State Services Commission
ICT Branch

Privacy Impact Assessment of the Proposed Government Logon 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. Since the publication of those documents, the all-of-government authentication programme has considerably advanced its thinking, and has signalled a change in direction for the phased implementation of the project. These changes appear privacy positive, and have no doubt been affected by the analysis presented in the earlier privacy impact assessments. As such the process of privacy impact assessment appears to be both hardwired into the e-government policy development and analysis systems, and to be working as intended by advocates of privacy impact assessment.

1.4. Of considerable significance is the split between establishment (proving who you are once) and confirmation of identity (confirming who you are on an on-going basis through the Government Logon Service).

1.5. Much of the earlier analysis of privacy impact focused on issues around identity establishment, and the privacy problems of a central database, effectively a population register, to establish and assert identity. One of the themes of the earlier assessment was the establishment of an Authentication Agency, which may have functioned as a central repository of information about individuals' identities, and their electronic representations.

1.6. This privacy impact assessment expressly excludes discussion of an Authentication Agency, or of issues of establishment, proof, or evidence of identity. The terms of reference for this report are attached as appendix "A".

1.7. The Government Logon System does not depend on establishment or proof of identity, nor is it a centralised agency accumulating data about individuals' transactions with government. Rather, the system requires Service Agencies to continue establishment of identity of their service users to the extent they consider appropriate for their assessment of the identity related risks posed by use of authenticated online services offered by that Service Agency.

1.8. There may be privacy issues which are contingent on the ways chosen by Service Agencies to verify identity, but the challenge for this process of privacy impact assessment is to accurately delineate between the core Government Logon

Service proposal and the framework and business processes adopted by service agencies to allow online access to their systems.

Critical assumptions

1.9. 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.

1.10. There are a number of challenges to an assessor to ensure that the assessment remains current in the face of evolving processes of policy development, or of technologies. There are important choices too, in the degree to which one should engage in speculation, and which contingent events warrant inclusion in a PIA without ranging too far from the project's stated intentions or design.

1.11. 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 affect 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. The critical assumptions are;

- Ongoing adherence to the cabinet principles specified in paragraph 3.10.
- Identity establishment is not a part of this project – verified identity. information is not required by the GLS.
- Limitation of all aspects of the system (provision of all services) to government sector.
- Limited centralised collection of personal information.
- No use of biometric data.
- The functions of key provider and common login service are both provided by the same agency, the Government Logon Service.
- Operational policy documents and interagency instruments such as memoranda of understanding and standards are 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 Government Logon Service.

2. Methodology

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

- An initial briefing from the project team.
- "All of Government Authentication Project" Power Point presentation given to the Office of the Privacy Commissioner by the project team.
- 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
- Meetings with the Office of the Privacy Commissioner.
- IPP12 and the Shared Keys Implementation Report 27 September 2004
- Research of Issues for Māori relating to the Online Authentication Project, for State Services Commission 29 March 2004 Paua Interface Limited
- Authentication Programme Shared Logon Initial Implementation High Level Design (Jan 05)
- Shared Logon Infrastructure Request for Proposal
- Shared Logon Initial Implementation Application Architecture. SSC & Datacom April 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

Terms and Acronyms

2.2. There has not been consistent use of central terms over the life of the project, or even in that part of the project to which this report relates. The Government Logon System, is variously referred to as the Common Logon System, Shared Login System, the Common Login Site and other variants; Keys and key providers are referred to in some papers as authentication credentials and credential providers. Another workstream within SSC is underway to standardise terms, and develop a common glossary.

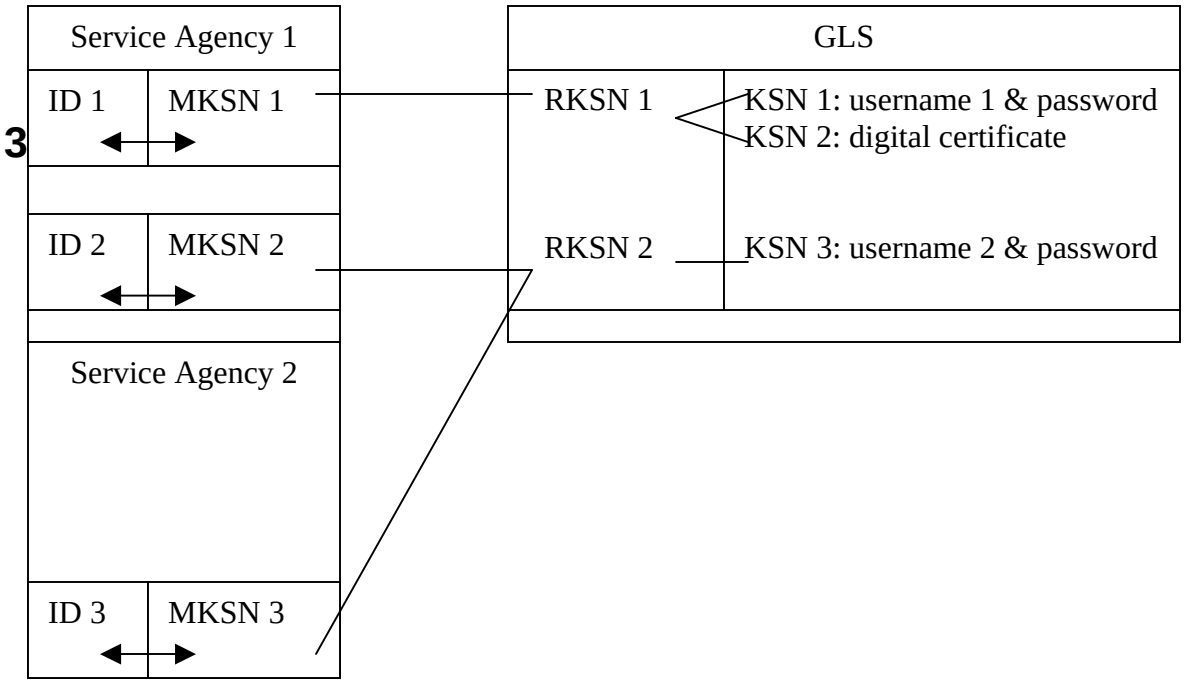
2.3. For the purposes of this report, the following terms and acronyms are used

Term	Description
GLS	Government Logon System, a shared all-of-government service for logon management. Comprised of the CLS and KP.
CLS	The Common Logon Site, a website that

	provides the Internet facing front end of the GLS to service users
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.
KP	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 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.
Service Agency	A government department or agency which provides an online service or services, and uses the GLS 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.
Session ID	A different unique number generated by the Service Agency, so that the returned authentication assertion from the GLS to the Service Agency is matched to the original user access attempt to the service.
Root Key Serial Number (RKSN)	The unique, random number associated with one or more KSNs that a Service User chooses to group together.

