e-government
www.e-government.govt.nz

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga

Authentication for e-government

Best Practice Framework for Authentication

APRIL 2004

About this handbook:

The CD ROM that accompanies this handbook contains the following resources:

1. A navigation map to help you use this document more effectively: map.pdf
2. A copy of the document as a pdf: bpf.pdf
3. E-government Strategy: strategy-2003.pdf
4. Online Authentication handout summarising Cabinets decision: handbook.pdf
5. Blueprint: Authentication for e-government: blueprint.pdf
6. Authentication for e-government: Privacy Impact Assessment Report: pia.pdf
7. Authentication e-government: Summary of RFI Response: rfi-summary.pdf
8. Authentication for e-government: Summary of proposed business processes: business-process.pdf
9. Online authentication: Summary report on consultation feedback from agencies and public representatives: feedback.pdf
10. Reference Standards and Guidelines for NZ Information Systems: Ref-stnd-guide.pdf

ISBN 0-478-24456-8

For more detailed information and document updates, see *www.e-government.govt.nz/authentication* or please contact:

Authentication Team
E-government Unit
State Services Commission
PO Box 329
WELLINGTON
E-mail: *authentication@ssc.govt.nz*

Foreword

New Zealand's e-government programme uses new technologies and processes to help public sector agencies work together to meet the needs of New Zealanders. The e-government mission is that:

> By June 2004, the Internet will be the dominant means of enabling ready access to government.
>
> By June 2007, networks and Internet technologies will be integral to the delivery of government information, services and processes.
>
> By June 2010, the operation of government will have been transformed through its use of the Internet.

This transformation of government will be characterised by agencies taking an all-of-government approach when designing and implementing services, and by the customisation of services to meet the needs of individuals and businesses.

Achieving this, and providing more sophisticated government services via the Internet, means that agencies and people need to be confident in the trustworthiness of online services. The basis for public confidence in dealing with government online is consistent authentication policies and technologies that enable both individuals and agencies to have confidence in the identity of each other when transacting over the Internet.

The Government approved a set of policy and implementation principles for online authentication in April 2002. Since then, the E-government Unit of the State Services Commission, with input from relevant experts and agency supporters, has been working on an online authentication solution for e-government in New Zealand.

This Best Practice Framework has been developed to summarise the lessons and learnings to date. Whilst work continues on an all-of-government solution, the Framework will allow those individual agencies that have an immediate need for online authentication to proceed with confidence in the steps they take now.

I commend this Best Practice Framework to agencies and encourage them to adopt its recommended approaches. Adopting 'best practice' in this area is an important step as we move towards an all-of-government solution to online authentication.

State Services Commissioner
April 2004

TABLE OF CONTENTS

Introduction

This Best Practice Framework outlines issues and approaches that government agencies should consider in planning and implementing online authentication solutions.

Online Authentication

The Internet, and its associated technologies and business models, are profoundly affecting the way government, business and people interact. Government is adapting to this new environment in a way that will eventually transform how it operates.The design and delivery of services are already changing to meet the changing needs of New Zealanders.

New Zealand E-government Strategy – June 2003

You can find further background reading about online authentication on the e-government website - see **www.e-government.govt.nz/authentication/**

Online Authentication is the equivalent of walking into a government agency and dropping your passport, birth certificate and latest phone bill on the desk of the nearest public servant, except you don't get your feet wet or have to search for change to catch the bus. You also don't have to empty the third drawer down to find your coffee-stained birth certificate or pay a fee to a government agency for a new one so you can take it to another government agency.

Online authentication enables Government to move beyond simply providing information online by transforming itself into a multi-channel, transactional service provider.

The objective of Online Authentication is to provide consumers of government services with the opportunity to apply for, and receive, services over the Internet without having to appear in person every time. Achieving this requires answering a number of important questions, including:

- What does a person need to do to establish their identity?
- Once identity has been established, how can another party trust that identity without requiring the person to fully re-verify themselves?
- If a person transacts with government online, how can the fact that the transaction occurred be proven if the person later denies it?

Online Authentication is about taking advantage of the opportunities the Internet offers for both the public and government agencies. This Best Practice Framework was developed to assist in achieving this, by providing guidance to agencies on the concepts involved, and on technical considerations and policy issues.

01 Context

The sections below explain the importance of online authentication to e-government and summarise the strategic direction planned for online authentication in the New Zealand government context.

E-government Strategy and Authentication

The New Zealand E-government Strategy sets out the Government's strategy for transforming the operation of government through harnessing information and technology, in particular the Internet.

The goals of the Strategy are:

- Better services – more convenient and reliable, with lower compliance costs, higher quality and value;
- Cost effectiveness and efficiency – cheaper, better information and services for customers, and better value for taxpayers;
- Improved reputation – building an image of New Zealand as a modern nation, an attractive location for people and business;
- Greater participation by people in government – making it easier for those who wish to contribute; and
- Leadership – supporting the knowledge society through public sector innovation.

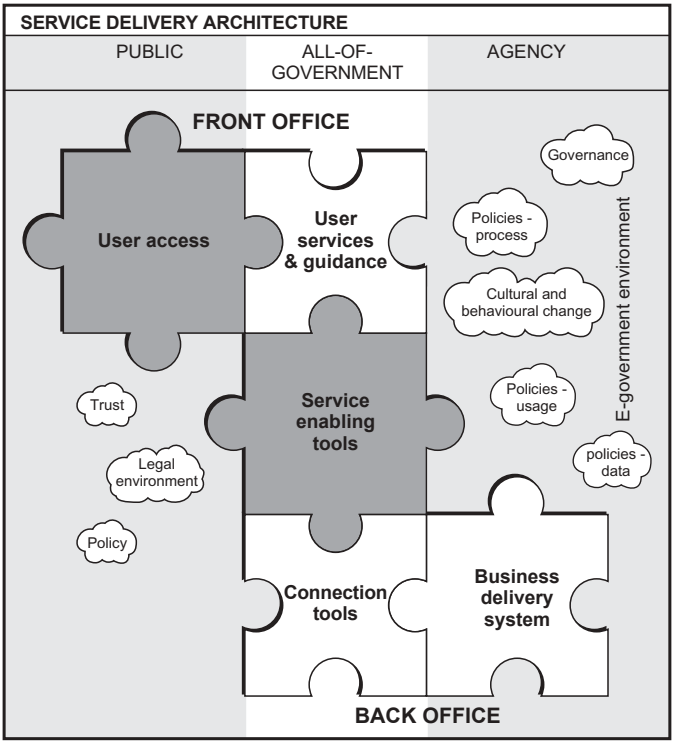
When the long-term transformational goal is achieved, it is expected that the delivery of government services, and potentially the operation of government itself, will be redefined. This will be reflected in an environment that is characterised by agencies taking an all-of-government perspective when designing and implementing services and the customisation of services, to meet the particular needs of individuals and businesses.

The E-government Strategy is published on the government website – see **E-government Strategy 2003**

Developing online authentication is an integral step in realising the transformational mission and supporting goals. Greater consistency in the way government deals with people will in particular contribute to the goal of better service, and the cost effectiveness and efficiency. It will be achieved by creating a consistent way for people to establish their identity in the electronic environment where this is required to transact with government.

The following diagram illustrates the significance of authentication to the New Zealand E-government Strategy – the highlighted pieces are those aspects where there is a requirement for an authentication mechanism.

Online Authentication addresses the 'User access' and 'Service enabling tools' components in the diagram on the next page. It provides the interface between the public and government.



