining personal information

4.7. **Information privacy principle 1** requires that an agency that collects personal information should only collect the minimum necessary to achieve a lawful purpose.

4.8. Nothing in the project planning documents or analysis undertaken to date suggests an intention on the part of the government, or any given agency to increase the net volume of personal information collected about individuals.

4.9. It should also be noted that responsibility for compliance with IPP 1 remains with each service agency. The IVS is not responsible for the activities of individual user agencies. Any user concerned about changes to the personal information collected by a service agency can take the matter up with that agency, or with the Privacy Commissioner.

4.10. The fact that the IVS does not control the user agencies does not mean that this process of privacy impact assessment should not attempt to assess the net effect of the personal information collections by agencies as a result of the system. There are two competing views on this point. One is that the availability of the service, with its high level of verification might become an attractive and convenient option for service agencies to offer users. One consequence of this could be that service agencies end up collecting more personal information, simply because it is available. For example, if prior to the establishment of the IVS a service agency required a user to furnish a name, and photo id, such as drivers licence or passport, and that the only information recorded was that the evidence of identity had been sighted (and perhaps the number of the document noted), that is a fairly low level of information collection.

4.11. If the agency decides instead to move to the IVS option, it has a number of choices about system design. It could enable a system that resulted in the collection from the IVS of place of birth, date of birth, mother's birth name, and alternative names. If it did, that would increase the personal information collection of the service agency, an arguably negative privacy outcome.

4.12. The alternative view is that the IVS will result in the collection of less or the same amount of personal information, and that in any case that decision is not driven by the availability of the IVS, but rather by the individual agency's assessment of identity-related risk, and consequent required confidence levels. The rigour of the risk assessment is driven by the level of adherence to the EOI standard.

4.13. Two further features mitigate concerns about increased collection. First is the requirement of every service agency to maintain an alternative means of authenticating to the required level (so the presentation of the passport, for example, would have to remain an acceptable alternative to using the IVS). Second, the use of the IVS would not *necessarily* result in the collection of more personal information by the service agency. As is discussed further elsewhere, the user gets to decide which (if any) of the items of the IVC are sent to the service agency (albeit possibly as a precondition of using that service online). However the service agencies' requirements should be no different from an offline service. That is, if the service agency does not need to know the place of birth of a service user, or the birth name of the service user's mother, it should not collect it as one of the IVC elements *or* in an offline context. Conversely if the service agency decides that its verification of identity requirements include receiving and checking those data items they should be collecting those items of information in the offline context as well. The existence of the IVS should not affect those decisions.

4.14. The retention of personal information may change the net information holdings of service agencies. For example, if in the past an agency has required verification of identity, that may have been met simply by an official seeing, but not noting the details of, an ID document such as a drivers licence. With the IVS, the personal information will be transmitted as part of the IVC, and retained by the service agency. This is not counted as significant in this analysis for three reasons. First, this change will be a factor of the EOI standard, not the IVS. Secondly, in the first example, the official is *verifying* personal information, therefore they already have personal information against which to compare the ID document. Finally, the fact that other forms of document, which were created for other purposes no longer need to be produced for noting (and often an official will make a record of the passport number, or driver licence number) might just as well *reduce* the net personal information collected by the service agency.

4.15. The idea of "authentication inflation" however, remains a privacy risk, and was commented on at length in the earlier privacy impact reports.

4.16. Over time, though, as the IVS becomes the standard means of authentication, it may mean that the requirements of all service agencies rise to meet the IVS standard. The IVC will be good for (almost all) purposes, therefore, even though for many online services it will be more than is strictly

needed, the option of service agencies abandoning any separate independent verification at the lower level, and simply opting for the IVS may look more attractive. This might even be demanded by users. If a service user has gone to the trouble of obtaining a "gold standard" IVC through the IVS, in most cases they would want to use that credential for any lesser level of verification required for their online activities. The attraction is such that they should be allowed to choose to do so. Privacy concerns should not restrict the free choice of an informed person to organise themselves for online business in the most efficient way possible. It would be a nuisance and counterintuitive to have to reauthenticate to lower levels to access lower risk online services, when the IVC would serve perfectly well.

4.17. The response to this concern is that if realised, it would represent a failure of the EOI standard, and the Cabinet principles. The standard requires that agencies require the lowest level of identity verification consistent with the level of identity risk represented by the service.

4.18. To an outside observer, a standard as opposed to regulations or an Act of Parliament may appear a weak response to privacy concerns. Standards lack prescription, sanction and enforcement. They are essentially bureaucratic or administrative instruments that do not deliver remedies and are not, in the legal sense, mandatory.

4.19. In defence of the standard however, it must be noted that in a service that is limited to Government to People, administrative remedies do have some force. To bureaucrats Cabinet directives are mandatory. The EOI standard for example will go through a process of development, and testing, and will then be incorporated into a Cabinet mandated e-government interoperability framework (e-GIF) where it will, over time, achieve a "recommended" status. Once it has been proven to work effectively, it will formally become mandatory for all public sector agencies.

4.20. On balance, the IPP 1 risks associated with the IVS would not seem significant, although whether the kinds of risks of "authentication inflation" discussed here could eventuate depends on adherence to the standards. As a minimum, the standards should clearly articulate that principles of lowest levels of authentication, and of minimum information collection.

4.21. The second issue associated with this principle has been much discussed during previous processes of privacy impact assessment. This is whether the systems can and/ or should accommodate multiple identities. The current model emphatically denies the possibility. One person can have one IVC only.

4.22. To some extent the debate around "multiple identities" which features in the PPP report, and in SSC's response may be based on different understandings of key terms. Those responsible for designing the IVS have a very precise and narrow meaning of the term "identity" in mind. It admits only one identity per person.

4.23. Privacy advocates speak of identity as an inherently contextual concept. This understanding of identity need not be fixed and constant. It can be subject to preferences of the individual concerned ("I do not choose to identify as a New Zealander"). Identity as conceived by the project is not mutable or selective. It is singular, unitary and fixed. It is not subject to the whim or preference or control of the individual to whom it is affixed. It is a purely objective measure.

4.24. In order to usefully discuss the privacy implications of the latter model in relation to the IVS, it is important to understand the true nature of the concerns underlying the privacy lobby's attachment to the former.