A Service User can choose to have one or more keys of the same or different strengths and group them together in one or more RKSNs. Each RKSN generates a unique MKSN specific to a Service Agency. The Service Agency links the MKSN with its user unique identifier created by an appropriate establishment of identity process.

As an illustration of this conceptually, consider a user choosing to use the system in the following way:


Service Agency 1
GLS
ID 1
MKSN 1
RKSN 1
KSN 1: username 1 & password
KSN 2: digital certificate
3
ID 2
MKSN 2
RKSN 2
KSN 3: username 2 & password
Service Agency 2
ID 3
MKSN 3

Description of the Project and Information Flows

3.1. The project and information flows can be described in a number of different ways. The most useful initial means is as a series of linear, chronological steps in an online transaction to conduct business with the Government.

3.2. The simplest description is that a service user goes to a government website, say the Ministry of Social Development (the Service Agency) to conduct some business, such as filing a required document, applying for a benefit or the like. The Service Agency will have business rules governing how an individual must confirm their identity before being allowed to use online services. This might involve some offline process, such as presenting evidence of identity at an office of the agency, or answering a series of questions on the telephone, or an online process, carried out in the initial session. Once the Service agency is satisfied that the person is who they say they are, i.e. identity has been established to an appropriate confidence level, the Service User will obtain a key from the key provider. The key will have a serial number. The GLS will assign a unique random number for the key that is specific to that Service Agency that will be transmitted to the Service Agency when the key is presented. The number will be the same each time the key is presented. When the Service Agency receives that number from the GLS, they will link it to the identity originally established and permit the Service user to conduct their transaction, according to the Service Agency's own business rules that apply for a key of the strength that has been presented.

3.3. Some important features of the process are as follows:

3.4. **Identity establishment is not a feature**

3.4.1. The Government Logon System is not involved in identity management, establishment or registration. It is for the Service Agencies to establish the level of verification of identity that will be required for certain transactions, and to implement sufficient procedures to ensure against identify theft and fraud in ways which minimize the impact on privacy.

3.4.2. While it may seem somewhat artificial to decouple establishment/ management of identity from the issuing and use of keys, to do so best suits the objectives of the project. The GLS can in no way be seen as a "Trojan horse" for a more comprehensive and privacy intrusive process of managing online access to government services.

3.4.3. It is self evident that there will be a demand from service agencies for an efficient centralised system of establishment of identity, and separate work is ongoing on the establishment of some form of "authentication agency". The natural home of such an agency is within the Department of Internal Affairs, but final policy decisions are yet to be confirmed on these matters.

3.4.4. It is clear from a consideration of the GLS project, and of the earlier work by Pacific Privacy Partners that it is in relation to establishment of identity issues that the majority of the most serious privacy issues arise. The project intends to commission and undertake further work on the privacy impacts of the establishment of identity component of online authentication for government workstream in the coming months.

3.4.5. One of the key features of GLS is that service users can use as many different keys as they choose to, including multiple keys with the same Service Agency. For example, the GLS will not know that the same service user has multiple different "identities" for the purpose of the GLS. The GLS will also not know whether a user with multiple separate keys are separate users or just one unless the Service User chooses to group them together for convenience. This gives a significant level of privacy protection. Whether that level of protection will be undermined by the establishment of identity options remains for consideration as part of the privacy impact assessment of that project. The GLS component is clearly sufficiently flexible to give effect to users choices as to the level of privacy protection they wish to achieve.

3.5. **Key Strength and role assignment is managed by the Service agency**

3.5.1. The GLS is a "passive" conduit for passing information about the validity of a key to the service agency.

3.5.2. Different service agencies will have different rules about the strength of key required to access different services. Further, each Service Agency will also have its own rules as to what a person is authorised to do, the role that the person is playing, the service entitlements, and the ways in which users can access services. For example, some service agencies may allow access to certain services with a low identity risk to a person with a weak key. An example might be the use of a username and simple password to file certain documents with the Companies Office.

3.5.3. These issues do not affect the way in which the GLS confirms identity for the Service Agency.

3.6. The second way to describe the project and information flows is to assume each actor is a separate agency, and to set out the information needs of each. Some items are personal information and some are not. For the purposes of this analysis, the functions associated with key provision, and with the common logon service are described separately, even though institutionally, the functions will be carried out in the same organisation, the GLS. These functions may be split in the future, or further key providers added, either of which will trigger further privacy impact analysis.

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

			Government Login Service	
	Service User	Service Agency	Common Login Service	Key Provider
Identity	*X*	*X*		
Key Serial Number			*X*	*X*
Root Key Serial Number			*X*	
Modified Key Serial Number		*X*	*X*	
Key	*X*			*X*

3.8. This table shows that no actor other than the Service User can link the key with identity and clearly demonstrates the separation of roles.

3.9. It is not however, a comprehensive list of personal information held, and for the purposes of the privacy analysis, an attempt at such a list is set out below. For the purposes of this list, the different functions of the CLS and KP are described separately, even though it is intended (at least initially) that those functions will be carried out by the same agency, the GLS.

3.9.1. Service Agency

- All the Service User's personal information generated by, or given to that Agency
- Transaction logs (e.g. date and time of access), together with details of services used on that occasion
- A session ID, a different unique identifier created for each attempt by a Service User to access a resource that requires authentication. This number matches the Service User trying to access a secure online service with the returned authentication assertion (that is, a message about the key validity and strength) from the GLS.
- A second session ID, a different unique identifier created during each session. This number remains constant throughout the session so that the Service Agency can perform its own business processes, e.g. access control, session

timeout, removing the need to re-authenticate with the GLS for online services with the same or lower key strength, etc.

