ALL-OF-GOVERNMENT ONLINE AUTHENTICATION

Update to the December 2003 Privacy Impact Assessment

April 2004

All-of-Government Online Authentication

Update to the December 2003 Privacy Impact Assessment

by
Pacific Privacy Consulting
in association with
Xamax Consultancy

for
E-government Unit
State Services Commission
New Zealand

April 2004

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

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

All-of-Government Online Authentication

Update to the December 2003 Privacy Impact Assessment

Contents

Executive Summary

This update to the December 2003 Privacy Impact Assessment (PIA) addresses developments in the Online Authentication project since that time, specifically the implications of the recommended Initial Implementation.

Given that the long term objectives of a centralised authentication infrastructure and ID Credential remain unchanged, most of the privacy issues remain valid, as do the recommendations as to how they should be addressed.

Some of the privacy issues will not arise in the Initial Implementation, but these should continue to be addressed in the policy and standards work and in the further investigation of evidence of identity and the role of ID credentials.

The shared key pilot, which will form part of the Initial Implementation, will involve the collection and use of some personal information, and further assessment of the privacy implications is recommended as the detailed design of the pilot is developed.

This update identifies which of the recommendations from the December 2003 PIA need to be addressed in which Components of the Initial Implementation.

Four further recommendations are made, dealing with the locking in of privacy protection; presentation of PI findings; governance arrangements; and continued consideration of alternative approaches to Credentials.

Introduction

1. Reflecting government recognition of privacy as a key issue in relation to any authentication initiative, the E-government Unit (EGU) of the State Services Commission (SSC) engaged Pacific Privacy Consulting in August 2003 to conduct an external Privacy Impact Assessment (PIA) as part of the Online Authentication Project.

2. The PIA, conducted in accordance with the PIA Handbook issued by the Office of the Privacy Commissioner, was completed between September and December 2003. The Report, containing 35 recommendations, was authorised by Cabinet for publication and is available at http://www.e.govt.nz/docs/authent-pia-200312/

3. The Executive Summary of the December 2003 PIA Report included the following:

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

> Other recommendations suggest a clearer articulation of the need for the scheme; and a review of the scheme design in relation to multiple Credentials; confirmation of identity rather than release of names; authentication of roles, and the use of the photograph and biometric."

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

5. Pacific Privacy was engaged again in February 2004 to assess what aspects of the December 2003 PIA apply to the Initial Implementation approach that is now being proposed. Specifically we were asked to:
- Review documentation relating to proposed implementation approach; decisions made and other developments in the project since December 2003.
- Discuss with the Project Team the December 2003 PIA recommendations and document the proposed response including clear exposition of relative positions;
- Meet with the Office of the Privacy Commissioner to discuss PIA recommendations and ascertain their views and priorities; and
- Provide a written view on the implementation approach that has been recommended to Ministers and the implications for PIA recommendations.

6. The consultant met with the Project Team, IQA consultants, other SSC staff and the Office of the Privacy Commissioner on 22-24 March in Wellington. A draft PIA Update report was provided for comment on 30 March 2004, and this final report incorporates revisions following feedback from the Project Team, IQA consultants and the Department of Internal Affairs.

Development of the Project

7. Significant changes have been proposed since the initial PIA was completed in December 2003. A phased approach has now been recommended which *excludes* the development of a 'full build' scheme including a formal shared Credential, at least in the immediate future. Consideration was given to two other options, being accredited standards only, and an Initial Implementation. This latter option is recommended by the EGU for government approval in the near future.

8. The Initial Implementation (II) option consists of five components[1]:

> **1. Accredited Standards**
> This comprises work to prepare all-of-government Online Authentication Standards. It includes tasks related to identifying and developing standards, consulting with agencies, establishing governance and management routines, and a formal accreditation process.

> **2. Evidence of Identity (EOI) and Credential investigation**
> This comprises work mostly, but not entirely, to be undertaken by the Department of Internal Affairs (DIA) to consider all-of-government Evidence of Identity processes. The component includes tasks related to:
> - reviewing the current Passports application process;
> - identifying possible synergies that may arise from combining existing internal EOI processes (eg Births, Deaths and Marriages and the Passports Office) or from leveraging other agencies EOI processes (eg Department of Labour – Immigration Service); and
> - researching and analysing evolving international trends (including the use of biometrics and 'in person proofing').

