

Chair
Cabinet Committee on Government Expenditure and Administration

E-GOVERNMENT: AUTHENTICATION OF IDENTITY

Purpose

1 This paper outlines the proposed policy framework and implementation strategy for the authentication of the identity of people seeking to access New Zealand government services and information electronically.

Executive Summary

2 Authentication is the process of confirming the identity of a person. This paper concerns the authentication of individuals carrying out online transactions with government agencies. This will be essential to achieving the e-government vision. Currently, there is a piecemeal approach to both standards and levels of authentication across government services. Establishing a whole-of-government approach to electronic authentication will facilitate public access to, and enhance confidence in, e-government services.

3 A policy framework is proposed to ensure that the authentication of individuals by government services is carried out consistently by agencies when doing business electronically; and the risks to people and government are managed while providing opportunities for the efficiency and integration of services.

4 I seek Cabinet's agreement to:

- a the principles to underpin the policy for electronic authentication;
- b a two-stage approach to implementation as follows:
 - i Stage one - the development of technology and process standards; a risk analysis of transactions and mapping to standards; and the development of a governance model - from April to August 2002, and;
 - ii Stage two – consideration of an opt-in solution, including a review of public opinion, the political and international climate and changes in technology; and consultation with stakeholders, leading to the development of a proposed solution for presentation to Cabinet - from September 2002 to June 2003; and
- c a whole-of-government approach to the development and implementation of authentication.

5 The policy framework and implementation strategy follows a process of research of international and technical developments, existing government authentication requirements and dialogue with sector groups including local government, Ministers and representatives of the Coalition and Opposition parties. Stakeholders have highlighted the need to be able to trust the electronic authentication process before they will undertake online transactions that involve exchanging information that is private to the individual. The Office of the Privacy Commissioner has assisted in addressing the need to treat privacy concerns appropriately in framing the policy, the implementation strategy and in communications around the whole process.

Background

6 Electronic authentication entails initial enrolment of a person or entity and subsequent online verification of identity for the transaction to proceed.

7 Electronic authentication is an essential part of the security infrastructure needed for the safe delivery of online government services. It uses personal information to ensure that the requested service is delivered to the intended person. Such a function is necessary for a number of e-government developments and to achieve the mission for the Internet to be the dominant means of enabling ready access to government information, services and processes by 2004 [CAB Min (01) 10/12 refers]. By providing authentication processes that effectively manage proof of identity and protect privacy, the government will be able to build public confidence in online government services that involve personal information.

8 As part of the e-government programme, an inter-agency project team has been working since January 2001 on developing a policy framework to be used as the basis for online Government-to-Person (G2P) authentication. This has included research of international developments and local perceptions, and has involved dialogue with sector groups during the last quarter of 2001. This project has focused on G2P authentication because of the complexity of the challenges involved in authentication of members of the general public. Extension of the G2P authentication solutions to other arenas, such as business and community groups, iwi and hapu, other institutions and individuals in both New Zealand and overseas will need to be explored.

9 A policy framework is proposed to underpin development of online G2P authentication. The purpose of this framework is to ensure that:

- a the authentication of individuals by government services is carried out consistently by agencies when doing business electronically; and
- b the risks to people and government are managed while providing opportunities for the efficiency and integration of services.

Comment

Whole-of-Government Approach

10 Currently, there is a piecemeal approach to both standards and levels of authentication required for existing G2P transactions. Although there is a common role of government in stewardship of identity information there are no consistent shared standards or processes across government services. A whole-of-government approach is expected to produce net benefits although there may be net fiscal costs at an agency level.

11 One option would be to allow agencies to continue to develop authentication processes on an ad-hoc basis. The implications, however, of not adopting a common approach to authentication include:

- a proliferation of government authentication processes that will make access to government online services more complex for people and business entities;
- difficulty in establishing recognised standard levels of authentication which offer a level of security and protection appropriate to the transaction; and
- people will avoid using online services if personal information is insufficiently protected.

Benefits

12 Authentication allows the user and the provider of government services to have confidence in the identity of the other party in a transaction, and is essential for many transactions involving money or personal information. Establishing a common 'look and feel' to authentication across government would be a logical step towards making online authentication a trusted and familiar process for members of the public. Stakeholders have consistently endorsed the desirability of establishing common authentication standards and processes for G2P online transactions.

13 Authentication of identity is an accepted part of a number of offline government transactions, such as presenting a passport or similar documentation to apply for a driver licence. Electronic authentication is already being developed for certain online government services (for example, visa applications). A whole-of-government authentication approach will facilitate public access to, and enhance confidence in, e-government services.