- Modified Key Serial Number, the number from which the Key Serial Number has been converted. It is unique to the Key and to the Service Agency and also communicates the fact that it has been validated.
- Key strength used by the Service User to authenticate at the GLS

3.9.2. GLS (Common Login Service)

- A Session Id that is used to track the Service User's request for authentication in a single session
- Transaction logs recording the date and times a particular key has been presented, outcome (successful, failed, etc.), etc
- Modified Key Serial Number
- Key Serial Number
- Root Key Serial Number which is the key(s) or KSN(s) that the Service User has chosen to group together to generate the same MKSN (in other words, where a service user chooses to use the same key(s) to access several Service Agencies, a new MKSN will be generated for each agency but is linked with the group of keys rather than each single key. The CLS must retain a record of the MKSNs that are derived from a given RKSN and KSN)

3.9.3. GLS (Key Provider)

- Challenge and response information for providing user assistance (i.e. a secret question and its answer provided by the user initially which the user can use to confirm themselves for online self service or offline customer support).
- User contact information (email address) for the Service User to be emailed their reset password. Other forms of contact information may be added in the future, depending on the nature of the keys offered. For example, a physical address may be required to dispatch tokens, or a mobile phone number to send text messages.
- Potentially, other personal information for billing purposes, where necessary, optional credit card details, postal address etc.

3.10. 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.

3.11. 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 policy principles set out in paragraphs 3.10 and 3.11 provide an answer to many of the potential issues around the proposal, particularly the opt-in nature of the proposed Government Logon Service. The information privacy principles are set out in full in Appendix 1 of this report.

Collecting and obtaining personal information

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

4.3. There is nothing in any of the project documentation that gives rise to any concerns over this principle. The project team appear to have been assiduous in ensuring that only the minimum of personal information is retained in the central agencies. This is reflected in the table above, showing that any one actor only has two of the data features that are central to the functioning of the GLS.

4.4. However, the GLS is an Initial Implementation Phase, with many further decisions to be made by Service Agencies, and Key Providers as technologies become available and usage of the service increases.

4.5. For example, nothing in the current design or policy settings appears to rule out the use of some biometric as a key. If a Service Agency required voice recognition, or thumbprint scanning as one factor in a key, and the GLS key provider arm agreed to offer such keys, the project would appear to have nothing to say about that. A range of similar incremental changes to the design could be made without the need for any external, or even cabinet consideration under the current arrangements.

4.6. However such initiatives might well have significant privacy implications, notwithstanding the consensual nature of the transaction. It is not possible to speculate as to all the possible collections of personal information that might theoretically become possible as the technologies improve, nor, in my view would it be desirable to lock the system into 2005 technology by prescriptive regulation, which might legislatively prohibit the use of biometrics in any part of the system.

4.7. A consideration that does not appear to have had much airing in the privacy related discussion of authentication systems to date is that the growth of privacy consciousness, and increase in privacy regulation, are both related to a desire in the community to preserve individual autonomy.

4.8. It is a legitimate approach to privacy impact assessment to note that restrictions for privacy reasons should not be imposed so as to reduce the utility of the system under review for those able to make an informed trade off between privacy risks and benefits. To do so may be to reduce and restrict, rather than to enhance, personal autonomy.

4.9. Rather than to prospectively prohibit new applications and functions then, the rules which govern the introduction of new technology should provide for ongoing assessment of privacy risks, prior to adoption.

Recommendation 1

Any new requirements or opportunities to collect further personal information, such as in the form of biometrics, as part of the system, whether by Service Agencies, the CLS, or Key Providers, should be subjected to further privacy impact assessment before being approved for use as part of the system.

4.10. Perhaps tenuously related to IPP 1, but an important point nonetheless, is the potential scope of the GLS. Once combined with an establishment of identity system, the system might well prove attractive to agencies outside the core public service.

4.11. Already the project team discusses use by local government. There may well be pressures from utilities providers, banks and insurance companies to also use the GLS as the means of granting access to their online services or to interoperate with it, such as by using keys acceptable to both systems. Indeed, the pressure might also come from Service Users, anxious to minimise the number of keys necessary to conduct the range of online transactions currently managed separately.

4.12. While some of the security issues associated with expanding the service might well be capable of being resolved by consumer education, throwing the system open to all would significantly alter the character of the personal information retained by the GLS.

4.13. A typical user interacting in their personal capacity with central government agencies might have a fairly limited number of transactions per annum. The transaction logs retained by the GLS would therefore not reveal a great deal about whoever the person behind the KSN, as the log might indicate that in a two year period, they accessed IRD, the LTSA, WINZ and their local authority. From such a log one might only surmise that they paid their taxes, renewed their vehicle registration, received some income assistance and paid their rates. Any or all of those assumptions might be incorrect.

4.14. However, if a user used the same keys in all their online transactions, and the system were expand to provide a means of accessing online services from a range of other consumer organisations, the transaction log at the GLS would

reveal a great deal more about the person than is currently recorded in any central register.

4.15. 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.[1]

4.16. The project has clear parameters prescribed by Cabinet. Those parameters, included in this paper as a "critical assumption" include that the GLS is to be for government agencies. Clearly there is no intention to expand that scope at this stage. However, in the absence of some extrinsic limitation, there is a risk that the current, or some future administration, could expand the scope of the scheme, in a manner that would have considerable privacy implications, without any transparent process. The potential responses to this concern range from the relatively light, such as recommending that prior to any extension of the scheme the SSC undertake a full process of privacy impact assessment, to the more heavy handed, such as requiring that the scope of the scheme be spelled out in legislation.

4.17. Mid way in that range, is the possibility that some form of delegated legislation, such as a code of practice, issued by the Privacy Commissioner under the Privacy Act, or a regulation, could specify, either by name or by class, the agencies entitled to use the GLS. There could be legal impediments to both of these approaches, in that the Privacy Act might not provide authority for such a limited code (i.e. one that on its face, does not have the primary purpose of modifying one or more principles – although that could arguably be the affect), and there is no readily apparent vehicle for regulation. Amendments to the Privacy Act proposed for introduction soon might provide an opportunity to remove any doubt about the potential scope of a code, if further analysis shows that there are indeed limits to the Privacy Commissioner's jurisdiction in that regard.

