

ONLINE AUTHENTICATION PROJECT DISCUSSION PAPER

Purpose

The Authentication project is still some way from determining a policy framework to recommend to the Government. Your feedback on the issues and key questions in this discussion document will assist the project team in identifying key priorities, to determine the validity of our approach and to identify any gaps. Any other comments or suggestions will be gratefully received and considered as we progress the analysis that will result in a draft policy framework for authentication of G2P (Government to Person) online transactions in New Zealand.

Background

E-government Strategy

The Government launched its e-government strategy in April 2001 stating, 'Turning government into e-government is essential if New Zealand's public sector is going to maintain its high quality performance in the information age. The Government's vision for e-government is:

New Zealanders will be able to gain access to government information and services and participate in our democracy using the Internet, telephones and other technologies as they emerge.

Its mission is:

By 2004 the Internet will be the dominant means of enabling ready access to government information, services and processes.

There are a number of instances where an authentication process will be needed to make that access sufficiently secure to allow the clear and reliable identification of an individual as well as the safe delivery of services to the right individual.

The Need for Authentication

Authentication – both proof and protection of individual identity – is a key component of the successful achievement of the Government's e-government objectives. Authentication presents issues of the proper management of proof of identity and protection of privacy and confidentiality about which New Zealanders must be confident before they will participate in e-government.

It is therefore essential to gain as comprehensive an understanding as possible of the issues authentication presents in order to be able to deliver the confidence about their management that the success of e-government requires.

The Authentication Project

The Authentication project is concerned with creating a policy framework to ensure that:

- government services delivered over the Internet go to the right person;

- people are who they say they are; and
- privacy is protected at all times.

This project is specifically concerned with G2P transactions, i.e. transactions between the Government and a person, but may have application for at least small businesses.

The project is jointly chaired by the Department of Internal Affairs and the State Services Commission, with a number of other government agencies contributing, e.g. Justice, IRD, Ministry of Social Development.

The first phase of the project, which began in April 2001, focused on fact-finding around four major themes:

- the need for authentication;
- overseas experience and implementation of authentication solutions;
- the New Zealand legal framework; and
- communications issues.

Findings to Date

The high-level findings of the first phase of work indicated that:

- a variety of manual and online authentication processes is already used in New Zealand for G2P transactions;
- the main processes used for authentication, both in New Zealand and overseas, offer a mix of advantages and disadvantages, and it is likely that a framework of guidelines for matching processes to transaction types (and their associated needs and risks) should be developed;
- it is likely that existing New Zealand legislation will cover the bulk of authentication needs;
- the protection of privacy will need to be addressed very carefully; and
- further information is needed in order to establish:
 - the relative priority of public interests and issues around authentication;
 - the desirability of having a central authentication option available; and
 - the range and level of transactions that may require authentication, and their relative complexity and risk.

A key objective of this discussion paper is to generate the information needed to make decisions in these three areas.

Four Key Principles

Phase one of the project identified four key principles that underpin the authentication project. These are:

- technology neutrality – ensuring that a range of technology options is considered;
- cultural fit – ensuring that the recommended authentication approach is appropriate to the New Zealand people and environment;
- public user focus – putting the user’s needs, concerns and overall perspective at the forefront; and
- avoiding over-engineering – recognising that the levels of authentication required for many transactions will be relatively low.

Phase Two

The second phase of the project has two main strands. One is focused on further exploration of specific needs and risks and on authentication technologies. The second is a process of dialogue with stakeholders (outlined below). The two strands of Phase two will feed into the final analysis underpinning a draft policy framework for authentication. Phase two is expected to conclude in November 2001.

Dialogue Process

The aim of the stakeholder dialogue process is to explore authentication issues with interested parties and to identify any views, issues and priorities that will need to be taken into consideration in developing a draft policy framework. Parties invited to contribute to this dialogue phase include members of the public, community groups and agencies, government agencies and members of the IT and security sectors.