Electronic Authentication Processes in Context

14 Current authentication technologies and systems range from simple to complex schemes, depending on the level of security required. Emerging technologies include biometrics using fingerprints, facial co-ordinates and other physical characteristics. New Zealand's G2P authentication framework needs to be sufficiently flexible to accommodate future developments in technology.

15 Methods of authentication that offer higher levels of assurance are generally more intrusive and expensive. Consequently, many countries (including the UK and USA) have opted for graduated, risk-based authentication systems for G2P transactions, using a simpler approach for transactions involving low risk and a more intensive verification process for high-risk transactions. A similar approach is proposed for New Zealand G2P transactions.

16 While authentication contributes to protection and security online, it also has the potential to evoke considerable apprehension from privacy advocates. There is a need to ensure that authentication systems are secure and do not infringe civil liberties or privacy law. There is public concern about the potential for government authentication processes to become intrusive and to involve indiscriminate sharing of personal information between agencies, particularly if a shared central G2P authentication service is established. These concerns may be a serious risk to public confidence, and hence to uptake of e-government services.

Stakeholder Input

17 Following the release of a discussion paper, there has been dialogue with key stakeholders representing government agencies, local government, voluntary and business sectors, and civil liberty lobby groups. Written responses have been invited from Ministers and members of the Coalition and Opposition parties. However, only limited responses have been received from these parties by the end of March 2002.

18 The Office of the Privacy Commissioner has assisted in addressing the need to treat privacy concerns appropriately in framing the policy, the implementation strategy and in communications around the whole process.

19 Stakeholders have highlighted the need to be able to trust the electronic authentication process before they will undertake online transactions that involve exchanging information that is private to the individual. However, public awareness of the need for online authentication or of security risks is still relatively low, though this is likely to change with the predicted gradual increase in online G2P transactions.

20 Stakeholder opinion received so far has emphasised the following points:

- the authentication process should facilitate access to online services by being simple, secure, consistent and reliable;
- government agencies need to adopt consistent processes of authentication;
- the solution should be enduring and build confidence and trust founded on good experiences;
- the person's needs should be considered above government convenience;

- it would be sensible to adopt a graduated approach to authentication built on an agreed framework for identifying levels of risk involved in transactions;
- not everyone will want to use the online authentication process so there should be an opt-in solution;
- the public does not want government agencies sharing personal information without authorisation by the individual concerned;
- it is critical that government agencies or their contracted service providers use technology to enhance services, not as an instrument of social control or commercial snooping;
- the adopted solution will require significant effort to ensure identity theft is minimised; and
- it must be possible to apply the authentication solutions beyond G2P transactions, to include other participants such as business (G2B), wider State sector agencies and local government in the future.

Policy Framework

Policy Principles

21 The following policy principles for the authentication of online G2P transactions are proposed:

Policy Principle	Explanation
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 G2P 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 G2P transactions without the use of the appropriate authentication process.

Implementation Principles

22 In considering the options for implementation, the following principles are proposed:

Implementation Principle	Explanation
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	Providing an approach based on agreed trust levels that protects identity and personal information
Legal compliance	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

Risks and Issues

23 The main risks and issues that affect authentication also exist in an offline environment. These include:

a Civil Liberty Concerns

- A very intrusive or mandatory approach to authentication will cause significant negative public reaction from civil liberty advocates and is likely to bring an adverse response from the broader public.
- The public will perceive that the introduction of electronic authentication is placing a further demand on them by government.
- The perceived loss of privacy or civil liberties could lead to loss of trust in authentication and impede overall uptake of e-government services.
- Failure to introduce a more ordered and consistent approach to authentication than is currently the case may result in user confusion and dissatisfaction in some sectors.
- In considering implementation solutions, it will be difficult to satisfy all parties where potentially controversial issues have to be addressed.

b Legal

- The key risk areas that are likely to give rise to privacy issues in an electronic authentication model are security, and error or failure with data and systems.
- Financial loss may occur if a transaction fails or a fraudulent transaction is accepted.
- Litigation against the Crown for consequences of relying on a failed authenticated transaction.

c International

- If authentication issues that impact across international borders are not addressed, conflicting

standards and loss of confidence from other jurisdictions may arise, e.g. requiring New Zealanders to seek visas to visit other countries where visa-free access currently applies.

d Security

- Appropriate security architecture is necessary in order to deliver the level of security intended and to prevent hacking, identity theft and denial of service attacks.
- Abuse of the system or data held on it by Public Service staff.
- Physical risk to an individual may occur as a result of a serious breach of privacy issues, as is the case with existing government systems that hold personal information.

24 These risks will be considered during the proposed two-stage implementation project. It may, however, not be possible to satisfy all parties and interests.