Strategic Vision for All-of-government Authentication

Key – an example of a Key in this context would be a username/password combination, PIN or token a user could use to access government services online.

Achieving an all-of-government approach to online authentication is a goal that the Government has been committed to since April 2002. The vision for all-of-government authentication is to provide a single means by which people and government agencies authenticate their electronic identity.

This vision will be achieved when:

- individuals can have a single Key or 'log in' for their online transactions across different agencies;
- individuals will only have to establish their identity once and it will be acceptable by all government agencies (in ordinary circumstances);
- government agencies operate in collaboration to ensure that authentication processes are seamless;
- individuals will be provided with a site they can use to log-in to government agencies, and individuals will know this is a trusted site; and
- a government agency implementing a new authenticated online service can use the existing government authentication mechanism rather than building its own.

Achievement of the vision would be evidenced by increased intra-government agency collaboration, and would also facilitate increased opportunities for people to participate in government using the Internet.

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 individuals use to authenticate themselves to government agencies could be relied on when they choose to transact with a non-government agency.

Towards All-of-government Authentication

Work is underway to achieve the strategic vision. This Framework is a significant step in ensuring that government agencies are well-positioned to adopt the all-of-government solution when it is eventually implemented.

Please refer to the **e-government website** for current information on the status of the all-of-government authentication initiative.

The following phases of agency evolution will be required to prepare for the implementation of the all-of-government solution:

- Standardisation – agencies design, implement and operate their authentication solutions in the same way. This will enable them to leverage off each other's experiences and means that the authentication systems and processes appear consistent from an individual's point of view;
- Collaboration – some agencies and sectors cluster together to share authentication solutions, reducing duplication of cost and effort for both agencies and individuals; and
- All-of-government Authentication – with a uniform approach to authentication already being followed by all government agencies, the all-of-government solution can be implemented with minimal change for agencies or individuals.

It is important that each government agency looks to adopt the guidance in this Framework in order to minimise the future need for the agency to carry out re-work. This is particularly important because the Framework will provide the basis for the mandatory standards that will be issued and audited against as the standardisation phase, outlined above, commences. Agencies that have already designed or implemented their own online authentication solution should look to adopt the Framework as part of solution upgrades or replacements to their systems.

About this document

This document was produced by the E-government Unit (EGU) of the State Services Commission as part of the Online Authentication Project.

The E-government Unit provides leadership and co-ordination of the e-government programme. It is working with government agencies to achieve the Government's vision for e-government.

The EGU has been working with a range of public interest groups and agencies to examine what online authentication might mean for New Zealanders dealing with government agencies. In 2002 this work resulted in Cabinet approving a set of policy and implementation principles for authentication.

In 2003 Cabinet decided to proceed with the design and scoping of an all-of-government approach to online authentication. The work programme

prescribed by Cabinet included the development of a framework to define authentication best practice for government agencies [CAB Min (03) 22/2 refers].

In line with Cabinet's direction, this Best Practice Framework focuses on the authentication of individuals and does not address the authentication of entities (such as organisations and businesses) or the verification of attributes (such as ownership, membership or qualifications) that are not primary attributes of identity.

Purpose

This Best Practice Framework is intended for those managers and agency staff planning or implementing an online initiative that has a requirement for authentication.

The Framework provides:

- information on concepts and terminology related to authentication;
- references to an all-of-government approach and the long-term strategic vision for all-of-government authentication;
- guidance and advice regarding the issues that need to be addressed through planning and policy work; and
- information on implementing an online authentication initiative and issues to consider.

The Framework provides guidance and advice for agencies to assist them in accurately determining their authentication requirements and investigate options for implementation. It is also intended to promote consistency in authentication practices across government agencies.

The Framework does not specify standards for mandatory adoption by agencies - where relevant, reference to more detailed information and applicable standards has been included.

Document Structure

The document is structured to provide readers with informational sections that are relevant and practical for online authentication initiatives within government agencies. Sections have been designed so that readers can easily locate the information that is most relevant to them.

A guide to the colour coding and document structure is set out below.

1. Context

This section provides information related to the E-government Strategy and the significance of the strategic vision for all-of-government authentication.

It is intended to provide readers with information and context around authentication, the objectives behind the Best Practice Framework and how it fits with the all-of-government vision. This section will be of particular interest to readers wishing to get a high-level view of government authentication initiatives and long-term strategic goals for online authentication.

2. Core concepts

This section acts as an authentication primer providing an introduction to authentication and some of the basic concepts involved.

This section will be of particular interest to readers wishing to acquire or build on their knowledge of authentication principles and concepts.

3. Planning

This section provides information on issues that should be considered during the planning stages of an initiative and to assist agencies to determine their authentication requirements and options.

It is intended for readers interested in the issues to be addressed during the planning or requirements stage of a project. In addition, information is provided to complement and provide input into risk management proposals and mitigation.

4. Policy

This section provides policy information related to government services, in particular on those related to online authentication. It provides 'high-level' policy guidance on issues related to any authentication initiatives. It should be referred to, both in any early planning stages of a project and at the end of subsequent stages to ensure a consistent policy approach is being maintained.

This section will be of particular interest to readers concerned with policy and the impact that any proposed authentication solution may have on their agencies and clients. It should also be read by technical staff who need to understand the types of policy consideration that arise from an authentication solution.

5. Implementing Authentication

This section describes and provides guidelines around implementing online authentication solutions. It provides detailed information on implementation options for the concepts covered in the earlier sections of this document, and focuses on positioning agencies towards an all-of-government approach.

It is intended for readers with an interest in the technical implementation of authentication, and those wishing to explore their authentication options around design and build. This section will be of particular interest to readers with a technical interest and some previous background in authentication.

6. Implementation Considerations

This section contains important considerations related to implementing authentication solutions, including those related to an all-of-government approach and selection of products and services.

It is intended for those readers exploring their implementation options by highlighting important points for consideration. It should be read in conjunction with the previous section 'Implementing Authentication'.

7. Advisory Roles

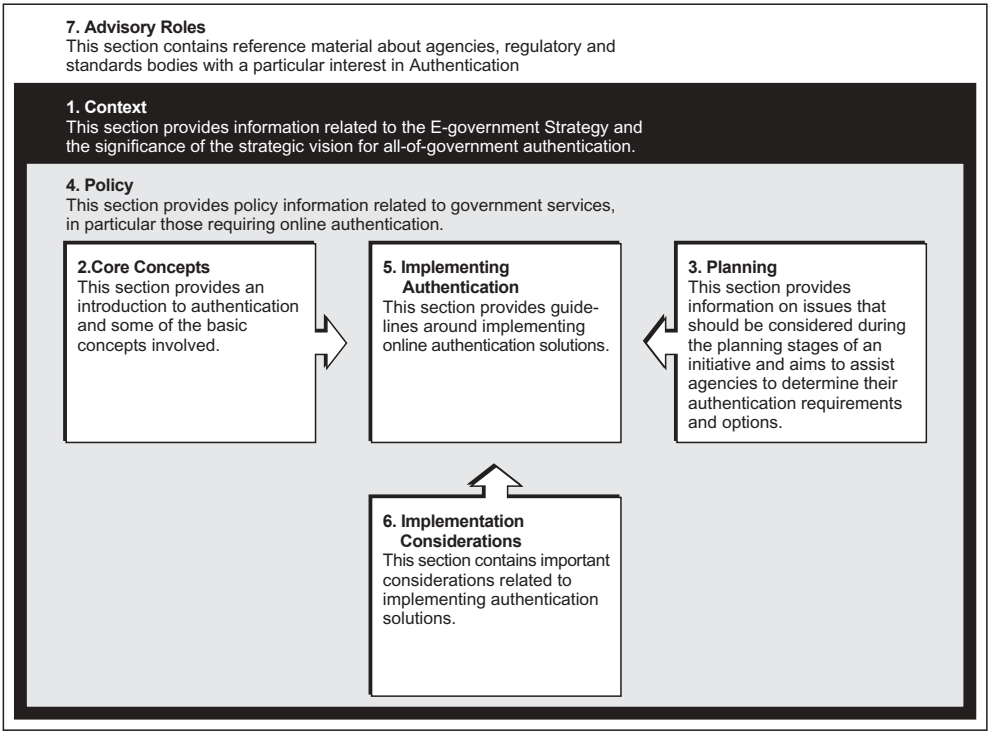
This section contains information related to agencies, and regulatory and standards bodies with a particular interest in authentication.