> Work is also to be undertaken on preparing for potential future development of an all-of-government identity Credential.

> **3. Policy Development**
> This component supports the development of policy to support the standards; associated governance and oversight arrangements; legal processes around the potential for future legislation and legal certainty (non-repudiation and legislative compliance) and legal liability; tikanga issues; and the extent to which authentication needs for business can be met by the same means as authentication for individuals.

> **4. Review Bodies and Privacy Impact Assessment**
> This component will assist in developing transparency and accountability in the authentication process. Support both for and from the Offices of the Privacy Commissioner and the Ombudsmen is to be addressed. This includes providing and receiving input into the developing process and the adoption of an education, monitoring and complaints resolution process.

---

[1] The following description of the five II components has been provided by the Project Team

An update or extension to the existing PIA is to be part of the next stage of this development.

5. Shared Keys

The next phase of this development is to construct and trial a Shared Keys system between 2 – 3 agencies. This will not involve the sharing of or reliance upon Credentials between the agencies involved. It will be an operational system and will require ongoing support.

9. Since December 2003, the Hight Level Technical Design (HLTD) has been further revised.[2] If the 'full-build' had been recommended, this PIA Update would have looked in more detail at this Design. However, the Initial Implementation will almost certainly lead to significant further developments and changes to the technical design of any longer term centralised authentication scheme. In this context it seemed wasteful to review the HLTD in more detail at this stage. Some references have been made to it where appropriate.

Implications for privacy - Overview

10. Since December 2003, as well as the recommendation for a phased approach, the long term intentions and objectives for the scheme have firmed up, removing some of the uncertainty identified in the initial PIA. The Best Practice Framework, which has emerged from the earlier design work but would fit within the Standards Component (C1) of the recommended Option, states:

> "The vision for all-of-government authentication is to provide a single means by which people and government agencies authenticate their electronic identity."[3]

11. While the increased certainty makes the privacy assessment easier, the language used confirms, in the PIA consultants' view, the likelihood of 'scope creep'; ie: an expansion of the scheme's functionality and application beyond that stated at the outset. For example:

> "The long-term vision is to move towards an 'all-of-New Zealand' approach to authentication. Private and public sectors currently use the same EFT-POS system in their transactions, meaning that individuals can use the same bankcard and PIN for all payments. A similar collaborative approach to online authentication would mean that the systems and processes that an individual uses to authenticate themselves to government agencies could be relied on when they transact with a non-government agency if the individual chooses."[4]

12. We note that while this reference to private sector use retains the 'choice' qualifier, there is no such equivalent qualifier in the first 'vision' statement, which

---

[2] High Level Technical Design, v.1.0 18 February 2004
[3] Draft *Best Practice Framework*, v.10, March 2004 p.14
[4] Draft *Best Practice Framework*, v.10 March 2004, p.15

could be read as implying a reduction in the element of choice available to individuals. A qualifier such as 'if they choose' at the end of the vision would have been more consistent with the 'Opt-in' design principle[5], but would of course have implications for the degree of standardisation and consistency which could be achieved.

13. Many of the privacy concerns identified in the initial PIA related to the 'full-build' implementation option that was being considered at the time the PIA was carried out. The subsequent recommendation to proceed only with an initial implementation (II) means that many of the concerns do not in practice arise immediately. Until such time as the II components lead to actual outcomes, such as standards, other guidance for agencies, or proposals for legislation; there are relatively few *direct or immediate* privacy impacts.

14. However, given the confirmation (and hardening) of the long-term objectives, all of the concerns raised in the initial PIA remain relevant.

15. The phased implementation means that there is a further opportunity to consider privacy issues alongside the merits of particular approaches to authentication, including evidence of identity requirements, the role of Identity credentials and the role of biometrics.

16. This consideration will be assisted by the Office of the Privacy Commissioner, which will be specifically resourced to be closely involved.

Statutory safeguards?

17. A major theme of the recommendations in the initial PIA was the desirability of entrenching safeguards in legislation (several recommendations, summarised in Recommendation 35). The revised incremental approach to implementation means that there is less of an imperative for legislation authorising the scheme (in which safeguards could be incorporated), at least in the short term.