Authentication Technologies

The range of technologies already in use in New Zealand for manual or electronic authentication includes passwords, PINs, “secret” questions, digital certificates, software or hardware based encryption keys and biometrics. An outline of these technologies and their major advantages and disadvantages is attached as an appendix at the end of this paper.

Key Authentication Issues

When is Authentication Needed – Managing Risk

Authentication is generally needed to manage the risks or prevent the adverse consequences that can arise when a transaction fails in some way. These risks or consequences may be borne by the government agency, the individual, both parties or, in rare cases, a third party. Risks exist in G2P transactions when:

- private information is involved;
- financial value is involved;

- the transaction verifies the individual's entitlement to something; and
- the transaction effects a change in legal status.

There are some exceptions. Transactions such as paying taxes are unlikely to attract impersonators, so authentication may not be a major issue. Other transactions may involve notifications to existing persons or addresses, or payments to known bank accounts, so that there is a lesser need for authentication.

The types of risk that may arise for individuals and Government include:

- inconvenience to the identity holder;
- risk to the identity holder's personal safety or property;
- release of personal or commercially sensitive data to third parties;
- the risk of financial loss to any party;
- risk to a party's standing or reputation, including loss of public confidence in core government systems or services; and
- effects on the commission or detection of serious crime.

(This categorisation is based on the UK Government's "Trust Level" framework, used to determine levels of authentication.)

Making Authentication Work - What do Users Need?

A number of user-focused questions need to be considered in developing an authentication framework. These include:

- how capable will the user group be of using the required technology?;
- will the user group access the authentication system from the same computer/application (eg many users of one PC in a household)?;
- how much will the authentication technology cost the user (including any need to upgrade personally owned technology, on both a one-off and on-going basis)? Can they afford this?;
- what are the compliance costs regarding time and effort?;
- do users perceive the authentication process as having sufficient security and managing their risks effectively?; and
- how does this group view the relative importance of risk and convenience?

Question:

what are the key usability limits that will need to be taken into consideration for G2P transactions (e.g. technology levels, complexity of process ?

Weighing up Risks and Convenience / Cost

At the current stage of development, authentication technologies which offer most protection also tend to be more expensive, complicated to learn, and are often inflexible.

New Zealand experience to date indicates that users tend to favour the most convenient methods of authentication. The question of the relationship between user preferences and who bears the cost in the case of an authentication failure is important. Some systems users may be acting as agents for those who will ultimately suffer loss from a failure in authentication and, therefore, could excessively favour convenience over security. Other users have been willing to bear considerable risk in order to avoid the inconvenience of a "strong" (PKI-based) authentication system.

The issues associated with tradeoffs between convenience and risk will often be different for government agencies than for commercial entities. Banks for instance, routinely transfer the risks of misuse of card/PIN systems to customers or vendors. Such risk transfer will not be possible or appropriate for the Government in situations where customers have a legal entitlement (say to a benefit) under statutory regulation.

Question:

are there types of transactions or risks where the potential risks involved mean that risk should always be considered ahead of convenience; or transactions where the needs of users mean that convenience should always be put before risk considerations?

The Registration Role

All authentication processes rely on an initial process that is frequently called registration. This is the process by which the individual's identity (or evidence of identity (EOI)) is established and registered with the agency, the result of which will be relied on to confirm that identity when authentication takes place. Some kinds of transaction may contain elements of registration, e.g. the processing of passport applications, which involves careful checking of identity.

PKI-based (Public Key Infrastructure) authentication processes rely on organisations known as Certification Authorities to collect and verify the EOI information. Some governments carry out the Certification Authority functions themselves or have oversight of the accreditation of commercial providers. Australia, for instance, has set up a system for accrediting certification authorities against stated criteria.

Question:

what is the appropriate role and level of involvement for the New Zealand government in registration processes underpinning authentication?