4.25. The principle underlying concern with a fixed and constant identity is that it can facilitate the connection of different "roles" (the project team's preferred alternative to the broader meaning of "identity" attributed to privacy advocates above). That is, restricting individuals to one set of data which links them to one official construct of identity, can deny their choice to identify themselves to different agencies in different ways for different purposes. Thus, a person needing to interact with Inland Revenue in their capacity as an employee of an organisation, for that organisation's tax purposes, might choose a different means of identifying themselves, (arguably a different "identity") when it comes to their own capacity (or role, or identity) as an individual taxpayer. An employee of a local authority might be known to the rates department of that authority in a different way to which she is known as an employee, or as user of noise control services.

4.26. The concern is that requiring reduction of each individual to a single "verifiable" identity might undermine some of these choices and autonomy, and might facilitate the bringing together of information about these different roles in order to build an otherwise unavailable picture of the person as a whole.

4.27. The two positions were reduced to their essence in the response to one of the recommendations of the PPP PIA:

PPP Recommendation	SSC Response
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)	Disagreed. This will potentially increase the amount of information held by the Authentication Agency about an individual as further information about them will be required with respect to the various identities they may have for different roles they have. In addition, linking of multiple identified likely to be technically complex and expensive. Further discussion – RC input.

4.28. The State Services Commission also noted that it disagreed with the recommendation on the grounds that "*It is a fundamental tenet of the project that there is only one identity per individual. It is accepted that a single individual may use multiple names and assume multiple roles but it is our view that ultimately there is only one identity…The assessor has adopted a definition of identity that is at variance to the definitions used by government agencies in New Zealand*".

4.29. Rather than discussing the contentious issue of terminology, (identity, multiple identities, roles), it is probably more productive to focus on the concerns underlying the apparent dispute. To the extent that issues of individual preference as to declared identity are at the heart of the privacy concerns outlined in the earlier papers, there are two responses. First, the IVS will only be used to authenticate for access to services where the highest level of confidence is required. Applying the EOI standard (which was not available to the earlier privacy impact assessors), it is difficult to conceive of any service using the IVS where the process of authentication would be able to use some alternative "identity" to that reflected in other official documents of the sort used to authenticate offline.

4.30. Secondly, if by multiple identities the earlier assessors mean multiple names, the IVS design now does allow multiple names (subject of course to passing the test of "evidence of use in the community"). The user will be able to select which name can be transmitted by the IVS to the service agency.

4.31. This solution appears to better preserve privacy (where privacy is understood to mean the preservation or personal autonomy), in that the alternative, off line systems of authentication are less likely to accommodate multiple names. For example, it is not possible to obtain a passport in several names at the same time.

4.32. The other privacy concern apparently underlying the desire for the system to accommodate "multiple identities" is to avoid the capacity for a central agency to link the various "roles" or self selected "identities" with which

individuals conduct their everyday transactions. The project response to this concern is to make it almost impossible to link data associated with those roles in a practical sense. The means by which this is intended to be achieved is discussed elsewhere in this paper (the issue is less one of collection of personal information under IPP 1 – than of aggregation, and unanticipated uses of personal information under IPP 10), but the principle mechanism is the use of numbers identifying the IVCN which are unique to each service agency, and the limits on use of the IVC as a whole as an identifier (both points illustrated by the table in paragraph 3.18 above).

4.33. The effect of this design is to achieve the outcome sought in the earlier privacy impact report that "*the interest of many individuals in maintaining separate 'silos' of information representing their separate interactions with unrelated areas of government*", in that the MIVCN concept provides each silo of government with identity data appropriate to it with no new unique identifier that enables tracking across the silos.

4.34. An earlier draft of this report also suggested that a failure to permit several identities may undermine the voluntary nature of the scheme. It was proposed that if an employee is required to conduct transactions online for their employer, they might have to obtain an IVC, regardless of ethical or other objections. However, it was pointed out in response, that for that individual the service agency would have to maintain an offline alternative for establishment and verification of identity, and as such the voluntary nature of the IVS will not be vulnerable to coercion of employers.

4.35. It is unlikely that the concerns underlying the "multiple identities" proposal will be realised if service agencies do adhere to the EOI standard, and only require appropriate use of the IVS. With multiple lower level authentication processes (i.e. not requiring IVS verification) concerned individuals can, in effect maintain multiple online identities. Where the IVS is involved however, except in the very narrow circumstances (yet to be defined, for personal safety etc), there will only be one identity.

4.36. Since the Pacific Privacy Partners reports were prepared, further work on the GLS has embedded the idea of multiple keys, with keys held by the same individual not necessarily all linked to that individual by the RKSN or otherwise. This goes some considerable way to addressing the concerns about a single credential system, but it remains vulnerable to the confidence level inflation discussed above. While not an unequivocally, or exclusively negative privacy value, the real risk with the intrusions into the opt in system, and the increasing pressure toward single credentials is as the second PPP report notes:

> The foundation that this lays for a population register and national identity system, … remains a major privacy risk for the proposed scheme.

4.37. Two points should be added to that conclusion. First, the GLS and IVS are not designed to allow the aggregation of information about access to service agencies or transactions conducted via those systems. Secondly, it is possible to argue that rather than address now (for example by legislation) the risk that the IVS might become "the foundation for a population register and national identity system" it should be recognised that to achieve the aim of a national identity system would require empowering legislation to make mandatory the obtaining of an IVC (whether subsequently to be used or not). Arguably that would be the appropriate time to have the debate about whether or not such a scheme is warranted.

4.38. Contrary to the view expressed by Pacific Privacy Partners, it does not necessarily follow that the scheme will unavoidably lay the foundation for a identity card system. The foundation is arguably there already, in the births registers and deaths registers, the passport and citizenship databases, although it is legitimate to note, in favour of requiring that the IVS be established under legislation that many of those existing national databases already have a statutory basis (even though some, like the national health index, and the national student index, do not).

4.39. Like passports, the IVC cannot become mandatory without legal intervention. A passport is only required for travel. An IVC is only required for (some) online transactions. People who do not which to carry on online transactions need not obtain an IVC. Whether IVCs become a de facto necessity is subject to some debate and conjecture, and depends to a considerable degree on service agencies adhering to the requirement that they maintain alternative, offline means of accessing services.