It is intended to provide readers with a list of agencies that can provide

further information and advice related to implementing an online authentication initiative. This section will be of particular interest to readers concerned with compliance with standards and government directives around implementing major IT projects.

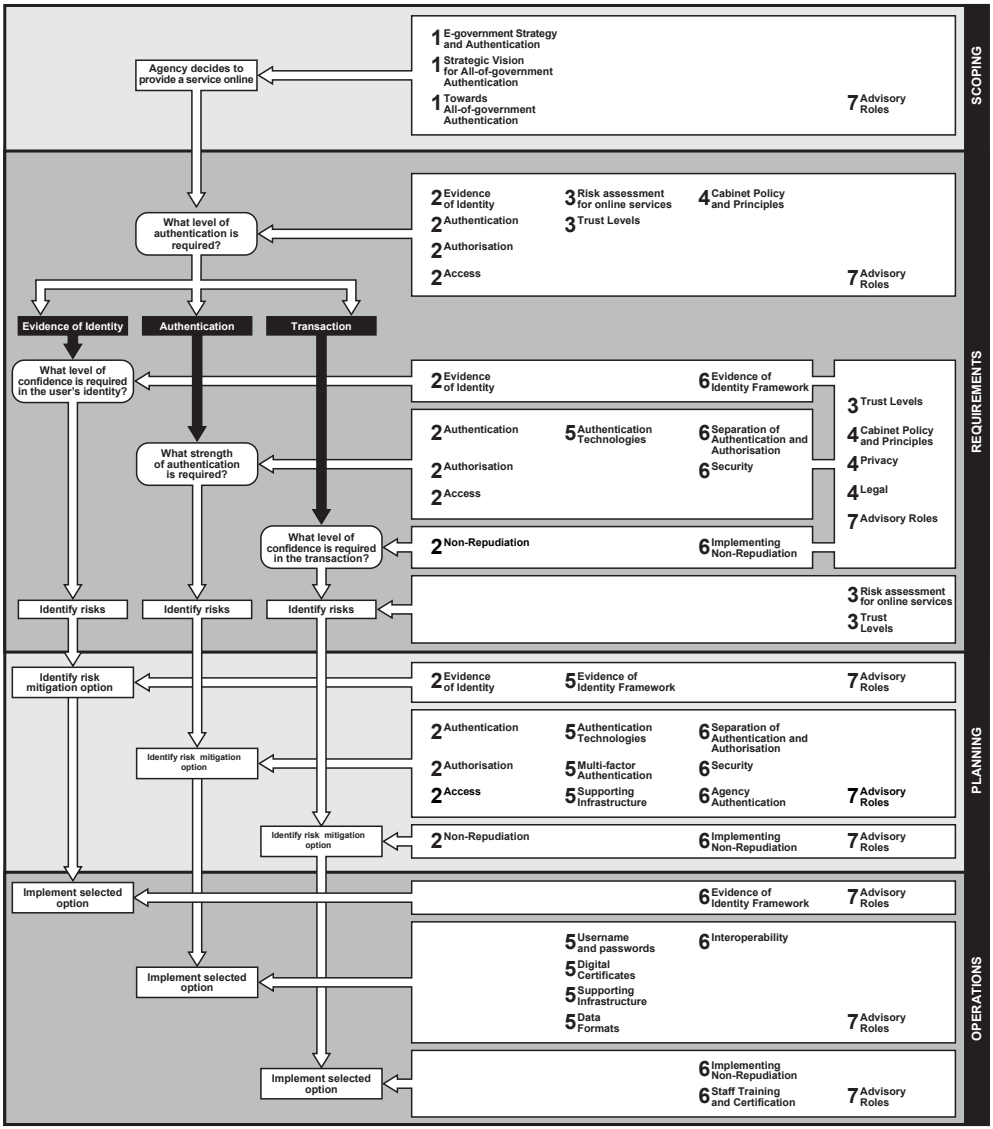
The Advisory Roles, Context and Policy sections are relevant across all phases of deploying an authentication initiative and are relevant to all sections. Core Concepts, Implementation Considerations and Planning sections should be used as references to the Implementing Authentication section.

This diagram provides a high-level view of the Best Practice Framework document and illustrates how the sections of the Framework relate to each other.



The following, more detailed, diagram illustrates which subsections of the Framework relate to the various implementation decision points that an agency might face. For each decision point, the diagram indicates the main sub-sections in the document and how they relate to the authentication process. Not all sub-sections are included in the diagram.

Note that a full-sized version of this diagram is included on the attached CD-Rom. (Nav Map)



For Advice and Updates

The Framework is one of a series of documents related to an all-of-government approach to online authentication and is aimed at providing a guideline for agencies in the area of authentication.

It is important to note that, as with any document of this nature, this Framework will be revised periodically to reflect changes in authentication technology and practices, and to reflect government decisions regarding the strategic direction of online authentication. Readers should ensure that they have the most up-to-date version of the Framework and liaise directly with the E-government Unit for further information.

It is a Cabinet requirement that all government agencies liaise with the E-government Unit around plans relating to online authentication. Cabinet Paper 2002 – Summary available at **http://www.e.govt.nz/authentication/cabinet-paper.asp**

For more detailed information and document updates, see *www.e-government.govt.nz/authentication* or please contact:

Authentication Project Team
E-government Unit
State Services Commission
PO Box 329
WELLINGTON
E-mail: *authentication@ssc.govt.nz*

02 Core Concepts

The main questions related to authentication are the same, whether performing transactions online or when receiving services in person from a government agency.

- What does a person need to do to establish identity?
- Once identity has been established, how can another party trust that identity without requiring the person to fully re-verify themselves?
- If a person transacts with government, how can the fact that the transaction occurred be proved if the person later denies it?

Solving these issues in an online environment requires addressing the same underlying concepts as found in an off-line situation and then applying the concepts to the Internet environment.

The sections below introduce the core concepts of authentication.

Evidence of Identity

Evidence of Identity – definition: The establishment of a person's identity attributes to a level of confidence for the required purpose.

An Evidence of Identity [EOI] process, is the process by which an agency establishes confidence in a person's identity. This means that the person provides sufficient evidence of their identity and also evidence that the identity actually belongs to them.

Examples of how an individual may establish EOI include: presenting a birth certificate or their passport to an agency, or providing the details of a referee who can vouch for their identity details.

For information on how a robust Evidence of Identity may be established refer to section – **Evidence of Identity Framework.**

Authentication

Authentication - definition: The act of establishing the authenticity of, or proving, something is genuine.

In the context of online transactions, authentication is the process of establishing, to the required level of satisfaction, the identity of one (or more) of the parties of the transaction. In more common terms, it is generally the act of an individual logging in to a computer or website.