4.18. 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.

[1] Who Goes There p12

Recommendation 2
Further consideration should be given to some extrinsic means of limiting the scheme to government agencies, and explicitly excluding others. Options include;

- Further cabinet decisions on limits to the scope of the GLS
- A code of practice
- Regulations
- An Act of Parliament

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

4.20. In one sense, the GLS may not know whether it has collected personal information about a person or not, let alone whether the information it has collected has come directly from the person to whom that information relates.

4.21. **Information privacy principle 3** requires transparency between the collector of personal information, and the subject as to why the information is being collected, who will hold it and who will have access to it.

4.22. There are some risks to transparency in the GLS proposal. Depending on the identity confirmation procedures and key strength required by a Service Agency, there is potential for the service user to misunderstand the pathways his or her information will follow, as the movement from Service Agency, to GLS and back can be seamless.

Recommendation 3
4.23. The GLS should develop a range of materials suitable for different readerships, and media, for explaining the matters contemplated by IPP 3, and other privacy issues, such as security, and implications of choices such multiple keys. Core information about the scheme and the personal information flows should be available to the Service User;

- Prior to the issue of a key
- Any time when changes, or improvements are made to the service, or to the privacy policy (this may be by email to all users, by pop ups, or some other means that strikes a reasonable balance between annoying and informing Service Users)

In relation to the initial provision of information, at the issue of a key, the system should be designed in a way that requires the active acknowledgement of the Service User that they have received the information, rather than merely been given an opportunity to follow a link.

4.24. **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

4.25. **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.

4.26. Security issues are at the centre of privacy concerns about the authentication project. If the GLS has security vulnerabilities, whether from within, or because of a key compromised by a Service User the security of the Service User's information in all Service Agencies could be compromised. The individual may be the victim of identity theft or fraud, or malicious actions intended to smear their reputation. Although the potential damage should be limited, as the key strength (1 factor, 2 factor or 3 factor) is proportional to the identity risk assessed by the service agency, there is nonetheless considerable scope for inconvenience and disruption. In considering security risks associated with the GLS, it is important to keep in mind that there are a series of inherent weaknesses in the internet as a channel of communication. A privacy impact assessment most often is concerned with identifying the incremental effect on privacy of a new proposal, rather than the systemic or inherent flaws. In other words, that the internet may not be a secure environment, is not a reason for not proceeding with the GLS. Government and other services will continue to be offered over the internet, whether or not the GLS intercedes. The GLS is not able to solve all the deficiencies of the channel, and this assessment must take many of those deficiencies as read.

4.27. The storage and exchange of data between the CLS, the Service Agency, and the Key Provider takes place in a secure environment, according to standards designed to prevent intrusions, and to rapidly detect them if they do take place. These standards and measures have not been subject to detailed review as part of this process of privacy impact assessment, but the project specifications are said to have been developed in accordance with Government Communications and Security Bureau guidelines and policies.

4.28. Whether there are weaknesses in the security of the means of transmission between those agencies is a highly technical question that is beyond the scope of this exercise in privacy impact assessment. However, the weakest points are obvious even to a those not technically minded, that is, they lie with the Service User.

4.29. As currently designed, the GLS has no control over the interface between the Service User and the Service Agency. That interaction takes place over ordinary telephone lines, with any freely available web browser. The GLS has

little knowledge as to whether the service is accessed from an internet café that has key logging software installed on it, or through some kind of proxy "man in the middle" such as the recently controversial "Market Score", or is traced and monitored with some other form of spyware. The GLS may get indirect evidence of such compromise, e.g. abnormal traffic flow from a single IP address, and take remedial action.

4.30. It would be possible to reduce the risks associated with Service Users vulnerability to such risks by means such as dedicated access lines, thin/thick/fat clients and the like, or information kiosks providing the only means of accessing the system. These would vest a greater degree of control over the whole system than the existing proposal.

4.31. None of these options is part of the system design for the GLS. The trade-offs for greater security would be against flexibility, accessibility, and cost.

4.32. In an opt in, voluntary system, users must accept a degree of responsibility for the safe and secure use of their access. Consumers accept responsibility for ensuring the safe operation of online credit card transactions, and it is difficult to see why they would not be expected to exercise a similar degree of responsibility over access to online government services. It should be emphasised that responsibility is not intended in this paragraph to be synonymous with liability. This report is not about the legal liabilities for online transactions with government. While there will be limits on the degree of control the GLS is able to exercise over users' behaviour, it cannot simply avoid taking responsibility for the entire security environment by purporting to contractually shift legal liability to the user as a condition of access.

4.33. The GLS has an important role in promoting user education, and providing the tools for users to safely carry one their online business. There are a number of challenges in communicating with users effectively, without defeating the purpose by imposing impediments to using the system, or annoying informed users. It will be important to test a range of options with some users representing different levels of familiarity and competence with the online world to arrive at the appropriate balance.

Recommendation 4

4.34. The system should require Service Users to familiarise themselves with "security tips", which will be readily available at the user education section of the CLS (and expressed in plain language). This should include links to spyware removal software. Where the GLS becomes aware of a specific threat to the system it should ensure that users are informed immediately of the threat, and how to mitigate any risks associated with the threat.

4.35. Another potential security weakness in the system is the relatively low strength check for resetting passwords associated with a username. On the first

occasion when a username & password is issued, the Service User will be asked to provide some information and a question intended to reveal that information through one or more pairs of questions & answers. For example, the Service User might authorise the Key Provider via the CLS to give access to resetting the password based on anyone answering "The Velvet Underground" to the question "What is your favourite band?" for a low strength username & password. For higher strength username & passwords, the Service User will need to answer correctly several randomly selected questions from the bank of questions initially set up.

4.36. Such a system is vulnerable particularly to exploitation by a person who knows the Service User well. For example, an estranged spouse, partner or sibling could conceivably take over a Service User's username & password relatively easily, and wreak havoc.

4.37. The one further check in the system is that the new password is emailed to the Service User's last known email address. While this does provide a greater level of security than relying on the shared secret alone, it is a relatively low-tech means of protecting a password.