18. Even when actual products emerge from the II components, it will be difficult to argue for stand-alone legislation to safeguard against purely speculative function- and scope-creep, in the absence of a legislatively based authentication infrastructure.

19. The absence of overall authorising legislation, at least initially, does not however mean that the need for *entrenched* safeguards is lessened. It does mean that the provision of these safeguards is a more complex and diffused task than if it was possible to attach them to a law establishing an Authentication Agency.

---

[5] The Independent Quality Assessors (Hunter Group) have commented that opt-in should never have been put forward as a principle for authentication, but only at the service level. The PIA consultants agree - Individuals will for many services not be able choose to transact with government online without agreeing to authentication of their identity. The only effective choices will be whether to transact online or offline (provided offline options are offered,) or not to use a particular government service at all (often not a real option). (Offline options may also involve some degree of authentication).

20. The project should now aim to secure the same level of privacy protection, and limit the prospect of undesirable function- and scope-creep, in three ways:

  ➢ By clearly identifying legislative changes which will still be required.
  ➢ By setting thresholds for implementation steps which should trigger further legislation.
  ➢ By locking in protections and safeguards through other devices, including potentially Codes of Practice[6], contracts or other publicly accountable agreements.

21. These options, which can be developed as part of the Policy Component (C2) should be promoted through the Standards Component (C1), and, where applicable, through legislation.

22. There is a consensus that legislation will be desirable in due course in the following areas of privacy concern:

  • Granting all users seeking to transact online with the NZ government the same rights under the Privacy Act (Recommendation 22 of the initial PIA) – this change which was flagged as necessary in connection with an all of government credential is an equally necessary pre-condition for any authentication, including that involved in a shared key pilot. It is understood that the government has already agreed in principle to this change, which was recommended for broader reasons by the Privacy Commissioner in 1998.[7]
  • To authorise information matching and clarify the operation of the unique identifier principle in the Privacy Act (see Recommendations 19 and 26).

23. Legal advice to the project team in relation to the Initial Implementation is not conclusive as to whether legislation will be required for other issues such as liability, evidentiary and 'minors' issues, and to provide appropriate criminal penalties.[8]

24. If legislation is required for other aspects of the scheme, this would give an opportunity for any other statutory provisions considered desirable to be attached, if the timing coincides.

25. The PIA consultants agree with the Project Team that any legislation (and other 'rules') should be 'technology-neutral' wherever possible, but where *on-line* authentication gives rise to specific issues, it may be appropriate to include provisions that are related to particular features of the online environment.[9]

---

[6] A Code of Practice approved by the Privacy Commissioner under the Privacy Act 1993 is one possibility – it effectively becomes the law, superceding the general default Information Privacy Principles in the Act

[7] Privacy Commissioner, 1998, *Necessary and Desirable: Review of the Privacy Act 1993,* Recommendation 61.

[8] Wigley & Company, *Is (or to what extent is) a statutory regime required?* v.1.0 21 February 2004, opinions from SSC Legal Officers, and *Review of Legal Issues* paper v.0.95 17 March 2004

[9] It is difficult to predict if this will be the case, but for example the technology of the Internet and its use has particular characteristics that may require specific controls; eg: the use of cookies, and security issues. The NZ Government currently addresses these issues through its *Minimum Standards for Internet Security*, but what we are suggesting here is that legislative controls *may* be required in some

Deferment of privacy considerations?

26. Some of the recommendations of the initial PIA related to the specific operations of the proposed Authentication Agency and processes associated with the centralised Credential. As these are not now proposed as part of the Initial Implementation, there is a temptation to simply defer consideration of the recommendations until such time as an Authentication agency or centralised Credential are established. While these recommendations can and should be 'parked' pending any decision to go ahead with these elements, the recommendations may also be relevant to any alternatives that emerge from Components 1, 2 and 3 during the Initial Implementation, and should not be overlooked during this phase.