4.40. One further concern needs to be elaborated however. The scope for the extension of the IVS "client base" beyond the public service does further challenge the "opt in" principle. The private sector will not be subject to the Cabinet restrictions. It is not inconceivable that utilities companies, banks and the like will further reduce their offline presence, requiring more people to interact online. It would not take many oligopolies to alight on the IVS before the service was effectively compulsory for all in the market place. This point does not require further comment, as the G2P scope of the project is set out in the "critical assumptions" part of this paper at paragraph 1.13.

4.41. As noted also in the GLS PIA, one commentator has suggested that:

Electronic authentication is qualitatively different for the public sector and the private sector because of a government's unique relationship with its citizens:

a. Many of the transactions are mandatory
b. Government agencies cannot choose to serve only selected market segments. Thus, the user population with which they must deal is very heterogeneous and may be difficult to serve electronically

c. Relationships between governments and citizens are sometimes cradle to grave but characterized by intermittent contacts, which creates challenges for technical authentication solutions

d. Individuals may have higher expectations for government agencies than for other organisations when it comes to protecting the security and privacy of personal data.[2]

4.42. These comments are equally valid for the New Zealand situation. At the very least, officials should consider seeking a Cabinet decision *restricting* the expansion of the scheme beyond the whole of government, pending analysis and public consultation. The current Cabinet decisions would appear to be insufficient, in that they *permit* the use of the scheme across the whole of government, but do not limit further expansion.

4.43. **Information Privacy Principle 2** is a statement of best practice, that personal information should be collected directly from the subject of the information.

4.44. The IVS has a component of collection of personal information from third parties that warrants further exploration. The IVS requires third party verification of the link between a photograph and a stated identity. This is not a breach of the information privacy principle, because it is with the consent of the person concerned (the applicant). What this information is used for, how the service responds where the third party does not verify the photograph, who can access it and for how long it should be retained are issues that arise under other principles below.

4.45. **Information privacy principle 3** requires transparency between the collector of personal information, and the subject as to why the information is being collected, to whom it will be disclosed, whether the collection is voluntary or mandatory and so on.

4.46. The way in which such a statement is drafted can influence the potential for scope creep. No such statement has yet been prepared by the SSC or DIA, but the statement should be closely scrutinised from a privacy perspective when a draft is to hand. Having a tightly drafted statement of purposes as part of the terms and conditions on which the IVC is issued will also provide consumers with a level of contractual protection absent in many interactions with government agencies.

4.47. The IPP 3 statements and terms and conditions of issuance of an IVC ought to explicitly describe and proscribe the uses and limits on use of the credential, and the IVS' undertakings as to the policy settings under which the credential is issued (eg limiting to government only), thereby enabling an individual to "opt out" if the service were opened to wider use.

[2] Who Goes There p12

4.48. **Information privacy principle 4** proscribes the collection of personal information in ways that are unlawful, unfair, or that intrude to an unreasonable degree into the personal affairs of the individual. There is nothing to indicate that any part of the project will breach this principle.

Use, disclosure and retention of personal information

4.49. **Information privacy principle 5** requires that an agency that holds personal information must ensure that it is protected by adequate security safeguards against loss misuse or unauthorised access.

4.50. Many of the issues in relation to the GLS part of the project apply equally to the IVS. In one sense, the project is all about security, and is security enhancing, given the potential to deliver reliable and trusted access to online services. However the same frailties that apply in relation to the GLS are also a risk to the IVS.

4.51. While security is central to the effective operation of the IVS, and the way in which the IVC is managed, and the MIVCN is transmitted, have significant implications for information privacy, a detailed discussion of technological solutions to security weaknesses need not form a substantial part of this report.

4.52. The credibility and uptake of the project as a whole depends on rigorous adherence to high standards of security. IT project teams are well equipped to assess security requirements and ensure state of the art responses to weakness, far more so than privacy lawyers. Rather than make specific findings and recommendations about the security requirements of the project, it is sufficient for the purposes of privacy impact analysis to recommend that a full security assessment and audit should be part of the process of going to tender, monitoring the build and ongoing operation and that the systems are consistent with the standards devised for online communications in government by the Government Communications Security Bureau.

4.53. **Information privacy principle 6** provides that individuals are entitled to have access to information about themselves. Nothing in any of the project documentation indicates any intention to restrict or reduce this right.

4.54. The right to have access to information is an essential means that individuals have of holding agencies to account. IPP 6 will give any applicant the right, for example to access information as to the reasons an IVC has not been issued. The strength and enforceability of the right in the existing law means there does not need to be any enhancement of the right in any empowering legislation dealing with the IVS. There may be legitimate restrictions on the right of access, such as those provided in the Privacy Act, to protect security and defence, the maintenance of the law, and the affairs of third parties (such as

informants and trusted third parties), however, nothing in the IVS is sufficiently distinct to warrant a separate set of rules, or to raise unique issues that have not already be dealt with adequately in other contexts.

4.55. **Information privacy principle 7** gives individuals a right to correct information that is incorrect, out of date or misleading.

4.56. Like information privacy principle 6, this principle has proved durable and sufficient in a wide variety of circumstances. Aspects of the principle do create challenges for the designers of computer systems however. For example, the principle requires that where an agency refuses to correct an item of personal information, the individual can ask a statement of the correction sought but not made be attached to the information, and that the agency must then;

> take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought

4.57. Some consideration of this requirement will be needed in the detailed design of the system to ensure that statements can be accommodated where practicable.

4.58. **Information privacy principle 8** requires that agencies should not use personal information before taking such steps if any as are necessary to ensure that the information is complete accurate up to date and not misleading.

4.59. This principle can be helpful in identifying vulnerabilities in a system of automated decision making.

4.60. The IVS has several points of automated verification, such as in the information matches with the birth register, and the death register, and other source documents. The principle requires that before declining to issue an IVC on the basis of some defect in the information supplied as compared against the official documents held, the IVS should take reasonable steps to confirm the accuracy and currency of its conclusions. The processes documented in the project documentation ought to ensure compliance with this principle, and avoid actions taken on the basis of out of date or inaccurate information. If (as is planned) the matches with the public registers are to be information matches under the Privacy Act, further steps to ensure individuals are given an opportunity to comment on an apparent discrepancy will be a legal obligation, as "adverse action" notices will need to be sent to the applicant prior to declining the application for an IVC. As a default position, in the absence of the yet to come detailed process design, the business processes to be adopted are intended to mirror those followed in the passport application process. Errors in applications, risk profiles, and the means of follow up discrepancies will be as if the same issues arose in the course of assessing an application for a passport.