4.38. Ultimately this will be an issue for Service Users, who will need to take care to choose a sufficiently secure secret, and take steps to protect their username and password, the secret, and keep their email secure as well as to act quickly if any of these are compromised. The GLS have recognised the weakness of username and password, and has advised Service Agencies that this form of authentication should be considered as a low strength key appropriate for online services that have a low level of identity risk. Where higher key strengths are used, e.g. digital certificate, then appropriate procedures to reissue or revalidate the key needs to be introduced so that no weak link is created.

4.39. Authentication Standards being developed by the State Services Commission for Service Agencies suggest that Service Agencies categorise their online services under one of four categories related to the identity risk of the service:

0	No, or negligible identity risk
1	Low level identity risk
2	Moderate level identity risk
3	High level identity risk

4.40. Functions which have no identity related risk (such as access to forms) should not require authentication and therefore not use the GLS. Services that have negligible identity related risk (such as allowing pseudonymous users to save incomplete sessions) should have a non-verified identifier, such as email address, or a low strength username and password verified via the GLS. Functions requiring a very high level of identity authentication, such as non repudiable electronic signatures required for forensic purposes that also verify

the integrity of the data exchanged and the exchange itself, requires a correspondingly very high level of key strength that is only expected to be introduced sometime in the future. It should be noted that standards that proscribe the use of an authentication system for low level transactions are privacy positive, and allay the fear that authentication systems can become an "internet toll booth"[2] This is related to one of the problems identified in the Pacific Privacy Partners privacy impact assessment, that there may be a potential for the service agencies to allow the required level of authentication to drift upwards, so that ultimately all transactions require the highest level of authentication. This is unlikely to occur in relation to the GLS, provided that Service Agencies adhere to the Evidence of Identity standards being developed by the Department of Internal Affairs. The GLS should ensure that the standard is referred to in the relationship instruments between the GLS and the Service Agencies, and that the Service Agencies are actively monitored and audited against the standard (whether or not that monitoring and auditing is carried out by the GLS).

4.41. The draft standard provides that services with no, or negligible identity risk, such as transactions that can be conducted anonymously, or pseudonymously should be categorised as Category 0, with consequently low security and authentication requirements. Security/authentication requirements for category 1 are likely to be fairly weak, such as a simple user name and password. Category 2 is likely to require two factor authentication, such as user name and password, and a token, digital certificate, SMS text message and the like. Category 3 is likely to require a strong two factor authentication, such as username and password plus a hardware token, or possibly three factor authentication which could include biometrics.

Recommendation 5

The project team should carefully evaluate the business procedures that will be used for reissue or revalidation of category 2 identity authentication once the specific technology is identified and planned for implementation so that no weak link is introduced.

4.42. As an adjunct to the technological mechanisms, the GLS needs protocols as to how to deal with identity theft or compromise. Service Users will be able to suspend or revoke keys themselves online from the self service section of the CLS or request assistance offline from the help desk. Given the weaknesses in the system (albeit largely at the Service User end), any policy for dealing with alleged misuse or compromise should require suspension of the key validity by GLS, and of all online access by the Service Agency. Investigations of allegations of misuse of keys should be conducted by the GLS in conjunction with the Service Agency promptly and with no cost or inconvenience to the Service User. Business rules should treat the key as having been compromised, and transactions conducted during the compromise period as unreliable until the

[2] http://www.epic.org/privacy/authentication/projectliberty.html

contrary has been proven by the GLS/Service Agency. Both the GLS and services agencies will need to develop rules and policies governing their responses to such allegations in the same way as banks have had to develop policies as to which risks it is reasonable to expect the customer to accept (such as the risk arising from writing a PIN number on an eftpos card, or posting one's username and password for online banking on the internet), and which risks the Bank must accept (such as user names and passwords compromised by phishing scams and the like).

Recommendation 6

The GLS needs to develop robust and responsive complaint procedures. These should include the appointment of a privacy officer, and the inclusion in the memoranda of understanding with Service Agencies, means to ensure that Service Agencies are required to cooperate with any investigation of an allegation of corruption or misuse of keys or data (and visa versa).

4.43. **Information privacy principle 6** provides that individuals are entitled to have access to information about themselves.

4.44. Section 45 of the Privacy Act provides:

> Where an information privacy request is made pursuant to subclause (1)(b) of principle 6, the agency—
>
> (a) Shall not give access to that information unless it is satisfied concerning the identity of the individual making the request; and

4.45. This requirement potentially provides an interesting challenge to the GLS. GLS does not record a Service User's identity or in fact know if the Service User is an individual a business, or some other entity. It may be that "presentation of a valid key" would need to be considered as synonymous with identity in the context of section 45.

4.46. Service Users will be able to access logs of their activities through the self service section of the CLS. These transactions could be considered to be IPP 6 transactions, however, there will be cases where, for a range of reasons, an individual might want to obtain from the GLS, more detailed records of their usage than is available via the system. A user might seek access to audit records, records of access attempts that were denied, details of the MKSNs associated with any keys, or any other information held by the CLS or Key Provider.

4.47. The GLS will need to have procedures for dealing with such requests, including how identity of the person seeking the information is to be established. Service Users' ability to exercise their rights under IPP 6 will to a large extent be dictated by the information they are able to give the CLS to enable the CLS to retrieve associated data. For example, a request stating "*please give me all information you have about me, John Edwards*", is unlikely to elicit any data

unless supported by the user names such as “edJ4”, JoEDWs, challenge question and answers and possession of the key in the case of two factor authentication, and so on.

Recommendation 7
The GLS should develop procedures and processes for dealing with requests under IPP 6. The procedures will need to provide for the confirmation of identity, without the compromise of security.

4.48. **Information privacy principle 7** gives individuals a right to correct information that is incorrect out of date or misleading. It is difficult to conceive of any issues arising out of the project with implications for this principle.

4.49. **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.

4.50. As described in the project documentation, the system depends on information provided by the Service User. This principle would appear to have limited lessons for the project.

4.51. **Information privacy principle 9** however does highlight some potential issues. The principle requires that personal information should not be retained for longer than is necessary for a lawful purpose.