The notion of authentication also applies in the reverse direction; that is, establishing the identity of the computer or website that the individual is connecting to.

For information on techniques and options on Authentication, refer to section – **Authentication Technologies.**

Authentication for an individual can be accomplished by several means by:

- demonstrating that you know a shared secret;
- presenting a token (which presumably cannot be forged); or
- demonstrating physical characteristics unique to the individual (biometrics).

Depending on security policy, authentication may require multiple forms of authentication, usually of different types. This is called multi-factor authentication.

Only after an entity is authenticated, can authorisation or access control be performed.

For further information on establishing the identity of the website, refer to section – **Agency Authentication.**

Authorisation

Authorisation – definition: The act of giving authority or legal power.

Whereas authentication is used to establish the identity of a party to a transaction, authorisation is used to determine what privileges that party will enjoy. With typical online applications, individuals are authorised to view/change information related to themselves and conduct transactions such as purchases, using their own resources.

Authentication is a prerequisite to authorisation.

There are two common types of authorisation:

- *Group - based Authorisation*

Group - based authorisation is the more common of the two types. Users are organised by groups and each group is given a specific authorisation profile. While generally suitable for managing access for large groups of people to a website, this scheme sometimes lacks the flexibility required for fine-grained control of a large group of resources or a diverse group of users.

- *Role - based Authorisation*

Role - based authorisation is the other common authorisation scheme. User roles are defined, each with specific authorisation privileges or limitations. Users are given one or more roles. The advantage over role - based authorisation is that business processes and rules usually map more easily onto this type of system.

Access Control

Access Control – definition: The mechanism(s) by which systems grant or revoke rights to view/modify information or to perform some action.

Access control is the provision of authorised privileges to an individual. It is the mechanism that controls at a low level, what actions an individual can perform, or will be performed on their behalf.

While authorisation and access control seem very similar, they are different. Authorisation gives permission for an activity, access control conducts the activity.

It is very common for authorisation and access control to be tightly coupled in software products.

Non-Repudiation

A communication has the attribute of 'non-repudiation' if it is protected against a successful dispute of its origin, submission, delivery, or content. In other words, non-repudiation offers a party to a communication protection against a false claim by another party that the communication never took place.

Secure Electronic Commerce

Authentication is concerned with establishing the identity of a party during a transaction. Non-repudiation is a much broader issue related not only

to establishing identity but also to establishing:

- that the transaction took place;
- the authenticity of the message contained within that transaction;
- that the message was both sent and received by the parties involved;
- the authenticity of the message over a period of time and that the message has not been tampered with or altered in any way; and
- that either party cannot deny any of the above points.

Non-repudiation requirements arise in both the offline and online worlds. When a government agency and an individual sign a contract on a single piece of paper, each party authenticates itself by a handwritten signature. In doing so their signatures are linked to the promises on the same page and they cannot go back on those promises. Flowing from the authentication is the desired outcome of non-repudiation. The same outcome is needed in similar online situations.

It is important to note that non-repudiation is not seen as solely a technical or e-commerce issue. Its origins are in legal history and precedence. Early examples of non-repudiative actions include wax seals commonly used in the 18th century and hand-written signatures used today.

Without non-repudiation, the agency and person must bear the increased risk of:

- contractual obligations on either party not being enforceable;
- liability for any loss by either party being the sole responsibility of the agency;
- reduced public confidence in agency capability and trust; and
- services being provided to the wrong person.

Many online systems are not designed with sufficient robustness to meet non-repudiation needs, particularly where the courts demand a high level of proof (such as in relation to fraud prosecutions).

Achieving non-repudiation, or more importantly, being able to achieve enough non-repudiation to dispute any denial by the other party that any part of the transaction took place, requires the same level of robustness in both the offline and online worlds.

When considering their legal and practical position in real-world digital transactions, parties are better advised to ask themselves, not "Will we have non-repudiation?", but rather "Will we have credible evidence to persuade the third-party dispute-resolution authority (for example, judge, jury, or arbitrator) that we have enough non-repudiation?"

Agency Authentication

Generally, when discussing authentication, the concern is primarily with identifying the end user. However, it is equally important to consider that the end user (individual) is concerned that the agency authenticates that it is genuine. This is Agency Authentication.

People often make the assumption that when they type in a web address (a URL) or click on a link, that they are guaranteed to go to that website. While generally correct, this assumption can be wrong.

For guidelines on how to mitigate agency authentication risks – refer to the section in this document – **Mitigating Agency Authentication Risks.**

There are a number of ways that users can find themselves unintentionally visiting a website that is masquerading as a legitimate provider: keyboard typing mistakes; false links from websites or email messages; or DNS spoofing attacks. These masquerading websites can look and behave exactly like the legitimate website, making it difficult for the user to detect.

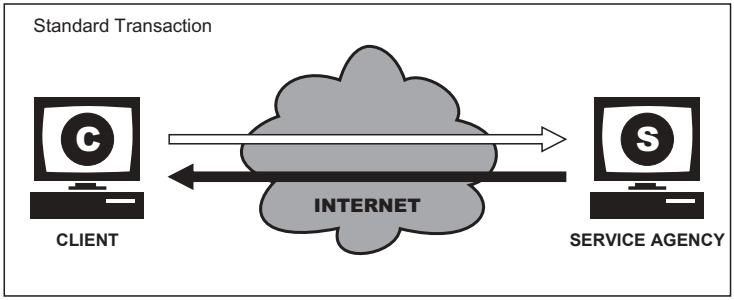
The risk is that users may visit a false website then enter their username and password in an attempt use the 'services' that the website supposedly provides. The false site could record that information (the username and

password) and use it later for fraudulent purposes.

The sections below provide background information on types of risks agency authentication mitigates, and that advice on best-practice mitigation techniques.

Examples of Agency Authentication issues.

In a legitimate online transaction, the Client transacts directly with the service agency. The Client visits the legitimate service agency website and, when requesting a service, provides their username and password (or other method) to that site to authenticate themselves. Once authenticated, the Client's transaction can be handled by normal business processes.



Issues arise when the service agency website is targeted by hackers in an attempt to obtain client identity information and thereby access to Client records. These attacks fall under two broad categories:

1. Re-direction to a fake website (Phishing).

2. Man-in-the-middle attack (MITM).

1. Redirection to a fake website (Phishing).

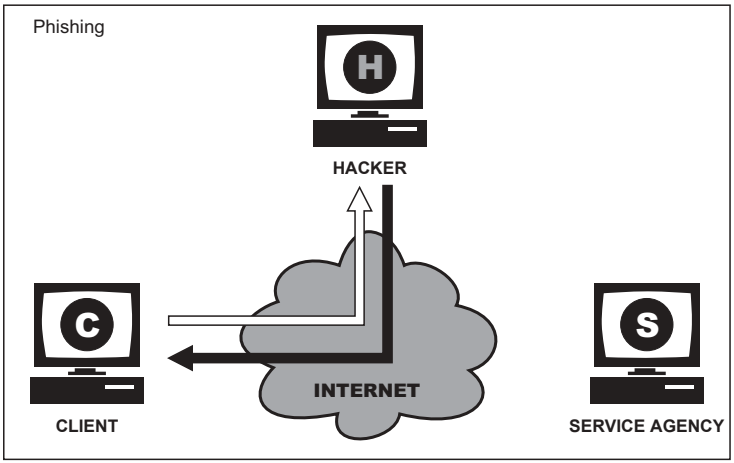
The Internet is based upon open standards. This makes replicating the appearance of a legitimate website reasonably easy for a competent hacker, and very difficult for the user to detect.