This seems an appropriate response in relation to an electronic evidence of identity system which is to have the same high level of confidence as a passport.

4.61. As discussed above, matching the photograph derived biometric on a "one to many" basis may not yet be viable given the reliability of the technology. Launching such a process prior to being satisfied of a very high level of confidence in the technology would have significant privacy risks related to this principle.

4.62. An issue that was subject to some discussion earlier in the project design phase was the level of detail, or data elements that should be transmitted by the IVS to the service agency in order to enable the parties to understand where a discrepancy between the personal information held by the service agency, and that held by the IVS as part of the IVC might reside. The most recent iteration of the project plan available to this privacy impact assessment appears to strike an appropriate balance, by enabling the user to determine which parts of the credential (except the IVCN) are transmitted to the service agency.

4.63. The PPP report said:

> 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[3]. 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?

4.64. The response to this is the default position mentioned above. The same process will be used as is used for passports. This seems appropriate.

4.65. **Information privacy principle 9** requires that personal information should not be retained for longer than is required for a lawful purpose.

4.66. Issues arising under this principle can be categorised as either relating to the identity information, or to the transaction information. In other words, the retention of the application, the expiry of the IVC, the ongoing retention of the biometrics etc all relate to the identity, and the ongoing record of frequency and instances of use of the IVC related to transactions.

4.67. The IVS position in relation to the former category is that the information must be retained indefinitely, presumably according to the theory that identity is a single, constant concept, lasting over the life of the individual. However, given that an IVC is voluntary – people choose to acquire one if they wish to transact certain business online, it is difficult to see why they would not be

[3] 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.

equally free to relinquish the IVC, and in doing so, remove the legitimacy for the IVS' retention of the associated data. If the scheme is to adhere to the "opt in" principle required by Cabinet, it must also provide an "opt out".

4.68. Having said that, while the IVC remains in use, there are good reasons to justify the ongoing retention of all information associated with it, in case questions arise, such as the IVC turns out to have been incorrectly issued.

4.69. The scheme intends to expire the IVC every five years, so that users have to resubmit applications, provide a fresh photograph, and be reverified. If the individual chooses not to reactivate their expired IVC, consideration should be given to purging the record associated with that IVC. The IVS should notify users of the impending expiry of the IVC a reasonable time in advance to enable them to renew it without disrupting their ability to conduct online transactions.

Recommendation 4
The IVS should notify users of the impending expiry of the IVC a reasonable time in advance.

4.70. There is an even stronger case for non-retention of the transaction information. Although the record is likely to show no more than the date and time that the IVC was presented to a specified service agency, there is potential for the service to generate considerable profiles on online activity. This potential is multiplied by a considerable degree if the use of the IVC expands to the private sector. Retention for a certain period will be necessary for audit purposes, although these should be limited. The more important auditing function will be at the service agencies, which will record the details of the presentation of a credential linked with the transaction details, regardless of the IVS's retention policy.

4.71. Arguments have been presented that law enforcement and audit purposes demand indefinite retention of all elements. However, a compelling case with examples, broken down into the categories of information has not yet been made, and as such the nascent retention policy resembles more of a "just in case" justification than a demonstrable need. Further analysis is needed to establish legitimate periods of retention for each category of personal information, namely;

4.71.1. Information associated with the application for the IVC
4.71.2. The IVC itself
4.71.3. Information associated with the use of the IVC.

4.72. It should be noted that there may also be privacy benefits in retaining credential information, to assist the individual concerned in tracing transactions, and proving or disproving they have done certain things, and in facilitating the issue of a new IVC without the need to go through the full EOI process. These issues need to be weighed and balanced and reflected in the final policy. Where

assumptions of a benefit to the individual concerned is the defining factor in a particular policy however, there is usually no reason why the individuals preferences as to retention cannot be determinative of the agencies authority to retain the personal information.

4.73. System designers should be asked to consider ways of limiting what can be gleaned from data collected at every stage. For example, if a user obtains an IVC, and uses it with service agency 1, an MIVCN for that agency will be created at that time. Later MIVCNs will be added, showing a pattern, and sequence of use to a subsequent observer of the record. It may be that each IVC could have a prepopulated set of MIVCNs for a range of agencies when created to avoid the disclosure of the pattern. However, not all users will want to use the IVC for all agencies, and the storage space such a table would require may mean the idea is not practicable, but nonetheless the idea, and similar should be explored in the design stage.

4.74. **Information privacy principle 10** restricts permitted uses of personal information.

4.75. This principle has a number of implications for the service. First, the creation of the IVC involves the use of a number of government databases, arguably for purposes other than those for which the personal information on those databases was collected.

4.76. In the case of the IVS, it would clearly be arguable that those uses for the purposes of verifying identity are not a breach of IPP 10, first because the births register and deaths register are public registers, and second because for the purposes of applying for the IVC, the individual authorises the use of those other databases for that purpose.

4.77. Nonetheless, there may well be good reasons to characterise the IVS' use of those databases as "information matching programmes" which will impose a higher level of transparency, and regulation on the service. Doing so will also embed the idea that although inhabiting the same corporate structure, the IVS is a separate entity requiring specific authorisation to access other DIA databases for unrelated purposes.

4.78. The greatest concern with any centralised system of authentication is the potential for the collating of data that would otherwise be disparate, enabling "profiles" to be generated of consumption habits or other values particularly where establishment and confirmation of identity are not separated and no opportunity is provided to users to set up multiple identifiers. Such concerns have fuelled debate about other authentication systems such as Microsoft Passport[4]. A distinguishing feature of the IVS design from other federated authentication systems is the separation between verification of identity (by the

[4] http://www.epic.org/privacy/consumer/microsoft/passport.html

IVS), and the ongoing usage (by the GLS), which inhibits the aggregation of information about transactions and usage patterns of particular individuals.

4.79. Again there is room for debate as to whether the Privacy Act is sufficient to deliver a protection against the IVS making novel or undeclared uses of even the limited transaction information the system creates to generate the kinds of profiles that alarm privacy advocates. If there is to be a legislative basis for the IVS, it would be a simple matter to declare in statute the purposes for which the IVS can use information it collects. However in the absence of a clear and explicit statutory basis, the IVS is vulnerable to new Cabinet declarations changing the nature of the organisation, and broadening the purposes for which it is entitled to use the personal information it holds.