4.52. This leads to two questions not directly addressed in the project documentation to date. The first is how long the transaction logs will be retained. The second is how the CLS should treat apparently “inactive accounts”, that is, keys which have not been used for a specified period of time.

4.53. The first question needs to be considered with reference to the applicable laws, business rules, and requirements of service agencies and auditing requirements of the GLS. Privacy interests would emphasise minimum retention, to avoid building up a centralised picture of an individual’s interactions with government. Audit and forensic needs will require some period of retention, but the period should be assessed with reference to the fact that the principle records will be retained by the Service Agency. The Service Agency will have a record of the date and time of a GLS facilitated transaction, and a detailed account of what was transacted.

4.54. GLS would need a very good case to justify retention of transaction logs for any period greater than say, 12 months. Once the GLS has determined its legitimate needs for audit and other purposes, it will be necessary to assess any proposed policy against other statutory requirements (such as the Public Records Act 2005), and consult with other interested parties such as Service Agencies, and control agencies such as the Chief Archivist.

4.55. In relation to the length of time an account is left "open", privacy interests would favour the opposite conclusion. If an individual creates an online presence, they may wish to retain it indefinitely regardless of sporadic and infrequent usage. On the other hand, the inactive accounts are a known security risk to authentication systems.

4.56. Ultimately, the rules on retention need only be clearly established and communicated to Service Users, who will be able to make their own choices and tradeoffs as to whether they accept the service on those terms.

4.57. If "accounts" are to expire after a given period, Service Users should be advised of that fact in advance, and then given emailed warnings prior to the suspension of the service. This will enable them to undertake appropriate steps to keep their key live.

4.58. A further issue which requires consideration is how to give effect to a Service User's desire to cancel keys, and either revert to offline dealings with government agencies, or change keys. Subject to the presumably temporary need to retain the KSN for audit purposes, those numbers should be deleted from systems on the Service User's request.

Recommendation 8

The GLS needs to develop policies for the retention of information, for closing "inactive" accounts and for enabling users to leave the system, and disable keys.

4.59. **Information privacy principle 10** restricts permitted uses of personal information. In the context of the authentication project, it makes sense to link the discussion with information privacy principle 12, which deals with unique identifiers.

4.60. 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[3].

4.61. There is nothing in the project documentation to suggest that the designers anticipate using any of the information generated in the course of an online transaction with the GLS interposed between Service user and Service Agency, for any purpose outside that transaction.

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

4.62. The expected ancillary uses of the information such as auditing and the like would fall within the "directly related purposes" exception to the principle, and as such are not of concern, and do not require separate comment.

4.63. The greatest potential privacy risk relates to the capacity for the system to facilitate the bringing together of what are now disparate items of information to a central place.

4.64. The ability to do so with an authentication system depends first on the use of a common key with many different agencies (an option which is available to GLS users, but not mandatory), enforcing a rule of one person-one identifier (which is ruled out by allowing Service Users to have multiple RKSNs) and the existence of some form of common identifier across Service Agencies (which is rule out by having different MKSNs for Service Agencies even though the RKSN or KSN may be the same).

4.65. The GLS has been designed with the express purpose of limiting the ability of any present or future agency using any component to bring together records from multiple agencies, regardless of whether Service Users elect to use one or many keys for accessing online services. This provides Service Users the convenience of being able to use a single key across government while preventing Service Agencies obtaining a way of matching records or data from that use.

4.66. Each RKSN will be assigned a randomly generated but unique number to be used as the basis for generating a MKSN or modified key serial number. No two Service Agencies will have the same MKSN even though the RKSN is the same. A future government could not associate records held by two or more Service Agencies with reference to the MKSN.

4.67. It would be possible for a future government to instruct Service Agencies to replace the MKSN with the RKSN in their systems, and then to match data on the basis of that number, however the utility of such an exercise would be limited, and short lived, given the Service User's ability to simply cancel the keys. This is further limited by the fact that a person or other entity can have multiple RKSNs even with the same Service Agency with no way of connecting them up.

4.68. **Information privacy principle 11** restricts the agencies to which personal information may be disclosed. Taking a narrow view of the project, disclosure issues are not particularly significant. The only information that is transmitted is the not very personal series of characters required to access a website, including user name and password, session ID, MKSN, key strength, and the fact that the key is valid.

4.69. The adoption of appropriate procedures should ensure that other disclosures (such as the disclosure of the logs, shared secret or other information associated with the GLS) are not disclosed other than in accordance with the exceptions to the principle.

4.70. **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.

4.71. It is not necessary to tease out and analyse those concerns in any greater detail, as the proposed system (at least the GLS component of the authentication project) both complies with the legal requirements of IPP 12, and achieves the policy objectives underlying the principle.

4.72. 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:

4.73. At an admittedly facile level, it is possible to argue that none of the numbers generated in the GLS are "unique identifiers", because they do not uniquely identify an individual. They identify a key (KSN), a group of keys (RKSN), a RKSN for a Service Agency (MKSN), or a transaction request (session ID). In addition, the system does not assume that the number is the only one by which a Service User will interact with the system, and as such any nominated number fails the first definitional test of "uniqueness".

4.74. The principle protection against using any one number as a means of aggregating otherwise disparate items of information, is the split between the RKSN, and the MKSN.

4.75. Although it is important, to prevent the aggregation to have separate numbers (each Service Agency will have a different MKSN, but each MKSN associated with a common key will be traceable at the GLS to a single RKSN), it is also necessary for security, auditability, and the prevention, detection and prompt rectification of identity theft for the GLS to retain an ability to link the MKSN to the RKSN. If the GLS did not have an ability to derive the RKSN from the MKSN would limit the ability of the GLS and Service Agencies to communicate and resolve issues with each other. The MKSN is the only common data element about a user that both GLS and Service Agencies have to refer to a

specific user. In the absence of a way to refer to a user commonly and persistently, the system would not work in practice. This would limit day to day functions, as well as auditability. If a Service User discovers that their identity has been appropriated by a fraudster by taking over use of a key it is important to enable the GLS to trace all sites where the key may be used, in order to alert the other agencies to the problem.