A working group called the *Anti Phishing Workgroup* recorded 176 unique phishing attacks in January 2004 – a 52% increase from December 2003.

Phishing (or redirection) involves the hacker (phisher) substituting their false website for the service agency's authentic website. The Client logs into the false website and, believing it is authentic, provides their username and password to the hacker.

There are many variants on how phishing is accomplished, including:

- sending the Client an email and asking them to click on a fake website address;
- DNS spoofing (where the website address entered by the Client is translated into a fake Internet Protocol address);
- superimposing a fake website over the top of the legitimate site; and
- taking advantage of Internet browser configuration security flaws and the inherent security limitations in the use of URL's.



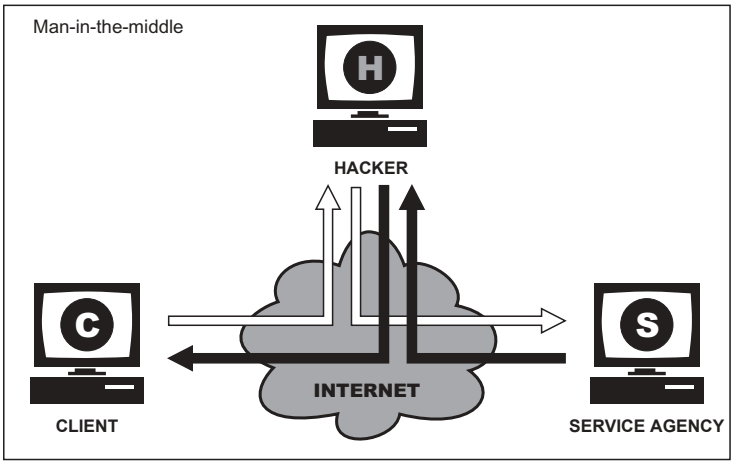
2. Man-in-the-middle [MITM] attack.

This occurs when a hacker intercepts a transaction between the Client and service agency. By 'positioning' themselves in the middle of the transaction, the hacker monitors and records transaction details between the Client and service agency. Once the hacker has the identity details, they can either use them to request a service, authenticating themselves using the Client's username/password, or simply to monitor the transactions and record the Client's behaviour.

MITM is a complex and difficult technique to mitigate against. Any information the Client uses to authenticate themselves can be repeated by the hacker back to the agency and vice versa. The Client believes they are transacting directly with a legitimate service agency.

From a hacker's perspective, a 'man-in-the-middle' attack is complex to set up. Currently it is less common than other forms of hacking techniques.

Guidelines to assist in mitigating Agency Authentication risks are discussed in the **Mitigating Agency Authentication Risks section.**



Notes:

03 Planning

3

Online authentication establishes to the required level of confidence, that the person you are interacting with online, is the person they claim to be. The interaction may be around something as basic as providing information on an agency website, or it could be a transfer of land title or a benefit application. It is important for agencies to clearly understand the type of transaction they are seeking to deliver online, and to understand the level of risk related to the transaction. This is because, as the level of risk rises, so does the level of authentication required to provide the service online in a secure fashion.

This section explains how risk assessment and the classification of online services by 'Trust Level' provide a guide to determining the best means to implement authentication for your online service.

Risk Assessment for Authenticated Online Services

Risk management is an iterative process of well defined steps which, taken in sequence, support better decision making by contributing a greater insight into risks and their impacts

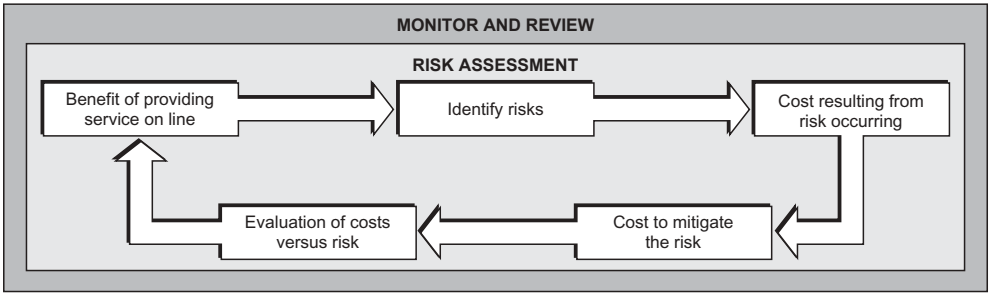
AS/NZS 4360:1999 – Risk Management

Authentication for online transactions should be considered in the context of an agency's overall information system security framework. As this section focuses only on authenticated online services, government agencies should refer to the following sources for more comprehensive and detailed analysis of the risks associated with a complete information system:

- Information Technology – Code of Practice for Information Security Management. AS/NZS ISO/IEC 17799:2001;
- Risk Management. AS/NZS 4360:1999;
- Government Communications Security Bureau. New Zealand Security of Information Technology [NZSIT] publications; and
- Guidelines for Managing and Monitoring Major IT Projects – published by the State Services Commission and Treasury.

Risk Assessment Approach

Risk assessments are intended to enable agencies to identify the risks relating to a proposal or operation and to determine what, if anything, could and should be done about those identified risks.



The risk assessment process set out in the chart and steps above is designed to provide agencies with guidance on how to develop their own assessment plan, based on their organisation's individual requirements and objectives.

Risk assessment is an iterative process. With each iterative cycle, risk criteria and management processes become more detailed and stronger. It is important to note that even after an online service has been implemented, periodic monitoring and review to identify any new risks, potential opportunities and benefits should be carried out.

Benefit of providing the service online – Step 1

Positive Client benefits are also a useful predictor of the likelihood of the service's popularity with Clients.

The first step in assessing risk is to complete an assessment of the benefits of providing the service online. This may include financial benefits (such as a reduction in transaction costs if the client can initiate and partially complete a service request online), and client benefits (such as a reduced requirement to appear in person at an agency). Determining the benefits to Clients may require a qualitative approach to measuring aspects such as convenience, acceptance, usability and satisfaction. For a detailed explanation of quantitative and qualitative analysis, refer to section 4.3.4 of 'Risk Management – AS/NZS 4360: 1999'.

Other benefits will not be so easily quantified and will have a reliance on:

- management's strategic vision to determine how providing the service online complements the agency objectives and mission statement;
- business units determining how it best fits with business drivers and existing processes; and
- client feedback and consultation around areas such as convenience, ease of use and acceptability of the service.

Identify risks – Step 2

A comprehensive identification of risk includes consideration of risks to Clients.

Allowing online access to all personal information and services may be beneficial to the agency and the Client, but this must be balanced against the risk of the information being fraudulently or erroneously obtained or accessed by an unauthorised individual.

To allow for accurate mitigation action to be identified, it is important to accurately identify the potential risk itself and not to get side-tracked by the result if the risk eventuates. For example, a stolen password may allow unauthorised access to account information and the subsequent fraudulent receipt of a service. In this example the risk is that a password may be compromised and not the provision of an unauthorised service.

Detailed and accurate risk identification will assist in identifying cost-effective mitigation factors.

Cost resulting from risk occurring – Step 3

Once the risks have been identified, the cost to the agency and its Clients of the risk occurring can be investigated - and subsequent mitigation plans can be developed. Similar to the quantification of benefits in Step One,

the cost of a risk occurring may not be easily quantifiable. For example, quantifying loss of trust and confidence in the agency, reduced acceptance of future online initiatives and loss of data integrity.