27. Privacy recommendations of the initial PIA in this category are as follows:

Recommendation (December 2003)		Comment
R.5	Justification for requiring alternate names	fundamental to Component 2.
R.7, 13 & 14	Ensuring credentials do not lead to ID cards/UIPs	may arise from Component 2 but should also be considered in Component 3.
R.8	Retention of biometric templates	may arise from Component 2 but should also be considered in Component 3.
R.9	Limiting secondary use of photos/biometrics	may arise from Component 2 but should also be considered in Component 3.
R.10	Role of biometrics in authentication	will be part of Component 2.
R.11	PIA and legislation before any other biometric	may arise out of Component 2 but should also be considered in Component 3
R.12	Limits on scope	may arise out of Component 2 but should also be considered in Component 3.
R.15	Analysis of points of failure	should be considered in Components 2 and 5, with consequences for Components 1, 3 and 4.
R.16	Legal basis for authentication agency	legitimately deferred pending a decision on the central AA role – to be considered in due course in Components 2& 3.
R.18	Public presentation of privacy compliance	The Project Team have suggested that this is covered by the allocation of resources to OPC, but it is important that all participants do not exaggerate the effect of the Privacy Act – this should be recognised in all Components.
R.21	Security review	will arise first in the shared key pilot (C5) but also in due course in Standards (C1) emerging particularly from Component 2.

technology specific areas, and it should not be assumed that legislation can always be 'technology-neutral'.

R.23	Withholding personal information on security grounds	this was directed to the Authentication Agency but is equally applicable to any other data held as part of an authentication process – including the shared key pilot. Should be considered as part of Components 3 and 5.
R.24	Data Retention and Disposal	While this will be within an Archives Act framework, decisions will be required that are specific to the online authentication scheme - should be considered in Components 2, 3 and 5, leading to Standards under Component 1
R.25	Use and disclosure of personal information	The adequacy of the existing Privacy Act regime, and ways of further limiting access to and uses of data should be discussed with the OPC as part of Component 3. Note that the research on issues for Māori has secondary uses as a general concern, with possible specific concerns about statistical uses.[10]
R.27	Outsourcing	May not arise in II but should be kept in mind in all components.
R.28	Privacy Act compliance	Continuing requirement, but important to ensure scheme sponsors accept responsibility to draw user agencies attention to specific compliance issues prior to any implementation. Part of Component 3.
R.32	Training	May not arise in II but important to ensure no statutory constraint on training and education by scheme participants – should be considered under Component 3.

Scheme rationale and the role of Privacy Impact Assessment.

28. Privacy Impact Assessments can potentially influence the projects for which they are carried out in three interrelated ways.

  ➢ They can inform the internal development of the project, with the project sponsors and designers taking the findings into account.
  ➢ They can inform external stakeholders including the general public so that their opinions can influence the political process.
  ➢ They can inform decision makers directly so that political choices are made in full awareness of the privacy implications.

---

[10] Paua Interface Ltd *Research of Issues for Māori relating to online authentication*, 29 March 2004, Sections 5.8-5.9

29. Publication of the initial PIA, in December 2003, should have allowed all three of these mechanisms to operate.

30. The first mechanism appears to have worked – the scheme design has changed, both during the PIA process, and since December 2003, to reflect some of the findings of the PIA, although there are other contributing reasons for these changes.

31. The second mechanism has not worked, although this cannot be blamed on anyone associated with the project. There has been a resounding silence from the media and public interest groups. Whether this reflects a genuine lack of interest, or a failure to notice the PIA and appreciate its significance is open to speculation.[11] The Office of the Privacy Commissioner had also not responded substantively, until interviewed for this Update, mainly due to resource constraints, but will be in a position to make significant input in the Initial Implementation.

32. The third mechanism could have worked to the extent that decision makers outside SSC were aware of the PIA findings. While the PIA itself was available, it is more likely that busy decision makers will have relied on other sources – specifically the Business Case.

Treatment of Privacy in the Business Case

33. Recommendation 1 of the initial PIA was that the rationale for the scheme be more clearly articulated so that it could be balanced against the privacy impact (and other costs). The Business Case[12] goes a considerable way towards doing this, but will only serve this purpose effectively if it is made public, and if it accurately reflects the privacy risk identified in the PIA.

34. It is highly desirable that the Business Case, including financial estimates, be made public, to demonstrate and where possible quantify the predicted benefits that can be set against privacy and other costs (see also Recommendation 33 of the initial PIA).