4.80. A more specific issue relates to the use of the photo biometric. The Pacific Privacy Partners report recommended that the authorising legislation should expressly limit the purposes for which the photograph, digital image or biometric of the image can be used. Such restrictions would be consistent with the approach taken to photographs on drivers licences (Land Transport Act 1998 s.200 refers). This report concurs with that conclusion.

4.81. Care also needs to be taken about the uses to which the trusted referee information can be put. For example, "A" might verify "B's" identity for the purposes of obtaining an IVC, and then later also verify "C", who it transpires has fraudulently applied for the IVC. Care should be taken in making assumptions about the validity of "B's" credential based on the discredited application from "C".

4.82. Similarly, the trusted referee field in the database might well prove to be a valuable resource for ascertaining relationships between individuals. Mechanisms to avoid improper use of that information should be adopted to avoid snooping, and the implications of "guilt by association". In addition to the obvious competing maintenance of the law vs privacy interests here, policy will also be informed by something approximating a market approach. That is, it is in the interests of the system that people are encouraged to, and not discouraged from volunteering to act as trusted referees. Any official overuse, or over-intrusive use of trusted referee information will act as a disincentive to referees.

4.83. The project documentation does not disclose any policy for dealing with declined or withdrawn applications, individuals who, because they fit a risk profiling algorithm warrant closer inspection prior to issuing of the IVC and the like. As with many of the issues raised about aspects of design which have not been finalised, the default position, that the same rules as apply to passport applications are likely to apply would appear to be an appropriate response.

4.84. **Information privacy principle 11** restricts the agencies to which personal information may be disclosed.

4.85. Discussions about information privacy are often dominated by issues of disclosure of information from one agency to another. However, in many cases, the intended interagency flows of personal information turn out not to be the most significant features of the project.

4.86. In the case of the IVS, the service resides within the Department of Internal Affairs. There is no issue with the transmission of the verification information to and from the different registers, also housed in that department. The most significant issue is the question of how much personal information needs to be disclosed by the service to service agencies when verifying the identity, the whole IVC, just a part of it, or simply an assertion of verification/failure of verification. These issues are discussed above. There are positive and negative privacy implications for each option. On balance, enabling the individual to choose what components of the IVC to transmit seems the best solution.

4.87. The other significant disclosure issue is the dissemination of the IVCN. That this is a potentially critical area for enabling or restricting the ability to aggregate information across disparate data sources has been recognised by the project team. The design solution to this has been to send only a modified IVCN, which is unique to the individual and service agency, so that no two agencies have the same reference number.

4.88. There is a real question as to whether the IVS should be disclosing a data item such as “mother’s birth name” to a service agency, as part of its required IVC components, however, given the design parameters, any such disclosure would be by consent and therefore not a breach of IPP 11 by the IVS. The real issue however, is whether the service agency has any need to collect such information, given that it has no role in ongoing verification of identity. As such a full response to this question is expected as part of the response to the issues raised under IPP 1.

4.89. The Official Information Act will no doubt apply to the IVS, as a public sector organisation, which means that anyone will be able to ask for access to any IVC. In practice, requests are likely to be declined on the basis privacy protection under section 9(2)(a) of the Act, however, those decisions are made on a case by case basis, and do not provide users with certainty that their information will be prevented from disclosure. The alternative is to explicitly exempt individuals IVCs and associated data, such as transaction logs from coverage of that Act. This should be considered as part of any legislation.

Recommendation 5

Consideration should be given to exempting personal information collected in connection with IVCs from coverage by the OIA.

4.90. **Information privacy principle 12** seeks to restrict the assignment and use of unique identifiers. The creation of a universal unique identifier is one of the principle areas of resistance toward centralised authentication systems. The reasons for the sensitivity are various, but mostly revolve around the ready ability to link records across agencies by using a common identifier, and the step toward a mandatory document of identity that universal identifiers represent.

4.91. The term "unique identifier" is defined in the Privacy Act as meaning:

> … an identifier—
> (a) That is assigned to an individual by an agency for the purposes of the operations of the agency; and
> (b) That uniquely identifies that individual in relation to that agency;—
> but, for the avoidance of doubt, does not include an individual's name used to identify that individual:

4.92. As discussed above, the IVCN is the most obvious candidate to be considered a unique identifier, however its intended limited circulation, and masking by use of the MIVCN when being transmitted to service agencies removes many of the threats associated with unique identifiers. A different MIVCN will be generated for each service agency to which an IVC is sent, thereby limiting both the potential for the service agency to assign the same unique identifier as the IVS or another service agency, and preventing the number from being used to aggregate data or profiles from different agencies.

4.93. Any use of a common MIVCN for particular sector authentication (such as a one point of authentication for the health sector, or for the education sector) will need to comply with IPP 12 or the relevant codes of practice in operation. Proposals to strengthen the enforcement of IPP 12 are included in reform of the Privacy Act, and will act as a considerable incentive to service agencies to ensure they have the appropriate authority before enabling multi-agency, sector wide use of the new identifiers.

Other Privacy Issues

The information privacy principles are not the only source of privacy risk measurement.

4.94. As touched on above, one of the principle concerns of privacy watchers is the development of national identity cards. There are several reasons for the concern. One is that for an identity card to be unique, it needs to be associated with unique number. The IVCN could serve that function. If a trusted identity card becomes the principle means by which agencies identify and refer to individuals individual dignity and humanity can be reduced, as people are described as "just a number". The use of a number also can facilitate the

aggregation of information across a range of agencies, that has been collected for a variety of purposes.

4.95. The potential to use such a facility to centralise a database of information about individuals, to crunch data to learn their habits and patterns and to trace their movements and transactions is of course anathema to privacy advocates. It is this concern which underpins the design, with the separation of the verification from ongoing use, and the use of MIVCNs and MKSNs.

4.96. These concerns are at the heart of some of the design parameters of both the GLS and the IVS. In accordance with the Cabinet principles, there has been adherence to the "opt in", or voluntariness principle. The systems are designed to make matching of information using any of the numbers used in the online process very difficult, if not impossible. In this respect, the design is commendable. The concerns associated with the authentication scheme laying the foundation for a national identity card system is allayed somewhat although not eliminated by conformance to the Cabinet policy and implementation principles.