Cost to mitigate the risk – Step 4

Once likely risks and their impacts have been identified, options and solutions to mitigate the risks can be investigated. A combination of technology, policy and processes should be looked at as potential mitigation options. For example, it may be possible to mitigate the most severe risks by designing applications that allow most of the transaction to be completed online, but to require the person to complete that part of the transaction with the most risk potential using an in-person, offline component.

In formulating risk mitigation approaches, care needs to be taken to ensure that risk avoidance, in the form of being overly risk averse, is not mistaken for risk management, which is adopting a proactive approach to minimising the impact in the event of a worst-case scenario.

Having identified the most appropriate approach to mitigate against the identified risks, the agency can then determine the cost of that risk mitigation approach.

Evaluation of costs versus benefits – Step 5

The final step is to evaluate whether the benefits of providing the service online are greater than the cost of providing the service and managing the risks involved.

One means of ensuring that the evaluation is carried out consistently is to use a pre-determined threshold based on business objectives and cost-benefit returns. If the assessment indicates that an online service is consistently below the threshold - this may be an indication that more benefits can be obtained and/or that the implementation is too risk averse. Being consistently above the threshold may indicate the risks and/or the projected returns from the service have been set too high. For these reasons it is important to establish the threshold prior to performing the assessment, to ensure the initial objectives and business drivers of the project maintain an influence on the direction of the project.

The business objectives should include benefits to the Clients, such as increased access to services that are convenient and easy to use.

Trust Levels

One of the key factors influencing the authentication requirements for an online service is the degree of certainty required about the identity of the individual seeking to use the service. The Transaction Trust Levels ('the Trust Levels') were developed to provide guidance to those agencies considering providing a service online - by enabling them to categorise transactions on a consistent basis. This was intended to ensure that transactions of a similar type are implemented using similar authentication solutions.

A Trust Level assessment is ordinarily carried out in parallel with a Risk Assessment.

Four Trust Levels for transactions

The policy framework for online authentication in New Zealand specifies the following Trust Levels. The definition of the Trust Levels is based upon the Trust Levels developed by the UK Office of the e-Envoy:

Level 0 – Anonymous user. Transactions that do not require the user to be identified or require protection of a user's identity. For example, access to online publications.

Level 1 – Pseudonymous user. Access is provided for transactions that do not require a person to be uniquely identified, but the service agency must be able to respond to the user. For example, to 'recognise' the person when he/she accesses the service on return visits.

Level 2 – Identified user. Access is provided for transactions that require that a person be specifically identified. For example, establishing a bank account.

Level 3 – Identified user and verified transaction. Access is provided for transactions that require the person to be specifically identified; verification of the integrity of the data exchanged and the exchange itself; and the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction. For example, obtaining a passport.

Categorising Online Transactions

Trust Levels assist in categorising transaction types based on individual agency requirements around three components of an authentication transaction. The three components are:

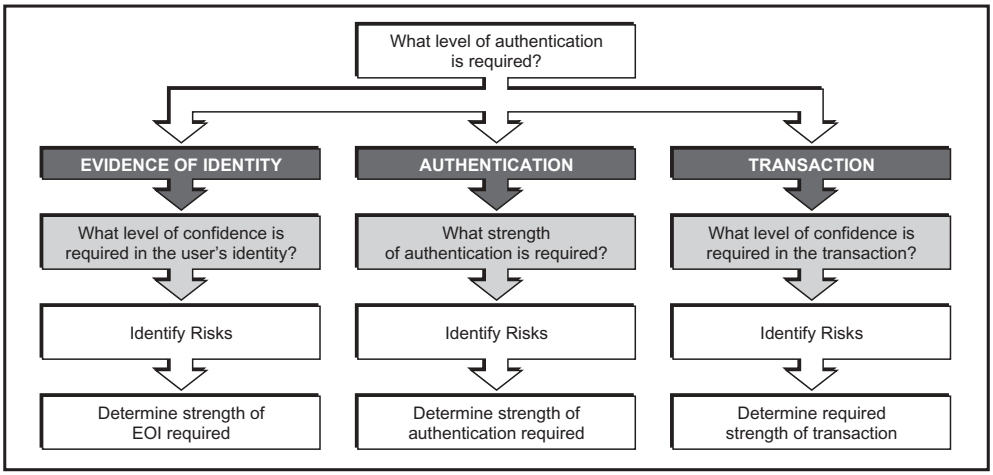
It is important to clarify that authentication strength is not solely provided by technology. For example, the banking industry implements 4-digit PIN's to allow their customers to use ATM machines. This should not be considered a low strength option as it also relies on the user having possession of their money card and the ATM machines themselves also provide additional security considerations.

1. Evidence of Identity [EOI] Strength. EOI strength is the level of confidence an agency requires in any identity information provided by the user. For example, a utility bill with the user's name and address compared to the user's passport and confirmation of the details from a third party.

2. Authentication Strength. Authentication strength is the level of confidence implied through the use of an authentication method. For example, a simple 4-digit PIN on its own would have a lower authentication strength compared to a digital certificate or complex userid/password combination.

3. Transaction Strength. Transaction strength is the level of confidence an agency requires in an online transaction. For example, a low-strength transaction may only require an acknowledgement via email that a service request has been received; a high-strength online transaction may require many of the factors related to non-repudiation of a transaction, for example evidence of who authored the request, proof a message was sent and received, and the message was not tampered with and can be stored securely.

3



Determining component strength

The requirement for component strength is based on the need for protection against a pre-determined risk level. These risk levels should be based on an individual agency' risk assessment using their own criteria and specific risk management processes. This would include impact on their Clients, effect on existing business processes and the overall agency strategy and objectives.

For example, for a transaction where there is a high likelihood of identity fraud taking place, the Evidence of Identity component would need to be strong. However, for another transaction the risk of identity fraud might be low but the fall-out from information being released inappropriately could be very high. In this case the agency may determine the need for a strong transaction strength component.

For further information and guidance on determining individual agency risk levels refer to **Standards NZ publication - Risk Management – AS/NZS 4360:1999**

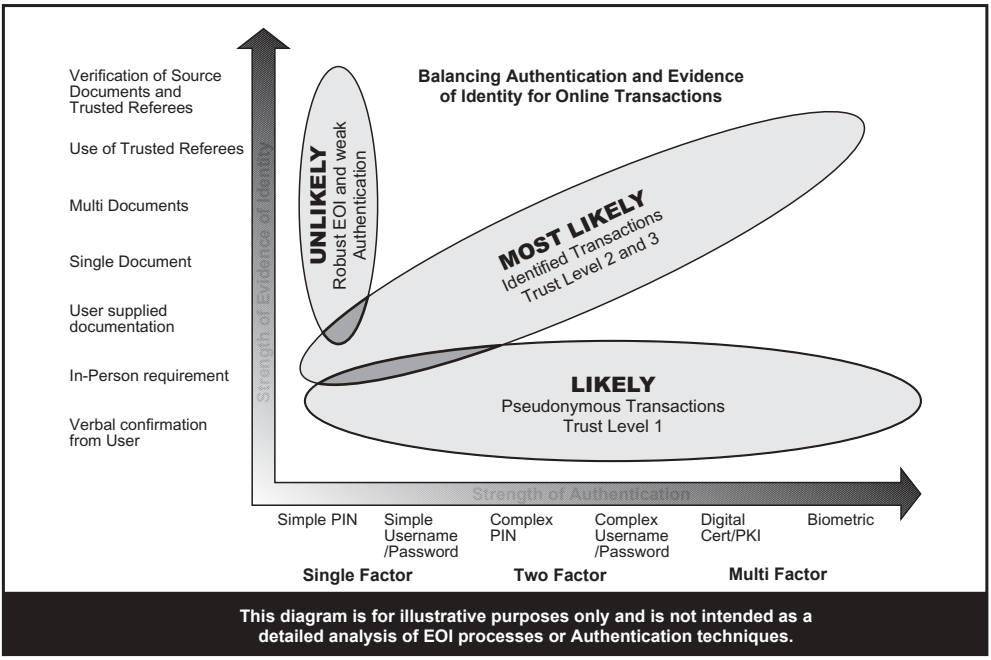
Balance between the components

Within each Trust Level there are valid combinations of the three components at different strength levels. This means that a particular transaction can be assessed at Trust Level 2 with the need for very strong Evidence of Identity, while another Trust Level 2 transaction may only need moderate Evidence of Identity.