An Alternative System - Holding Individuals' Identity Data

The Irish Government has provided for an electronic 'dossier' of information about individuals' identity, which can be held on their behalf by an independent agency. Individuals will be able to update their information and control the access to it by government

agencies. This system has the potential to save individuals the task of repeatedly providing the same information, and could provide agencies with a level of assurance about the quality of the information they receive.

Although such a system offers potential benefits to authentication, and lowers compliance costs, it is wholly dependent on public acceptance and uptake. It is also predicated on an existing system that has already assigned a unique identifying number to each potential user. The ease with which such a model could be applied in New Zealand is unknown. It is certainly clear that New Zealand privacy legislation explicitly bars the type of unique identifier used by the Irish government.

Question:

do we want to adopt an authentication framework such as that in Ireland that requires changes to existing privacy legislation to allow for unique identifiers? (This approach could be included as an opt-in element in a broader framework that did not use a universal unique identifier for G2P transactions).

A Graduated Approach to Authentication

The level of risk involved in each type of G2P online transaction will vary. If a graduated approach to authentication is adopted, the type of authentication used can be matched to the level of risk the transaction entails. Where the risk is considered high, a “strong” authentication process is likely to be recommended. Where the risk is lower, a “weaker” form of authentication would be considered acceptable and appropriate. This approach would depend on acceptance of an agreed framework for identifying levels of risk. Frameworks of this type are already in use by the USA and UK governments.

Questions:

*do we want to adopt a graduated approach to authentication built on an agreed framework for identifying levels of risk?; and
what should the framework consist of?*

A Single “Strong” Authentication Approach

One alternative would be to apply a “strong” authentication approach to all G2P transactions. This approach has already been adopted in certain countries; examples are Singapore and a number of European countries such as Finland. The common factor in all cases is that these countries have a long-standing acceptance of the use of a unique identifier that individuals use in their dealings with Government. It is also generally accepted, even expected, that a substantial amount of personal information will be automatically divulged to the Government and publicly available. In contrast, New Zealand has a long-standing aversion to the use of a unique identifier in dealings with Government, and New Zealanders tend to set a very high value on personal privacy.

Question:

do we want to adopt a single “strong” authentication approach built around the use of a unique identifier that individuals use in their dealings with government?

Central Provision for Authentication

It would be possible to provide for individuals to authenticate themselves (possibly to different levels) at a central location, say on the Government portal. They would then be able to transact (at the level to which they had authenticated themselves with different agencies). Such a system would be desirable only if individuals needed to transact with several agencies and valued a consistent and central means of authentication. It could be compared with having a “master key”.

The disadvantages of centralised authentication include the possible perception that other things (such as information sharing) may be occurring behind the authentication process. Centralised authentication (even if levels of authentication were involved) would also reduce the ability of government agencies to match authentication techniques to their judgements about the risks involved in transactions, and the demands of the statutory regimes under which they occur.

Question:

do we want to adopt a central system of authentication where individuals authenticate themselves (possibly to different levels) at a central location – say, the Government portal?

How Much Consistency?

It is tempting to assume that users will want authentication methods to be consistent between similar government services, and possibly similar to those applied in comparable commercial transactions. However, it is not yet clear how many different government agencies people would transact with in a way that required authentication at any particular period in their lives. Many kinds of transactions (such as retrieving information) will not require authentication at all, and others (such as payments and purchases) may be sufficiently authenticated by the funds transfer element of a transaction.

If most individuals needed to conduct authenticated transactions with only one or two agencies (e.g. IRD or DSW), consistency might not be a very significant issue. If an individual is, however, dealing with a number of government agencies online, using a range of different authentication processes could cause significant inconvenience. The application of common standards at common authentication levels could ease this problem (e.g. all user-name/password authenticated transactions could use the same type of user-name syntax and password rules).

Question:

do New Zealanders want authentication methods to be consistent between government services and possibly similar to those applied in comparable commercial transactions?