4.97. However, another of the concerns about identity cards may not have been removed in the design, of the services and supporting systems. That is the sense of intrusion when an identity card is demanded. People who have lived through oppressive regimes in which pass cards, or legal requirements to constantly carry identity papers have been part of the machinery of subjugation, report the feelings of fear and powerlessness attendant on random demands for inspection of their papers/cards.

4.98. The point should not be overstated, and is not universally accepted. For example, objections to centralised instruments of identity verification is mostly a feature of Anglo-Saxon jurisdictions. However in our region there is a strong tradition of antipathy toward such schemes.

4.99. However, given that the authentication project involves new technologies, it is important to attempt to analyse and understand consequences that have not been anticipated.

4.100. In this regard it may be that there is little difference to the liberty of the person concerned if they are stopped in the street and asked to produce a document of identity, or invited to logon to a site via a mobile device to prove that they are who they say they are. Whether the potential for the service to be used as an "on demand" verification of identity, even in the absence of a physical document recording identity warrants regulation depends on the technology, and scope of access to the service. This element may warrants further consideration at a later stage.

4.101. At this stage of the project however such speculations are not particularly revealing as to the foreseeable privacy impacts of the IVS and online authentication generally. For such a potential to be realised, and for the IVC to become kind of virtual ID card, permitting regular intrusive and coercive interventions by the state, enabling legislation would be required. The time when such steps were proposed would be the appropriate time to debate the relative tradeoffs to privacy and law enforcement or legitimate public policy objectives.

4.102. The scope for the scheme to lay the foundation for a national register of identity, which in turn could be easily converted into identity cards, would be significantly increased if the scheme were opened up to the private sector.

4.103. Concerns about moving toward a national register of identity, or a de facto, or de jure system of compulsory identity cards are arguably sufficient to warrant some regulation proscribing the ways in which the IVS operates. Without regulation the argument runs, all that protects privacy is the very general Privacy Act, and a range of administrative instruments and the best intentions of officials. The promise that the IVS will remain restricted to government, and that alternative means of authentication must continue to be offered, are simply promises that can be reneged on by the next wave of bureaucrats and/or politicians.

4.104. On the other hand, there are a wide range of other possible instruments to form the basis of a national ID card that are far more advanced, and readily convertible. These include drivers licences, the National Health Index, the National Student Index, or the passport and births, deaths and marriages registers themselves. Some of these would require legislation to exploit, but others, such as the NHI, exist without statutory authority at present, and therefore can be expanded in scope without the necessity for any further legal authority. The fact that such systems exist, (unregulated except, as will be the IVS, by the Privacy Act) at a significantly more advanced state is an argument in itself against specific legislation to regulate the IVS simply to avoid an ID card system.

5. Privacy Risk Assessment

5.1. Any centralised system of identity establishment and verification has very considerable privacy implications.

5.2. Privacy has been central to the development of the project, a fact reflected in both in the Cabinet principles, and in the way that many of the concerns pointed out in the earlier privacy impact assessment have been addressed.

5.3. The risks that remain are in the main, contingent and inherent. That is, there is very little in the design that could be characterised as a breach of privacy if the

scheme operates as currently intended. The risks relate to further expansions and as yet unanticipated developments probably contrary to the Cabinet principles.

5.4. The inherent privacy objection is that which says "why should the government be in the business of confirming identities for online activities". The answer to that question is probably, "because there is a demand for it, and the government is best placed to deliver the service". Provided it is voluntary, why should those who do not wish to avail themselves of the benefits of the convenience of online transactions care about the system built for those who do?

5.5. There are two responses to such a "brush off" of privacy concerns. First, the scheme potentially affects everyone in New Zealand. Even if I do not wish to obtain an IVC, one of the other John Edwards' in the country may apply, and that application may involve access to my identity documents, mistakes and identity confusion. Secondly, if the system does, as a by product lay a foundation for a scheme that could later be easily converted to a compulsory (de facto or de jure) system, or used to issue identity cards, it is in the wider interest of the community to have some of that discussion now, rather than on the occurrence of the contingency event. This latter point is addressed in para 4.94 above. For that issue, perhaps the best that can be expected is an undertaking to thoroughly examine the privacy impacts of any change in scope that increases the likelihood of the creation of a national database of identity. The former concern is not so readily dismissed, and does demand a more tangible commitment to protect the rights of those who elect not to be a part of the opt in system.

6. Privacy Enhancing Responses

Institutional responses

6.1. The earlier privacy impact assessments made a number of recommendations as to the constitution and governance of the institutions involved in delivering authentication solutions.

6.2. If legislation is to be used as a mechanism for achieving privacy assurances, there would not appear to be a compelling case for elaborate institutional arrangements to oversee the work of the IVS. In other words, provided legislation specifies the permitted/prohibited uses of the information, it does not matter if the legislation imposes the rights and obligations on a stand-alone independent crown entity, a government department, or an individual such as a "registrar of identity verification services" or "the chief executive for the time being appointed by the State Services Commissioner to administer the identity verification service". Policy considerations other than relating to privacy will probably determine which is the preferable institutional or regulatory model.

6.3. Some brief discussion of suitable oversight and monitoring bodies is also warranted. There is clearly no compelling case for any new agency to oversee

the work of the agency. The existing monitoring and complaint investigation agencies such as the Ombudsman, the Privacy Commissioner, the Controller and Auditor General, and Parliament should, between them, suffice.

Policy and legislative responses

6.4. The first paragraph of Chapter one of the Legislation Advisory Committee Guidelines on Process and Content says:

> A decision to prepare new legislation should not be taken lightly, as the development and implementation of new legislation often involves significant costs for the community. These costs include the direct development costs, the time and expenses of those who review draft legislation, the costs of the enactment process, printing and publication costs, and the time and expenses of those who need to adjust to, learn about, enforce, administer, implement, or comply with the new legislation.

6.5. The LAC Guidelines go on to list the possible alternatives to legislation:

- no government intervention;
- status quo;
- use of existing law;
- increasing enforcement;
- information and education campaigns;
- economic instruments (taxes, subsidies, and tradable property rights);
- voluntary standards/codes of practice;
- self regulation; and
- co-regulation.

6.6. It is for policy makers to determine whether legislation is warranted to provide for the scheme. There appears to be no compelling case that legislation is *necessary* as in a prerequisite for any aspect of the scheme, in the sense that the scheme would be unlawful without authorising legislation. Given the way in which access to some public registers administered by the Department of Internal Affairs is regulated, it is arguable that the use of those registers for IVS purposes would require specific legislation, however, given the consent basis of the transactions, it is likely that a way could be found to conduct all the necessary checks without specific authorising powers.