35. The presentation of the PIA findings in the Business Case is generally accurate. However there is an unfortunate inconsistency and omissions in the comparison of privacy risk between the three options. The table at paragraph 348 (reproduced in the Executive Summary at paragraph 36) and paragraph 226 assert a privacy negative for the Base Case (Option 1) which is not supported by the PIA and with which the PIA consultants do not agree. In our experience, agency inconsistency almost always has a privacy protective effect on balance. The result of this assertion is to leave all three options with the same 'medium' rating for privacy risk. In contrast, the table at Appendix 4 rates Option 1 as having high compliance with the privacy protection principle, whereas Options 2 & 3 have only medium compliance. While this is more consistent with the PIA consultants view, the explanation given for these ratings highlights only one of the range of issues identified in the PIA report.

---

[11] Publication over the summer holiday period was not ideal, but cannot be the sole reason for the lack of response. While there was no pro-active publicity from SSC, the Privacy Commissioner welcomed the PIA in a media release and in its "private Word' Newsletter (issue No 50).
[12] All-of-government Online Authentication Business Case, 30 January 2004.

36. The PIA consultants would also not agree with the equivalent rating given to both Options 2 & 3 in both tables and in paragraphs 227 & 228. It is understood that Option 3 involves considerably more work than Option 2 in the area of an all-of-government Credential.[13] Whilst the vision is for both Options to ultimately lead to a full-build of the centralised authentication scheme, it is our view that Option 3 makes this considerably more likely and also likely to occur more quickly than under Option 2. The selection of Option 3 therefore incurs a greater risk of the negative privacy consequences outlined in the initial PIA, and in our view this should have been made clear in the Business Case.

37. The PIA consultants are disappointed that the findings and recommendations of the initial PIA are not fully reflected in key sections of the Business Case. The Project Team take the view that the summary tables include not only the PIA input but also their own perspective and opinion. This could helpfully have been made clear, as readers might reasonably assume that the privacy conclusions were endorsed by the PIA consultants. While it is unlikely that a more consistent account would have altered the choice of Option 3 – Initial Implementation, it would have ensured that that choice was fully informed, and additional emphasis might have been placed on addressing those privacy risks that are greater under Option 3.

38. We suggest that any public presentation of the Business Case acknowledge this reservation, and that participating agencies are expressly informed of it in the context of the work programme under the Initial Implementation.

Agency responsibilities for the Initial Implementation Programme

39. The Initial Implementation envisages some (but not all) elements of Component 2 (EOI and Credential Investigation) being carried out by the Identity Services Business Group of the Department of Internal Affairs (DIA).

40. The rationale for this is understandable, and DIA's undoubted expertise is highly relevant. The fact that DIA's Identity Services Business Group has existing responsibility for the wider evidence of identity (EOI) framework arguably gives it an even wider perspective on these issues than the EGU. This wider perspective may be better able to take account of over-arching privacy concerns – many of which are equally applicable to other applications of EOI for off-line transactions. It is also possible that DIA may revisit some of the assumptions and conceptual foundations of the proposed scheme and consider alternatives which could be less privacy intrusive.

41. However, there are risks associated with DIA's greater involvement. Any agency with operational responsibilities will inevitably find that these influence their approach to new systems. For instance, DIA's responsibilities in relation to Passports administration, and international pressures in that area, are leading them down particular paths in relation to evidence of identity and biometrics for that application. Also, the Passports, Citizenship and Births/Deaths registration programmes in DIA

---

[13] See Option descriptions in the Business Case. Both Options include work on Credentials standards but Option 3 takes this further, specifically in the context of on-line authentication, although this is not made as clear as it could be in the Business Case.

involve a legacy of existing systems, processes and thinking. It would be undesirable if the all-of-government authentication scheme was influenced too much by these legacies and current developments, rather than by an independent view of the best way of achieving either wider authentication objectives, or the specific requirements for on-line transactions with government.

42. One of the underlying risks to privacy of any all-of-government approach to authentication is that a 'highest common standard' will be preferred, leading to a 'ratcheting up' of identification requirements in areas where a lesser standard would suffice.