Robust authentication is achieved through balanced components and cannot be achieved solely through use of a strong authentication technology.

However, when considering an authentication system it is important that the strength of the components is appropriately balanced. For example, imposing a robust and onerous Evidence of Identity process on a user and then allowing them to authenticate themselves using a low-strength authentication technique reduces the overall security strength of the system.

The diagram below illustrates how the Trust Levels provide an indication of how the Evidence of Identity and Authentication components should be balanced for a robust transaction.



This diagram is for illustrative purposes only and is not intended as a detailed analysis of EOI processes or Authentication techniques.

Applying Trust Levels across different stages of a transaction

Online transactions may be broken down into Trust Levels across various phases of the overall service.

For example: to take advantage of online access, an agency may allow a customer to complete a service application online.

The application can then be formalised inperson at a later stage, thereby taking advantage of the online access and reduced requirement on the user to establish an online identity and maintain a username/password that they may use infrequently.

This approach also allows the online service to be introduced, and at lower cost to the agency, and provides a phased approach that can be added to and developed as expected returns are realised and customer acceptance and expectations increase.

It also takes advantage of the all-of-government approach of separating authentication from authorised access to an online service. The long-term strategic vision for all-of-government is to provide a single robust online authentication service to agencies and the public that they can use to establish their identity online. If this strategic vision is realised, the in-person requirement to achieve Level 3 status could be substituted with the online identity provided as part of the all-of-government approach. This would reduce agency cost and development in this area.

Application of Risk and Trust Levels to this Framework

This section explains how the outcome of an agency's risk assessment and Trust Level analysis can be used to determine how to apply this Framework.

How to interpret the diagram and concepts

To assist in illustrating the concepts the following diagrams use three risk levels of:

- minor;
- moderate; and
- significant.

These are not intended as an indicator of how many levels of risk there are or what they should be. This is for individual agencies to determine and is likely to include more levels of detail or granularity. The three risk levels used are for illustrative purposes only.

Once the risk levels have been determined, individual agencies need to determine the appropriate strength levels required to mitigate each risk, and to decide how it can be achieved within each of the transaction components. This will be influenced by available agency resources, existing infrastructure and long-term agency strategy.

For guidelines on risk mitigation options for each of the components refer to section – **Risk Assessment for online services.**

Guide to the diagrams.

Height of the bar indicates the level of strength required in the component.

Indicates the individual components.

Trust Level 0 – Anonymous

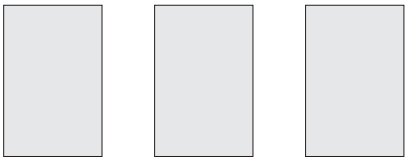
Transactions that do not require the user to be identified or require protection of a user's identity. For example, access to online publications. The only risk would be incorrect information provided in the website.

Trust Level 0 – Anonymous

Online Transaction A
Minor Risk

User access is limited to publicly available information

For example, a user browsing the agency website and downloading information



Trust Level 1 – Pseudonymous

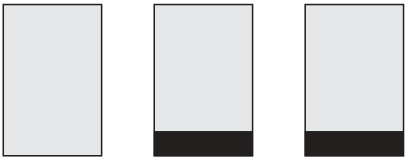
Access is provided for transactions that do not require a person to be uniquely identified but the service agency must be able to respond to the person; e.g. to 'recognise' the person when he/she accesses the service on return visits.

Trust Level 1 – Pseudonymous User

Online Transaction A
Minor Risk

User's authentication level is matched by the minor strength of the Authentication and Transaction components.

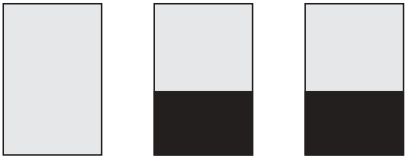
For example - a user partially completes an online application form and is provided with a temporary ID to enter so they can return to the agency site later and complete the application



Online Transaction B
Moderate Risk

A user's access to information is matched by the moderate strength of Authentication and Transaction components.

For example - a user acting in their professional role completes a transaction on behalf of their company



Online Transaction C
Significant Risk

A user's access to information is matched by the significant strength of Authentication and Transaction components.

For example - a user is on a methadone programme with their identity protected but the history of previous treatments is available.

3

Trust Level 2 – Identified User

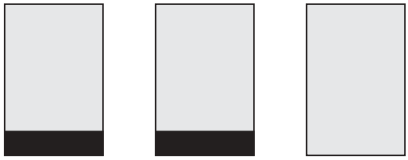
Access is provided for transactions that require that a person be specifically identified. For example, establishing a bank account.

Trust Level 2 – Identified User

Online Transaction A
Minor Risk

User's access to information is limited to the minor strength of the EOI and Authentication components.

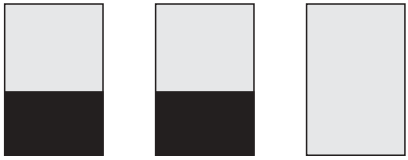
For example - a user providing an email address to be sent information.



Online Transaction B
Moderate Risk

A user's access to information is matched by the moderate strength of the EOI and Authentication components.

For example - a user goes to an agency website and enters their username and password to view their student loan history.



Online Transaction C
Significant Risk

A user's access to information is matched by the significant strength of the EOI and Authentication components.

For example - a user appears in person at an agency and uses their smart card to identify themselves, and change their customer details.

Trust Level 3 – Identified user and verified transaction

Access is provided for transactions that require:

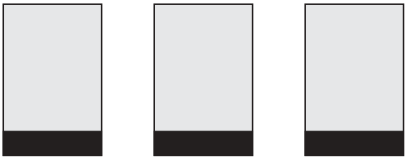
- the person to be specifically identified;
- verification of the integrity of the data exchanged and the exchange itself; and
- the creation of sufficient evidence to indicate that the person agreed to be bound by the transaction e.g. obtaining a passport.

Trust Level 3 – Identified User and Verified Transaction

Online Transaction A
Minor Risk

User's access to information is limited to the minor strength of the EOI, Authentication and Transaction components.

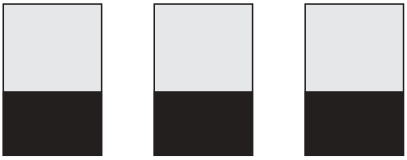
For example - a user completing an application form online and then appearing in person at the agency to receive the service.



Online Transaction B
Moderate Risk

A user's access to information is matched by the moderate strength of the EOI, Authentication and Transaction components.

For example - a user accesses their customer account online and changes their name and address details.



Online Transaction C
Significant Risk

A user's access to information is matched by the significant strength of the EOI, Authentication and Transaction components.