6.7. The Privacy Act and Ombudsmen Act already deliver a readily accessible remedy for anyone believing they have been treated improperly by a government agency.

6.8. Given the contingent nature of the most prominent privacy concerns, legislation cannot be said to be required to prevent those concerns from being realised, as for a national identity card system to be implemented off the back of the IVS online authentication system would itself require legislation. The public debate about relative merits, and balance could occur then.

6.9. There are also arguments against legislation. One is that if the service is established with a legislative mandate, it may lose some of the voluntary "market based" character that might well better serve privacy objectives. If the IVS has to structure its policies and procedures in a service-oriented way, and sell the service to a willing public without any statutory backing, it may be more sensitive to the privacy concerns of its client base than would be the case if it were simply discharging bureaucratic statutory functions. There are privacy risks in legislation, in that as the Bill passes through the House, legislators may decide that other values (security etc) are more important, and pass amendments to that effect. Without a legislative vehicle, that possibility does not so readily arise.

6.10. If legislation were to be proposed, a minimalist approach of the key elements would include:

- Establishment of the IVS (in any of the forms suggested above, at its simplest, this could simply be a statutory officer, eg the Registrar of Online Identity Verification)
- Extending the Privacy Act to have extraterritorial effect for users of the IVS.
- Description of scope and purpose (limiting scope to public sector, limiting use of IVC to online transactions), requiring the maintenance of alternative/offline means of authentication.
- Limitations on the use of the photograph image and biometric (such as in s.200 Land Transport Act)
- Constituting new information matching programmes for access to other DIA registers for purposes of issuing IVC.

7. Summary of Recommendations

Recommendation 1

That further privacy impact assessments should be undertaken before

- Any proposed amendments to the Cabinet principles specified in paragraph 3.20 are put to Cabinet.
- Any proposal to relax the requirement that service agencies are obliged to provide alternative offline means of establishment of identity are considered.
- Any expansion of the use of the IVS and IVC beyond individuals transacting with Government Agencies (G2P) is proposed.
- Any substantial amendments to the EOI standard or the requirement on agencies to comply with the standard are made.

- Any changes to the IVS or IVC that would lead to the greater central collection of personal information are proposed.
- Photo biometrics are used for "one to many" matches with any government photo biometric database.
- Any exemptions from information privacy principle 12 are proposed to accommodate wider use of unique identifiers associated with the IVS.
- Operational documents supporting the IVS, such as access agreements, memoranda of understanding, standards and the like are put in place.

Recommendation 2
That the IVS maintain and regularly report to its governing body on a privacy risk register, such a register to include risks such as:

- That the proposed systems of monitoring and control of service agencies will not be adequate to ensure adherence to the EOI standard and other central controls such as e-GIF.
- Replacement of existing lower-level authentication with high confidence requirements necessitating wider than currently anticipated us of the IVS & IVC.
- Weakening of alternative (ie non-IVS) forms of online or off-line authentication.

Recommendation 3
The Privacy Act should be amended to provide for its extraterritorial application for users of the IVS.

Recommendation 4
The IVS should notify users of the impending expiry of the IVC a reasonable time in advance.

Recommendation 5
Consideration should be given to exempting personal information collected in connection with IVCs from coverage by the OIA.

Appendix 1- The Information Privacy Principles

INFORMATION PRIVACY PRINCIPLES

PRINCIPLE 1

Purpose of collection of personal information

Personal information shall not be collected by any agency unless--
(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and
(b) The collection of the information is necessary for that purpose.

PRINCIPLE 2

Source of personal information

(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.
(2) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,--

(a) That the information is publicly available information; or
(b) That the individual concerned authorises collection of the information from someone else; or
(c) That non-compliance would not prejudice the interests of the individual concerned; or
(d) That non-compliance is necessary--
    (i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or
    (ii) For the enforcement of a law imposing a pecuniary penalty; or
    (iii) For the protection of the public revenue; or
    (iv) For the conduct of proceedings before any court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation); or
(e) That compliance would prejudice the purposes of the collection; or
(f) That compliance is not reasonably practicable in the circumstances of the particular case; or
(g) That the information--

(i) Will not be used in a form in which the individual concerned is identified; or
(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
(h) That the collection of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 3

Collection of information from subject

(1) Where an agency collects personal information directly from the individual concerned, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of--

(a) The fact that the information is being collected; and
(b) The purpose for which the information is being collected; and
(c) The intended recipients of the information; and
(d) The name and address of--
(i) The agency that is collecting the information; and
(ii) The agency that will hold the information; and
(e) If the collection of the information is authorised or required by or under law,--
(i) The particular law by or under which the collection of the information is so authorised or required; and
(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and
(f) The consequences (if any) for that individual if all or any part of the requested information is not provided; and
(g) The rights of access to, and correction of, personal information provided by these principles.

(2) The steps referred to in subclause (1) of this principle shall be taken before the information is collected or, if that is not practicable, as soon as practicable after the information is collected.

(3) An agency is not required to take the steps referred to in subclause (1) of this principle in relation to the collection of information from an individual if that agency has taken those steps in relation to the collection, from that individual, of the same information or information of the same kind, on a recent previous occasion.

(4) It is not necessary for an agency to comply with subclause (1) of this principle if the agency believes, on reasonable grounds,--

(a) That non-compliance is authorised by the individual concerned; or
(b) That non-compliance would not prejudice the interests of the individual concerned; or
(c) That non-compliance is necessary--

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That compliance would prejudice the purposes of the collection; or

(e) That compliance is not reasonably practicable in the circumstances of the particular case; or

(f) That the information--

(i) Will not be used in a form in which the individual concerned is identified; or

(ii) Will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned.

PRINCIPLE 4

Manner of collection of personal information

Personal information shall not be collected by an agency--

(a) By unlawful means; or

(b) By means that, in the circumstances of the case,--

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

PRINCIPLE 5

Storage and security of personal information

An agency that holds personal information shall ensure--

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against--

(i) Loss; and

(ii) Access, use, modification, or disclosure, except with the authority of the agency that holds the information; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

PRINCIPLE 6

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled--

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with subclause (1) (b) of this principle, an individual is given access to personal information, the individual shall be advised that, under principle 7, the individual may request the correction of that information.