43. One of the advantages of the authentication project being located in SSC is that the E-government unit had no *prior* history of, or vested interest in, particular solutions, although its current commitment to the centralised ID credential could now be considered to be a constraint on consideration of alternatives which could be less privacy intrusive. While the centralised Credential is a key component of the Cabinet endorsed approach, having DIA take over some of the further investigation may open the door for re-consideration.

44. In short, it is uncertain whether, on balance, having DIA rather than SSC leading Component 2 is likely to be more or less privacy protective. Whether the allocation of responsibility for elements of Component 2 to DIA proves to be a positive or a negative in terms of privacy interests will depend partly on whether its Identity Services Business Group can maintain a neutral broker role without allowing DIA operational programmes to be any more of an influence than the interests of other stakeholders.

45. In this respect 'governance' arrangements for the Initial Implementation are very important. It is understood that there will be a formal agreement between SSC and DIA on what aspects of the II Components DIA will be responsible for; its objectives and terms of reference; what will be involved and what outputs will be delivered. It is desirable that OPC be consulted in relation to this agreement, and for it to be made public in due course.

46. We note too that appropriate governance arrangements (governance-kaitiaki) are also seen as critical to addressing issues for Māori, including their potential concerns about uses of personal information, collective privacy and related matters.[14]

Conceptual issues

47. There is a significant outstanding issue over the conceptual basis of the proposed scheme, which was addressed in Recommendation 2 of the initial PIA. Leaving aside differences in terminology[15], it remains the view of the PIA consultants that a significant opportunity is missed by not allowing for multiple registrations

---

[14] Paua Interface Ltd *Research of Issues for Māori relating to online authentication*, 29 March 2004 Sections 7.1-7.20

[15] We note some inconsistency in the use of the term 'identity' as between different documents. Given the significance of this and related concepts, we strongly recommend a review of the usage to ensure consistency.

(credentials) by the same individual, including in different names. It is accepted that this would require *some* additional personal information to be kept for *some* individuals by one or more agencies, but is more than outweighed in our view by the interest of many individuals in maintaining separate 'silos' of information representing their separate interactions with unrelated areas of government. It appears that this may be an issue of particular concern to Māori [16], but is by no means a 'minorities' issue. Controlling the breakdown of information silos is recognised by most privacy regulators as one of the most important challenges they face.

48. We do not accept that an alternative **one individual:multiple credential** approach would necessarily be overly complex or costly, or that it would necessarily be a ess effective counter to ID fraud and theft, although some government agencies hold strong views to the contrary, and the relative merits of the two approaches in this respect should be further explored.

49. The design for the ultimate authentication solution, even though it is now deferred and subject to further development, clearly remains a centralised **one individual:one credential** registration system.[17] The foundation that this lays for a population register and national identity system, as explained in the initial PIA (paras 3.17-3.24; 3.34-3.46 and 3.60-3.63) remains a major privacy risk for the proposed scheme.

50. We maintain our view that there is a central flaw in the chain of logic being used in all the discussions about evidence of identity, levels of trust and requirements for authentication of identity. This is the often implicit assertion that it is necessary to *uniquely* identify individuals for many government transactions. We continue to suggest that there is far greater scope than is commonly recognised for authentication that an individual is *who they say they are in a particular context*, without government needing to know, at least in most cases, that the individual is the *same* individual as they deal with for other purposes. We note that the Australian Federal Privacy Commissioner has recently made a similar distinction between what he calls 'bare identity' and 'social identity'.[18] He states:

> "As well as respecting the multiplicity of real world identity, allowing individuals to adopt multiple identities prevents a drift to one number per person systems, and adds another layer of practical obscurity by acting as a natural (but not insurmountable) barrier to function creep and inappropriate data linkage and aggregation."

51. The Office of the Privacy Commissioner may wish to pursue this conceptual issue, and the alternative of a **one individual: multiple credential** approach, in the Initial Implementation.

---

[16] Paua Interface Ltd *Research of Issues for Māori relating to online authentication*, v.0.3 15 March 2004 – Use of aliases or multiple names can be common practice [for Māori] but does not imply any intention of illegal activity. (Section 5.7 p27)

[17] Best Practice Framework, v.10, March 2004.