Implementation Strategy Development

25 Given the level of concern expressed by stakeholders about the role of government in authentication, a phased approach to developing an authentication solution is recommended. Consultation with stakeholders will be undertaken during the solution development process. The first step would be the promulgation of the policy framework set out above within the Public Service with other government agencies and local government. At the same time, a project would be launched (to be carried out from April 2002 to 31 August 2002) to undertake the first stage of implementation that involves:

- a risk analysis of all proposed G2P online transactions for government agencies (including SOEs and Crown entities) to establish levels of need for authentication;
- b establishment of agreed evidence of identity (EOI) standards;
- c development of process standards for each authentication level and identification of any appropriate technology requirements;
- d exploration and analysis of the feasibility of a future opt-in G2P online authentication function;
- e an initial estimate of the costs and privacy impact assessment for each of the various options;
- f development of an appropriate information security model; and
- g development of a governance model for the authentication solution.

26 The second stage of implementation to take place from September 2002 to June 2003 will include a review of current developments (to include the political and international climate, public opinion and changes in technology), leading to the development of a proposed solution, including an enhanced privacy impact assessment and a cost estimate for presentation to Cabinet.

27 The E-government Unit would manage the set-up phase for a whole-of-government approach for online authentication of G2P transactions (stage 1). There would however be an ongoing need, beyond any project activity, to maintain and monitor the authentication levels and standards and to review agency behaviour in accordance with the policy framework.

Governance

28 In considering a possible opt-in whole-of-government solution, my initial view is that the Government would retain the responsibility for managing the authentication process, in particular

initial recording of identity details. The proposed solution may require an independent party such as an ombudsman or commissioner to maintain and monitor standards and behaviour, handle complaints and provide advice, as well as an independent audit function. Such an appointment would encourage public trust and protect human rights in a government authentication process. Further work to determine the requirements and cost of an independent authority will be undertaken during stage 1 of the implementation strategy.

Links to Other Government Initiatives

29 The proposed approach includes consideration of a service that would offer the potential for individuals to provide their details once, but for that information to enable transactions with multiple agencies. This is consistent with the Policy Framework for New Zealand Government-held Information that states that government departments should make information available easily, widely and equitably to the people of New Zealand (except where reasons preclude such availability as specified in legislation).

30 The implementation project constitutes a core element of the e-government programme and is essential to the achievement of the e-government vision. Successful acceptance of the authentication solution by people may lead to its broader approval for services outside central government. Coincidentally, this may assist the uptake of e-commerce.

Promulgation of the Policy Framework

31 It is important that any government developments that require electronic authentication are consistent with the policy framework and implementation approach set out in this paper. Cabinet direction to adopt the policy framework is necessary to ensure that the risks identified earlier in this paper, and expenditure of public funds on such developments, are managed effectively.

32 Such direction will require Public Service departments, and encourage other government agencies (non-Public Service departments, Crown entities and State-owned Enterprises), to liaise with the E-government Unit of the State Services Commission on any potential or existing developments that involve electronic authentication. Subject to Cabinet's approval, the policy framework will be promulgated to government agencies and liaison maintained with local government.

Consultation

33 Consultation on this paper has been undertaken with the Public Service departments and selected government agencies.

34 Overall the recommendations have received clear support. A number of implementation issues have been raised. These will be considered and discussed with agencies during the staged implementation project.

Financial Implications

35 Funding for the next phase of work through to June 2003 is covered by the budget of the E-government Unit. Implementation costs of any recommended solution will be subject to a bid for funding. Any future compliance costs to agencies arising from the implementation of authentication standards, as well as the costs of setting up, operating and independently monitoring any proposed opt-in authentication solution, will be identified in a paper to Cabinet at the end of the first stage of implementation (June 2003).

Privacy Implications and Human Rights

36 The proposals contained in this Cabinet paper have been assessed by the Ministry of Justice for compliance with the New Zealand Bill of Rights Act 1990 and do not appear to give rise to any issues of inconsistency with that Act. A final view as to whether the proposals comply with the Bill of Rights Act will be formed once the legislation and/or standards have been drafted.

37 A privacy impact assessment will be undertaken in stage I to identify the potential effects that a solution may have on privacy and to examine how any detrimental effects might be mitigated.

38 The Human Rights Commission notes that all the major human rights issues arising within this paper fall within the ambit and expertise of the Privacy Commission. Liaison with both Offices will continue during the implementation project.

Legislative Implications

39 The establishment of standards and a policy framework does not require legislative change at this time. It may, however, be necessary at a later stage to legislate for the establishment of governance (refer paragraph 28) and regulatory provisions to support an independent role, and to provide penalties to deter improper application or deliberate breach of the authentication standards and process.