(3) The application of this principle is subject to the provisions of Parts IV and V of this Act.

PRINCIPLE 7

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled--

(a) To request correction of the information; and

(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information, in such a manner that it will always be read with the information, any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under subclause (2) or subclause (3) of this principle, the agency shall, if reasonably practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to subclause (1) of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

PRINCIPLE 8

Accuracy, etc., of personal information to be checked before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

PRINCIPLE 9

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

PRINCIPLE 10

Limits on use of personal information

An agency that holds personal information that was obtained in connection with one purpose shall not use the information for any other purpose unless the agency believes, on reasonable grounds,--

(a) That the source of the information is a publicly available publication; or

(b) That the use of the information for that other purpose is authorised by the individual concerned; or

(c) That non-compliance is necessary--

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(d) That the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to--

(i) Public health or public safety; or

(ii) The life or health of the individual concerned or another individual; or

(e) That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained; or

(f) That the information--

(i) Is used in a form in which the individual concerned is not identified; or

(ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) That the use of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 11

Limits on disclosure of personal information

An agency that holds personal information shall not disclose the information to a person or body or agency unless the agency believes, on reasonable grounds,--

(a) That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained; or

(b) That the source of the information is a publicly available publication; or

(c) That the disclosure is to the individual concerned; or

(d) That the disclosure is authorised by the individual concerned; or

(e) That non-compliance is necessary--

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences; or

(ii) For the enforcement of a law imposing a pecuniary penalty; or

(iii) For the protection of the public revenue; or

(iv) For the conduct of proceedings before any court or Tribunal (being proceedings that have been commenced or are reasonably in contemplation); or

(f) That the disclosure of the information is necessary to prevent or lessen a serious and imminent threat to--

(i) Public health or public safety;

(ii) The life or health of the individual concerned or another individual; or

(g) That the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern; or

(h) That the information--

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(i) That the disclosure of the information is in accordance with an authority granted under section 54 of this Act.

PRINCIPLE 12

Unique identifiers

(1) An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out any one or more of its functions efficiently.

(2) An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of section 8 of the Income Tax Act 1976.

(3) An agency that assigns unique identifiers to individuals shall take all reasonable steps to ensure that unique identifiers are assigned only to individuals whose identity is clearly established.

(4) An agency shall not require an individual to disclose any unique identifier assigned to that individual unless the disclosure is for one of the purposes in connection with which that unique identifier was assigned or for a purpose that is directly related to one of those purposes.

Appendix 2- Terms of Reference

TERMS OF REFERENCE

PRIVACY IMPACT ASSESSMENT – ALL OF GOVERNMENT INITIAL IMPLEMENTATION AUTHENTICATION PROGRAMME

IDENTITY VERIFICATION SERVICE AND FUNCTIONAL INTEGRATION WITH THE GOVERNMENT LOGON SERVICE

Background

The State Services Commissioner (Commissioner) is undertaking the Initial Implementation phase of the All-of-government Authentication Programme (the Programme). The expected outcome of the Programme will be a solution that will enable people to transact on-line and off-line with New Zealand government agencies.

The solution includes two components, the Government Logon Service for which a Privacy Impact Assessment (PIA) has recently been completed and the Identity Verification Service. The purpose of the Identity Verification Service is to authenticate the identity of people wanting to transact on-line with government. Specifically it provides the evidence of identity and identity credential management function for the All-of-government authentication service.

The Government will consider a business case for funding in the 2006/2007-budget year to implement the Identity Verification Service design as a business function within Identity Services, Department of Internal Affairs. The conclusions of the PIA will be incorporated into this business case.

Privacy Impact Assessments (PIA) have been completed in earlier stages of the Programme. As the design for the Government Logon Service and Identity Verification Service functions and their integration as a full authentication service have evolved from that originally reviewed, the Commissioner considered it appropriate that a review be

undertaken of the Identity Verification Service and its integration with the Government Logon Service.

The Programme, under the ambit of the Passport Authentication Design Synergies project, is also undertaking a Legislative Impact Assessment.

Assignment

The purpose of the PIA is to identify privacy impacts arising from:

- The Identity Verification Service design including expected information flows and uses as a standalone service.
- The integration of the Identity Verification Service with the Government Logon Service in the context of an integrated All-of-government authentication solution.

The PIA will not cover any implementation details of the Government Logon Service except in so far as they clarify information flows or the uses of information associated with the Identity Verification Service or overall combination of the two services.

The PIA will provide advice on potential mitigation options available to address such privacy impacts identified in order that the policy objectives of the Programme are met. Decisions on the implementation of such options remain the prerogative of the Programme and of the Department of Internal Affairs in relation to the Identity Verification Service.

The PIA is to be delivered to the Authentication Programme Manager and is to be prepared generally in conformity with Privacy Commissioner's *Privacy Impact Assessment Handbook*. Particular attention will be given to IPP12: Unique Identifiers. The PIA will also incorporate reference to the Cabinet approved Principles for Authentication (http://www.e-government.govt.nz/authentication/Cabinet-paper.asp) in so far as they impact on the matters related to privacy. Similarly, the PIA should reference the Legislative Impact Assessment work being undertaken by the Programme.

When complete, the PIA is to be a public document available for use by policy makers, the Privacy Commissioner and other interested parties.

Approach

The work will commence no later than 12 July 2005 and will involve an iterative process including:

- Reviewing the Authentication Programme's Integrated Conceptual Design Documentation
- Reviewing the Identity Verification Service's High Level Design Specification.

- Convening and attending “white board” Q & A session(s) with key EGU and Department of Internal Affairs (DIA) project staff
- Meeting with EGU and DIA project staff and as required with the DIA Project Sponsor and Business Owners to discuss conclusions in draft PIA
- Meeting with the Office of the Privacy Commissioner (OPC)
- Completing the final PIA Report

Timeframes

The PIA reviewer will:

- Complete a first draft for review by Programme staff by 1 August 2005
- Finalise the draft PIA for submission to the Programme Manager by 15 August 2005
- Finalise the draft PIA for submission to OPC (to be sent by the Authentication Programme Manager once it has been finally reviewed by EGU and Identity Services and they are satisfied with the PIA) by 22 August 2005
- Meet with OPC to discuss and receive feedback and revise the draft, if necessary, to incorporate OPC feedback by 29 August 2005
- Submit the final version of the PIA to the Programme Manager by 2 September 2005.