[18] *Proof of ID required? Getting Identity Management Right*: Speech delivered by the Australian Federal Privacy Commissioner, Malcolm Crompton, 30 March 2004.
http://privacy.gov.au/news/speeches/index.html

52. The extent to which the authentication scheme deals with roles, and business to government relationships, is to be the subject of further consideration as part of the policy Component (C3). This is consistent with Recommendation 4 of the initial PIA. It seems likely that these issues will also arise in the EOI/Credential work as part of Component 2, and it is important that these two components communicate effectively.

53. The issue of collective privacy has been raised in the context of Māori perspectives[19]. This needs to be explored further in both the EOI/Credential and Policy Components. It also overlaps with questions of third party authority in the context of minors and others 'without capacity' which have yet to be resolved.[20] Collective privacy has a number of dimensions – the ability of a group to act on behalf of an individual; and the rights of a group both to access information about an individual member of the group, and to participate in decisions about the use of that information. These issues should also be explored further as part of Component 4.

Shared Key pilot

54. The decision to proceed with a pilot of infrastructure for shared keys, involving a number of 'live' agency applications (Component 5) is the only 'on the ground' product (as opposed to reports, standards etc) expected from the II during its expected (2 year) lifetime. Leaving aside any agency applications that follow Standards issued under Component 1, the Shared Key pilot is therefore the only component which has the potential to *directly* affect individuals privacy during the Initial Implementation.[21]

55. Whether it does affect individuals privacy in practice depends partly on which agencies and applications participate in the pilot, and partly on what if any personal information is involved in the use of the infrastructure.

56. The functionality of the proposed Key Hub has not been specified in any detail, but it is clear that it is intended to form the basis of a long term infrastructure for a much wider application – ie: it is not a 'throw away' pilot. In the absence of any detail about the pilot it is impossible to say which if any of the concerns expressed in the initial PIA, and resulting recommendations, will remain valid. However, a number of observations can be made on the basis of the documentation available to date.

57. The Project Team are confident that a shared keys function can operate independently of any EOI processes and without a centralised Credential.[22] Service Agencies (SAs) would remain responsible for registering clients, with a requirement for EOI processes appropriate to their specific trust levels[23]. New clients could be

---

[19] Paua Interface Ltd – section 5.6.
[20] Wigley & Company Draft Report v.1.0 28 October 2003
[21] There may of course be other agency authentication initiatives progressing in parallel with this project which will have direct privacy implications. While it is intended that these should operate within the framework of Standards issued under the all-of-government Initial Implementation, it remains to be seen (as with all non-statutory Standards approaches) how well this intention can be promoted and enforced.
[22] This view is supported by the Hunter Group IQA assessors
[23] The IQA Assessors suggest that the trust level analysis needs to be updated, and this is consistent with some of the reservations in the initial PIA about the justification for requiring authentication

issued with a one-time code which would allow them access to a website to associate one or more Key Serial Numbers (KSNs) with the agency's customer ID.

58. In a idealised system, Key Providers (KPs) would not need to keep any personal information about Key holders, but it seems likely that KPs would hold personal information for a variety of purposes including the initial issuance of Keys, and the provision of help-desk services. The design does however provide for separation of roles to minimise the information held by KPs. It is possible that KPs will not hold any records of enquiries by individual Service Agencies in relation to particular keys, even for billing purposes.[24]

59. The documentation about the Shared Keys pilot seems ambivalent about multiple keys – the purpose clearly anticipates multiple keys[25], but the objective appears to remain to enable individuals to have one Key for use in all of their authenticated government online transactions.[26] These are not necessarily incompatible, but it would be helpful to confirm that the scheme will accommodate individuals who choose to hold multiple keys and use different keys for different government services. (See Recommendation 6 of the initial PIA).

The issue of whether Service Agencies should also be Key Providers is to be given further consideration – privacy and security factors are involved.

60. The pilot will also need to address the privacy and security issues about the potential use of Key Serial Numbers, highlighted in Recommendations 7 and 20 of the initial PIA.

61. A 'report-back' on the development of plans for a Shared Key Pilot is proposed in October 2004. The PIA consultants recommend that a further privacy impact assessment/technical review of these plans be undertaken for this report-back.