Your Comments Invited

Your feedback on the issues and questions discussed in this paper will assist the project team in identifying key priorities and areas that require further investigation. The authentication

project team is holding a number of meetings to receive your comments. Otherwise please send your response to:

Laura Sommer
Joint Project Manager
Authentication Project
E-Government Unit
State Services Commission
PO Box 329
Wellington

Fax: (04) 495 6669
Email: laura.sommer@ssc.govt.nz

APPENDIX: AUTHENTICATION PROCESSES

As mentioned in the main paper, there is a variety of authentication mechanisms in use in New Zealand and overseas. The main types of electronic authentication currently in use, together with their major advantages and disadvantages, are as follows:

User-name / Password, PIN, Secret Answer

The most common authentication processes are based around one or more things that the individual knows, but that are more or less secret, e.g. passwords and PINs. The advantages of these methods are that they are relatively cheap and simple to set up, and they require little education of the user because of their familiarity. The technology is already in place, and the user can “roam”, and log in from many places. A password or PIN is relatively simple to replace if it is compromised or lost. Systems using passwords will also typically ‘lock’ an account if an incorrect password is entered more than a defined number of times when trying to log in. These are often used in combination with ‘something possessed’ e.g. the credit card.

The biggest disadvantage of passwords and PINs is that they do not offer a very high level of security. Most users tend to select simple passwords that are easily guessed (such as their first name, date of birth, or pet’s name), and it is relatively easy to find software that is designed to “crack” passwords. This risk can be mitigated by more stringent password policies (e.g. requiring a minimum of eight characters including alphabetic and non-alphabetic characters, and checking that a password has not been used by that user before).

Users also have a tendency to forget their passwords. Some causes are: the system generates them for the users or the password policy forces the user to pick passwords that are hard to remember! Helpdesks often use a pre-arranged “secret question” (e.g. mother’s maiden name, or a particular identifier) to confirm the identity a caller who claims to have forgotten their password.

A further risk of passwords is that they are often shared. All too often, users also store passwords insecurely (e.g. on post-it notes attached to the PC!). In addition, users are sometimes persuaded to divulge their password or PIN to a caller purporting to be the Helpdesk.

Public Key Infrastructure (PKI) and Digital Certificates

A PKI makes widespread use of public key encryption possible through the use of digitally signed certificates – ‘digital certificates’. Each user generates an encryption key, which is stored either in **software** or in **hardware**; this “private key” can be used to “authorise” transactions. A **digital certificate** contains the ‘public key’ that is mathematically related to the individual’s ‘private key’. This means the user can use their private key (and no other key) to decrypt and read messages that have been encrypted with their public key; and the service provider who receives a transaction can use the user’s public key (and no other key) in the digital certificate to check that the user’s private key was used to “authorise” the transaction.

There are still risks around PKI, in particular the security around private keys, and the quality of initial authentication by registration authorities. Although PKI does not enable private keys to be forged, it cannot discern who is actually using one. Poor security around the

keeping of private keys (especially when stored on computers) can severely compromise the level of authentication actually provided by PKI solutions. The authentication applied by registration authorities when initially registering a user is critical (e.g. checking the authenticity of the documentation supplied to verify an application). The issue of the private ownership of certification authorities and their susceptibility to take over or failure also needs to be considered.

Software-based keys

Software-based key storage, stores the private key on disk, and uses encryption to keep the private key confidential and authenticate anyone wishing to use the private key. Typically a password, or PIN or pass phrase, will be required to access the private key. (The private key is stored in encrypted form on disk and the password, etc., is used to decrypt it.) This approach offers stronger security than PIN or password alone.

The major disadvantages are concerned with cost and the physical security of the disk. Additional software must be purchased and installed on each PC used, and the digital certificates that contain that public keys themselves are moderately costly. There are some security risks – private keys can be stolen or deleted by gaining access to the PC (and password), and they can be lost due to software or hardware problems. There are also technical matters that add risk or inconvenience. Software-based keys can be shared without the system knowing and most computer applications have no inbuilt native support for authentication by keys such as those used in digital certificates.