4.76. The ability to audit to detect misuse is itself a privacy value. Given that, and the fact that first, users decide how many agencies may use any given key, and second that the use of unique MKSNs for each service agency would impede any ability to information match based on the MKSN, the tradeoff represented by the decision to maintain a central record of MKSNs associated with an RKSN does not appear privacy adverse. In addition to the need to respond to key compromises, the service also needs to be able to retain a record of MKSNs associated with an RKSN if the *identity* itself proves to have been compromised, that is, where a service agency has somehow allowed the wrong person to claim an entitlement to be associated with the records of another client. Issues relating to compromised identities will be addressed as part of the evidence of identity privacy impact assessment.

5. Privacy Risk Assessment

5.1. Overall the proposed GLS appears to have been devised to minimise privacy risk, and has done so successfully. What remains to be seen is how the introduction of the establishment of identity component will affect this initial impression. This will be done by a separate, later privacy impact assessment once the high level design of the identity function component is finalised and is out of scope of the present assessment.

5.2. The project design appears to fully reflect the policy settings prescribed by Cabinet, and the voluntary nature of the system is a significant factor in safeguarding privacy. This has been clearly reflected in the design, for example, and most significantly, in allowing Service Users to exercise their autonomy according to their privacy risk aversion, and perceptions of convenience and utility, by enabling multiple, or single keys.

5.3. Transaction logs have a potential to constitute a new central store of information about an individual's interactions with government, and this factor, combined with the potential for pressure to expand the availability of the system call for some constraints to be applied, both in deciding on policies for retention periods, and controlling the availability of the GLS to non-governmental agencies.

5.4. Many of the other privacy risks associated with the project are in the hands of the users, and as such the principle role of the GLS (outside its own security systems etc) would appear to be in promoting user education. However to say that matters of security are capable of being controlled by Service Users should not absolve the system designers from recognising the role of inherent human fallibility as the greatest risk to the system. Policies and procedures which acknowledge the frailty of many users in the face of technological challenges should be adopted to ensure the potential effects of errors are minimised. This may require agreements with Service Agencies as to how user frailty is reflected in the identity risk evaluation and authentication technologies consequently adopted. One approach is to recognise that any authentication system is but one component of the online identity management system and for Service Agencies to place adequate emphasis on complimentary efforts on business logic, authorisation, anomaly detection, rules based error checking.

5.5. There remain a number of lower level privacy issues to be resolved as the system is developed, such as the preparation of rules and polices incorporating IPP 3 compliance, retention periods for the transaction logs and other issues raised under the headings of the IPPs in the previous section.

6. Privacy Enhancing Responses

Security Responses

6.1. Given the analysis above, the most useful privacy enhancing response would appear to be user education. This should include not just security matters, but also privacy matters. For example, explicit materials about the risks associated with using the same key for many agencies should be prepared.

Institutional responses

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

6.3. However there does not appear to be any pressing need to spell out institution types and governance arrangements in relation to the GLS alone. It may be that if further analysis of delivery mechanisms is required in relation to the establishment of identity work, it will be necessary to consider the options available in relation to the CLS and Key Providers, such as whether they ought to be separate from any "Identity Agency", or what institutional models best fit the different functions allocated to different agencies.

Policy and legislative responses

6.4. That the authentication agencies would be regulated by specific legislation was a theme of the earlier privacy impact assessments. However looking in isolation at the GLS, and applying the Legislation Advisory Committee guidelines, there would not appear to be a compelling case for prescriptive legislation covering the GLS.

6.5. Legislation can provide confidence that functions developed for one set of purposes will not "creep" in to other, more intrusive purposes, and enforces a very public means of effecting changes to policy settings. However, it can also reduce flexibility and responsiveness. In addition there are real risks in legislating to preserve a particular technological status quo in a time of such rapid advancement of technology.

6.6. Subject to the need perhaps to provide a legislative solution for privacy issues that may be identified in relation to the separate establishment of identity initiative, the only issues identified in relation to GLS that may benefit from some regulatory oversight would be the expansion of use into other non-government agencies, and the introduction of biometrics as keys available in the CLS. At the least further privacy impact assessments should be undertaken of

any expansions of the scheme beyond the assumptions discussed in para 1.9 above.

6.7. The first issue could be adequately dealt with by using the existing regulatory framework, for example, by issuing a code of practice under the Privacy Act. Such a code could limit the number of agencies entitled to use the CLS to those approved by the Privacy Commissioner, in the same way as the Health Information Privacy Code 1994 regulates the agencies entitled to use the NHI number.

7. Māori Issues

7.1. The terms of reference for this privacy impact assessment require a consideration of the impacts of the GLS on Māori.

7.2. The E-government unit of the State Services Commission had commissioned work on the overall impacts of the authentication project on Māori, and as a result has published the paper "*Research of issues for Māori relating to the Online Authentication Project*[4] "("the Tikanga paper").

7.3. That report recommended that "*A preliminary Māori Cultural and Social Impact Assessment is completed to understand the high level impact on Māori*". The report noted that such a review should consider:

• Issues that relate to the speed of technology change and the risk of re-colonisation through the imposition of technology-based solutions
• The impact of E-Government on processes that are inherently Māori such that changes are appropriate to Māori and not detrimental to other forms of interaction (e.g. 'kanohi ki te kanohi')
• Project benefits for future generations are identified and can be articulated

7.4. No further report has been commissioned, and as such the analysis that might have informed a consideration of the impact of the GLS on Māori is not available.

7.5. The Tikanga paper quoted from a June 2003 Cabinet paper which set out the means by which specific issues for Māori were to be addressed:

• ensure there is a process for obtaining Māori participation throughout the design, development and deployment of the authentication model

• determine whether governance structures should include a Kaitiaki (guiding overview) group that formalises the interest of Māori stakeholders

• explore the implications of protecting authentication data so that it cannot be used for statistical purposes (for example, to publicise Māori take-up of online authentication)

[4] http://www.e.govt.nz/archive/services/authentication/tikanga-200408/index.html

• assess a view that government agencies should not collect or store whakapapa and, if appropriate, ensure that whakapapa is not included directly in the authentication model

7.6. Apart from the last bullet point, those matters do not relate to privacy, and as such the extent to which the project has or has not acted in accordance with Cabinet's instructions is a matter for consideration elsewhere, not as part of this process of privacy impact assessment and reporting. In relation to the final bullet point, given that the GLS is not concerned with issues of identity, does not require the collection and retention of information on whakapapa the GLS project does appear to meet Cabinet's expectations in relation to sensitivity to Māori issues.