Review Bodies
(Initial PIA Recommendations 29, 30 & 34)

62. Ministers have agreed in principle that the existing jurisdictions of the Privacy Commissioner, Ombudsmen, Human Rights Commission and Auditor-General can between them cover the review role. It is proposed that specific agreements be reached with the OPC and OoO in relation to their involvement in the Initial Implementation Programme. While both offices will need to give preparatory consideration to community education and the handling of complaints in due course, OPC will need to be adequately resourced for participation in all five of the components of the Initial Implementation in the immediate future. It should be confirmed that OPC will be just as closely involved in those components of C2 led by DIA as it is in the EGU led components.

---

[24] *High Level Technical Design*, v.1.0, 18 February 2004. KPs would presumably bill the Central Logon Site, which in turn would bill the Service Agencies.
[25] *Implementation Options for Shared Keys Pilot*, v.0.3, 22 March 2004, paragraph 2
[26] *Outline of Shared Keys Pilot*, v.1.0 December 2003, page 1

63. The proposal to rely on existing review body jurisdictions runs the risk of complaints about the operation of any online authentication scheme falling between gaps, or alternatively duplication of effort and confusion. A detailed protocol will be required in due course, identifying the type of complaints that could arise and clearly agreeing on responsibility for dealing with them.

64. Similarly, agreement will be needed on responsibility for overall periodic review of the operation of the scheme.

65. These issues will be addressed in Component 4.

Further Privacy Impact Assessment

(Initial PIA Recommendations 11 & 17)

66. The Office of the Privacy Commissioner (OPC) will be much more closely involved in the Initial Implementation than it has been in earlier stages. However, the resources to be provided to OPC to undertake this work will not cover the detailed impact assessment required at key points in the Initial Implementation and beyond. This has been accepted and included in Component 4. It is however important to recognise that further PIA work may be required in relation to all of the other Components, including work to be undertaken by DIA in Component 2.

67. Specific PIA work has already been identified as desirable in relation to the proposed October 2004 report back on the shared key pilot (Component 5), and the proposed report back on EOI and Credential scoping work by March 2005 (Component 2).

Summary of recommended action

68. The following table indicates which of the December 2003 PIA recommendations need to be addressed in each Component of the Initial Implementation.

Component of Initial Implementation	Recommendations of December 2003 PIA to be addressed (* indicates appearance under more than one component)
Component 1 Accredited Standards	15*, 18*, 21*, 24*,27*
Component 2 EOI and Credential investigation	2*, 4*, 5, 7*, 8*, 9*, 10, 11*, 12*, 13*, 14*, 15*, 16*, 17*, 18*, 21*, 24*, 27*, 29*, 30*, 34*
Component 3 Policy Development	2*,4*, 7*, 8*, 9*, 11*, 12*, 13*, 14*, 15*, 16*, 18*, 19, 23*, 24*, 25, 26, 27*, 28, 29*, 30*, 32, 35
Component 4 Review Bodies and PIA	11*, 15*, 17*, 18*, 27*, 29*, 30*, 34*
Component 5 Shared Keys Pilot	6, 7*, 11*, 15*, 17*, 18*, 20, 21*, 23*, 24*, 27*
Generic project management	1, 33

69. There are also four further recommendations arising out of this update, as follows:

Further Recommendations (paragraph numbers are references to this report)	Component of Initial Implementation
R36. Options for locking in privacy protection, developed as part of the Policy Component should be promoted through the Standards Component and, where applicable, through legislation. (Paragraph 21)	Components 1, 2 & 3
R37. Any public presentation of the Business Case should acknowledge the PIA Consultants reservation about the presentation of privacy issues in the Case, and participating agencies should be expressly informed of those reservations in the context of the work programme under the Initial Implementation. (Paragraph 38)	All Components
R38. Governance arrangements for the Initial Implementation are critical to management of both general and Māori specific privacy issues and OPC should be consulted about these arrangements, which should also be made public. (Paragraphs 45 & 46, and 53)	Component 2 & 4
R39. The Office of the Privacy Commissioner should pursue the unresolved conceptual issues, including the alternative of a **one individual: multiple credential** approach, in the Initial Implementation. (Paragraph 51)	Component 2 & 4

End.