40 Consideration also needs to be given to whether it will be necessary to have legislation affording an appropriate level of protection for the public against activity such as identity theft and denial of service attacks. In addition, if the authentication solution proposes variation from the requirements set out in the Privacy Act 1993, a privacy code may be required.

Regulatory Impact and Compliance Cost Statement

41 The regulatory impact and compliance costs of a proposed authentication solution will be identified in the Cabinet paper to be delivered in March 2003. There may be some compliance costs associated with the authentication standards. These costs cannot be estimated at this stage.

Gender/Treaty of Waitangi Implications

42 Te Puni Kokiri confirms the policy framework has no Treaty of Waitangi implications at this time. There are no gender implications at this time. Any implementation issues will be dealt with during the first stage of implementation.

Publicity

43 As there has been considerable interest in this project, a media statement will be released once Cabinet has reached a decision on the policy framework and implementation process.

Recommendations

44 I recommend that the Cabinet Committee:

- 1 **note** that consistent, secure and cost-effective management of electronic authentication – the original proof, maintenance and protection of individual identity – is considered necessary to gain the confidence of people before they will participate in New Zealand government services online;
- 2 **note** that the purpose of a policy framework is to ensure that the authentication of individuals by government services is carried out consistently by agencies when doing business with people electronically; and the risks to government and people are managed;

- 3 **agree** that the following principles underpin the policy framework for electronic authentication of people who undertake online transactions with the New Zealand government:

Policy Principle	Explanation
3.1 Security	Suitable protection must be provided for information owned by both people and the Crown
3.2 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
3.3 Protection of privacy	Ensuring that the proposed authentication approach protects privacy appropriately
3.4 All-of-government approach	Balancing public and agencies' concerns about independence with the benefits of standardisation while delivering a cost-effective solution
3.5 Fit for purpose	Avoiding over-engineering, recognising that the levels of authentication required for many G2P transactions will be relatively low
3.6 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 G2P transactions without the use of the appropriate authentication process.

- 4 **agree** that the following principles be included in the policy framework and apply to the development of authentication solution(s):

Implementation Principle	Explanation
4.1 User focus	Ensuring the recommended solutions are as convenient, easy to use and non-intrusive as possible
4.2 Enduring solution	Providing a solution that is enduring yet sufficiently flexible to accommodate change and a wide range of current and future transactions
4.3 Affordability and reliability	Ensuring the recommended solutions are affordable and reliable for the public and government agencies
4.4 Technology neutrality	Ensuring a range of technology options is considered, and as far as possible avoiding 'vendor capture'
4.5 Risk-based approach	Providing an approach based on agreed trust levels that protects identity and personal information
4.6 Legal compliance	The solution must comply with relevant law, including privacy and human rights law
4.7 Legal certainty	Relationships between the parties should be governed in a way that provides legal certainty
4.8 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

4.9 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
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 5 **direct** Public Service departments to:
- 5.1 adopt the policy framework set out in recommendations 2, 3 and 4 above; and
 - 5.2 liaise with the E-government Unit of the State Services Commission on any potential or existing developments that involve any aspect of electronic authentication;
- 6 **invite** non-Public Service departments, Crown entities and State-owned Enterprises to:
- 6.1 adopt the policy framework set out in recommendations 2, 3 and 4 above; and
 - 6.2 liaise with the E-government Unit of the State Services Commission on any potential or existing developments that involve any aspect of electronic authentication;
- 7 **note** that the E-government Unit of the State Services Commission will, as part of its continued liaison with the sector, invite local government to take advantage of the policy framework and to participate in the development project;
- 8 **agree** to the two-stage approach to develop an authentication model for implementation that involves:
- 8.1 Stage 1 (from April to August 2002):
 - risk analysis of all proposed G2P online transactions (including SOEs and Crown entities) to establish levels of need for authentication;
 - establishment of agreed evidence of identity (EOI) standards;
 - identification of the appropriate technology requirements and development of process standards for each authentication level;
 - exploration and analysis of the feasibility of a future opt-in G2P central online authentication function;
 - an initial estimate of the costs and privacy impact assessment for each of the various options;
 - development of an appropriate information security model; and
 - development of a governance model for the authentication solution.
 - 8.2 Stage 2 (from September 2002 to June 2003):
 - a review of public opinion, the political and international climate and changes in technology regarding an opt-in solution;
 - a cost-benefit analysis of implementation options;
 - detailed design of the preferred option;
 - a paper to Cabinet by June 2003; and

- 9 **note** that the Minister of State Services and State Services Commissioner will promulgate the policy framework for electronic authentication of the identity of people who undertake online transactions with the New Zealand government.

Hon Trevor Mallard
Minister of State Services