7.7. The Tikanga paper does make reference to a concept of "collective privacy". There has not been a great deal of international discussion of concepts of communal or collective privacy, and in fact the terms may appear to some to be oxymorons.[5] However they have been suggested as safeguarding the common rights and dignity of heterogeneous groups in society, particularly in relation to members of those groups being the objects of study or research, without necessarily being the beneficiary of the study or research. There are a number of conceptual difficulties in differentiating between the rights of an individual member of such a group, and the group as a whole, such as how to respond when the interests of the individual and of the collective are not aligned. It may be that the collective rights are more comfortably described with some alternative conceptual base, rather than privacy, in respect of which the preponderance of writing describes as a value inherent in one's individuality, rather than membership of a collective.

7.8. The extent if any of a right of or conceptual basis for communal or collective privacy are not questions which need to be resolved for the purposes of the GLS, as the GLS does not appear to afford any opportunities to intrude into collective rights however expressed. The GLS does not collect any information about ethnicity, whakapapa or hapu affiliation, and as such cannot be a vehicle for insensitive treatment of such information.

8. Summary of Recommendations

Recommendation 1
Any new requirements or opportunities to collect further personal information, such as in the form of biometrics, as part of the system, whether by Service Agencies, the CLS, or Key Providers, should be subjected to further privacy impact assessment before being approved for use as part of the system.

[5] see for example "Protecting Indigenous Peoples' Privacy
from "Eyes in the Sky" Wayne Madsen http://www.spatial.maine.edu/tempe/madsen.html

Recommendation 2
Further consideration should be given to some extrinsic means of limiting the scheme to government agencies, and explicitly excluding others. Options include;

- Further cabinet decisions on limits to the scope of the GLS
- A code of practice
- Regulations
- An Act of Parliament

Recommendation 3
The GLS should develop a range of materials suitable for different readerships, and media, for explaining the matters contemplated by IPP 3, and other privacy issues, such as security, and implications of choices such multiple keys. Core information about the scheme and the personal information flows should be available to the Service User;

- Prior to the issue of a key
- Any time when changes, or improvements are made to the service, or to the privacy policy (this may be by email to all users, by pop ups, or some other means that strikes a reasonable balance between annoying and informing Service Users)

In relation to the initial provision of information, at the issue of a key, the system should be designed in a way that requires the active acknowledgement of the Service User that they have received the information, rather than merely been given an opportunity to follow a link. For example, they may be required to click to accept before proceeding.

Recommendation 4
The system should require Service Users to familiarise themselves with "security tips", which will be readily available at the user education section of the CLS (and expressed in plain language). This should include links to spyware removal software. Where the GLS becomes aware of a specific threat to the system it should ensure that users are informed immediately of the threat, and how to mitigate any risks associated with the threat.

Recommendation 5
The project team should carefully evaluate the business procedures that will be used for reissue or revalidation of category 2 identity authentication once the specific technology is identified and planned for implementation so that no weak link is introduced.

Recommendation 6
The GLS needs to develop robust and responsive complaint procedures. These should include the appointment of a privacy officer, and the inclusion in the memoranda of understanding with Service Agencies, means to ensure that Service Agencies are required to cooperate with any investigation of an allegation of corruption or misuse of keys or data (and visa versa).

Recommendation 7
The GLS should develop procedures and processes for dealing with requests under IPP 6. The procedures will need to provide for the verification of identity, without the compromise of security.

Recommendation 8
The GLS needs to develop policies for the retention of information, for closing "inactive" accounts and for enabling users to leave the system, and disable keys.

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 1- Terms of Reference

TERMS OF REFERENCE

PRIVACY IMPACT ASSESSMENT – ALL OF GOVERNMENT INITIAL IMPLEMENTATION AUTHENTICATION PROGRAMME

Background

The State Services Commission is undertaking and leading the Initial Implementation phase of the All-of-government Authentication Programme (the Programme). A major project in this Programme is the Government Logon Service (GLS) (the Project).

The expected outcome of the project will be a solution for people (and businesses) and New Zealand government agencies to verify their identity when transacting electronically. GLS specifically deals with the Logon process and the management of a service user's Logon credentials (keys). Cabinet will consider the next steps at the conclusion of the Programme, expected to be December 2005, and will make a decision whether or not to roll-out the All-of-government Logon solution to other agencies.

Privacy Impact Assessments (PIA's) have previously been carried out on an initial design for the overall authentication model, of which GLS is a component. As the design for the GLS has evolved from that originally reviewed, the Commission considered it appropriate that a review be undertaken of the GLS design that is to be implemented.

Assignment

The purpose of the PIA is to identify privacy impacts arising from the Project and to provide advice on potential mitigation options available to address such privacy impacts in order that the policy objectives of the project are met. Decisions on these options remain the prerogative of the project team.

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*. 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 4 March 2005 and will involve an iterative process including:

- Reviewing project documentation (including the two Pacific Privacy Consultant PIA documents and the Paua Interface Ltd Research of issues for Māori relating to the Online Authentication Project report)
- Convening and attending “white board” Q & A session(s) with key project staff
- Meeting with the Office of the Privacy Commissioner (OPC)
- Meeting with the Authentication Project team to discuss conclusions in draft PIA

The Commission is particularly interested in the likely privacy impacts on Maori. It is expected the PIA will look specifically at whether there are any privacy impacts for Maori that need to be considered by the project.

Timeframes

The PIA reviewer will:

- Undertake international and domestic research and prepare a “rough cut” draft for review by the Authentication Project team's technical staff by 22 April 2005
- Finalise the draft PIA for submission to OPC (to be sent by the Authentication Project team once it has reviewed and is satisfied with the PIA) by 6 May 2005
- Meet with OPC to discuss and receive feedback and revise the draft, if necessary, to incorporate OPC feedback by 27 May 2005
- Submit the final version of the PIA to the Authentication Project team by 3 June 2005