Hardware-based keys

This category of authentication mechanism covers a range of options, all based on the use of a physical device (generally called a ‘token’) to hold the private key and the corresponding digital certificate. This approach has most of the advantages of software-based keys, including a robust level of security. Certificates are easy to use, and can generally be supplemented with a password or PIN that is required to access the information stored in the token (e.g. smart card with PIN). Unlike software-based keys, the secret information is not stored on a PC that might be vulnerable to attack, but always travels with the user. It can therefore be used at any location that has an appropriate token reader.

Like software-based keys, hardware-based keys are relatively costly, and require software to validate them. Some hardware-based devices such as smart cards also require additional hardware on each PC to read the key. Tokens can be lost, stolen or mislaid (for example, left at home). Like passwords, tokens can be shared; although once the token has been given back to its owner the compromise no longer exists. Technical difficulties can also arise, as most computer applications have no native support for authentication by either proprietary hardware devices or keys such as those used in digital certificates.

Digital certificates

Digital certificates are an increasingly common mechanism for assisting authentication of entities via public key encryption. Digital certificates are issued by Certification Authorities (CAs) that carry out the initial identification of certificate holders and provide the bona fides of the certificates that they issue. A user will send their public key and proof of identity to a CA. If the CA is satisfied as to the user’s identity, then the CA will issue a digital certificate

containing the user's public key. In effect, the certificate is a transaction to the world, "authorised" using the CA's own private key. Typically a, commercial CA will issue more than one class of certificate. The classes are differentiated by the amount of effort the CA goes to confirm the user's identity (and personal history).

Certificates may be issued by a public company or government agency that has been established as a CA, or agencies may undertake the role of CA directly for their own staff. In either case, there is a requirement for appropriate recognition of a CA before certificates issued by it can (or should) be accepted by any given system. Certificates tend to be relatively expensive.

Public Key Encryption

Public key encryption as already stated above, differs from normal encryption in that it uses pairs of keys. The two keys in each pair have the relationship such that a message that is encrypted with one key can only be decrypted with the other key.

By publishing one key - making it 'public' - and keeping the other key secret - 'private' - the person who generated the keys can receive confidential messages and "authorise" transactions. In the wider electronic commerce environment, the challenge is to publish the public keys in such a way that service providers and vendors have confidence that the public key is indeed from the user.

A PKI provides such an assurance, through the CA's using their own private keys to "authorise" digital certificates (each containing a user's public key). The publishing problem then is reduced to publishing 10s of public keys, as opposed to 1000000's. Currently, the public keys for the major CA's are included with each release of Netscape's and Microsoft's browser.

Biometrics

Biometrics refer to authentication processes that are based on the identification of individuals by means of unique human characteristics, e.g. fingerprints, retinal scanning, facial recognition, voice recognition. Biometrics offer a high degree of security, and cannot be shared with another person. It is almost impossible to lose a biometric identifier, and it cannot be forgotten. The biometric travels with its owner at all times, so is highly portable.

Arguably the greatest disadvantage of biometrics is that they generally require specialised hardware devices such as "readers", which are not yet generally available. At this stage of development, the systems that validate biometrics are proprietary and are not operable with standard systems. Most biometrics are not yet considered 100% accurate. There are also issues of privacy and cultural acceptability around some biometric processes, as some are considered intrusive or strongly associated with detection of criminal activity (e.g. fingerprinting).

Biometric authentication is typically expensive. The expense is incurred not only in hardware at each point of authentication, but also in the effort required to 'train' the system to recognise each individual user. Biometrics also present some security issues. They require a secure infrastructure to manage the risk of the abstract representation of a biometric attribute (e.g. the digitised fingerprint used for comparison) being stolen and replayed. Once a biometric

attribute has been compromised, it cannot be replaced (e.g. most people have only one right thumb).