For example - completing a land transfer transaction online.

04 Policy

4

This section provides policy information related to online government services and in particular those requiring authentication. It provides high-level policy guidance on issues related to authentication initiatives. It should be referred to in early planning stages of a project - and also at the end of subsequent stages to ensure a consistent policy approach is being maintained.

Agencies with existing authentication mechanisms should consider these policy issues when looking to enhance or update their current authentication solution.

Policy and Principles Related to Online Authentication

Over the past few years, the E-government Unit (EGU) has been working with a range of public interest groups and agencies to examine what online authentication might mean for New Zealanders dealing with government agencies. The EGU performed an analysis to determine which of the services provided by government agencies in New Zealand require or are likely to require online authentication. The EGU has also looked at overseas examples of online authentication - both for government and commercial services.

For more detail on the Cabinet decision, including the Policy and Implementation Principles, refer to the Online Authentication – **Blueprint: Authentication for E-government.**

In April 2002, Cabinet approved policy and implementation principles (the authentication principles) for online authentication and directed the development of a consistent approach to government authentication [CAB Min (02) 12/2A] refers. The authentication principles require that matters such as personal choice (opt-in) and privacy be given equal weight to considerations such as cost. These are to be referred to, and considered as part of, any government agency authentication initiative.

Comment on interpreting the principles

The principles are divided into policy principles, focusing primarily on the interests of individual users, and implementation principles, focusing on areas to address during design and implementation.

It is important that the principles are read and applied as a whole. Separating out individual principles and attempting to apply them, particularly in the later analysis or design phase of an authentication project, is not recommended and is inconsistent with the policy intent of the principles.

For example, emphasis should not be placed on achieving ‘technology neutrality’ at the expense of the ‘affordability’ principle. Similarly, the ‘technology neutrality’ principle should not be interpreted as a directive precluding the use of any particular package software.

Finally, readers are reminded that online authentication is an aspect of Information Technology that is still maturing. As such, there is the potential that these principles will be subject to further review by Cabinet in the future.

Policy principles for online authentication

Security: Suitable protection must be provided for information owned by both people and the Crown.

Acceptability: Ensuring that the proposed authentication approach is generally acceptable to potential users, taking into account the different needs of people and emerging industry standards, and avoids creating barriers.

Protection of privacy: Ensuring that the proposed authentication approach protects privacy appropriately.

All-of-government approach: Balancing public and agencies' concerns about independence, with the benefits of standardisation, while delivering a cost-effective solution.

Fit for purpose: Avoiding over-engineering, recognising that the levels of authentication required for many government to people [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 for online authentication

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 protect 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.

Privacy

The New Zealand public is particularly sensitive to the protection of individual privacy, and expects government to ensure that individuals' right to privacy will be preserved. This expectation is enshrined in the Privacy Act 1993, which provides the legal framework for privacy in New Zealand.

4

Privacy protection should be a consideration for any system or process that entails the collection, use and/or storage of information about specific individuals. Personal information plays a central role in most authentication solutions, and therefore privacy should be a key factor in determining the most appropriate implementation and operation of authentication solutions.

Privacy Impact Assessment

It is now established practice for a full analysis of initiatives with privacy implications, known as a Privacy Impact Assessment (PIA), to be carried out prior to commencing implementation of the initiative (see *www.privacy.org.nz* for guidance on conducting a PIA). A PIA is an analysis of the potential effects on privacy arising from a particular proposal.

Ideally a PIA should be conducted by someone with experience in the privacy field. A PIA that has been undertaken by an independent assessor and that is published upon completion is seen to be of greater value. In some cases an iterative process to developing the PIA needs to be followed, with an initial assessment carried out during the scoping phase and a subsequent iteration performed as design work is undertaken.

The more complex the authentication solution you are planning (in terms of scope and personal information collected), the greater the likelihood that you will need to have multiple iterations of developing the PIA. Ensure that you have allowed for this in your project planning and budget forecasts.

A PIA results in detailed conclusions regarding Privacy Act compliance and usually ensures the early identification of the need for any empowering legislation. If it is carried out early enough in a project, the PIA will also pinpoint design areas that could potentially be re-worked to be more privacy-friendly.

Compliance with the Privacy Act 1993

It can be expected that the sort of systems and processes required to implement online authentication will give rise to the need to consider the privacy principles and information-matching provisions set out in the Privacy Act 1993.

Non-compliance with the Privacy Act could mean not only customer dissatisfaction and negative media attention but, in more serious cases, it could result in formal legal action being taken against an agency.

Some agencies, such as those in the education, health and justice sectors, should also be aware of the need to comply with specific privacy codes in certain circumstances.

The sections below provide some guidance to areas of an authentication solution that are most likely to require careful review from an experienced privacy officer, consultant or lawyer.

Information Sharing

In many cases the sharing of individuals' personal information between multiple agencies is deemed to be information matching. Enabling legislation is required in order for agencies to legally operate an information-matching programme. The operation of a matching programme must be in accordance with the rules specified in the Privacy Act 1993.

If your authentication solution incorporates a process whereby personal information is 'checked' against another system or database, you should seek expert advice to ascertain whether the process constitutes information matching.

Unique Identifiers

While customer or ID numbers often appear to be the most efficient way to manage customers' information and/or locate the right record for the right individual, there are restrictions in the Privacy Act on the way these numbers (identifiers) can be used.

For example, from a practical point of view the simplest way for multiple agencies to be sure that they are dealing with, or interacting about, the same individual is to have a common unique identifier for that individual. However, Privacy Principle 12 specifies rules about the introduction and/or use of unique identifiers in this manner and, depending on the exact circumstances, this is probably a breach of Principle 12.

Principle 12 also states that you should not use another agency's unique identifier as a customer number or Key in your authentication solution. It might be convenient, but unless you have special approval to share unique identifiers, such as the special codes of practice approved by the Privacy Commissioner for the justice, health and education sectors, you are likely to be breaching the Privacy Act.

Informed Consent

Some of the principles state that an agency is able to operate in a manner that breaches certain aspects of the privacy principles IF the affected individual provides their consent. For example, Privacy Principle 2 stipulates that an agency that collects personal information should collect the information directly from the individual concerned. However, Principle 2 also allows individuals to authorise agencies to collect particular information from a third party.

To date it has been held that any consent of this nature requires choice, and that the choice needs to be genuine in order for the agency to rely on it to achieve Privacy Act compliance. For example, it may not be enough to simply rely on an individual's signature at the bottom of an application form for their consent to collect or use the personal information in a way that breaches the privacy principles. Rather, there may need to be an alternative opportunity for an individual to apply for the service without having to give their consent.

If ensuring genuine, informed consent cannot easily be achieved in the operation of your proposed authentication solution, then you may need to re-work some of your process design, or seek legal advice about the legal frameworks required when a system cannot operate in accordance with the **Privacy Principles.**

If an agency wants to rely on consent or some other privacy principle exemption to achieve compliance with the Privacy Act, then it should first seek expert advice.

Complaints

Individuals who believe that an agency has breached their personal privacy have the right to make a complaint to the Privacy Commissioner. Complaints against government agencies out number the complaints the Privacy Commissioner receives about any other types of agency. Ensuring that you carefully design and implement your authentication solution makes it less likely that it will be the subject of one of these complaints.

Legal

Legal considerations are a key factor in determining how to implement any authentication solution. In particular, consideration needs to be given to the following questions:

- Is the solution robust from a legal perspective, including liability considerations?; and
- Does the approach comply with the relevant law/codes?

Compliance with Relevant Law and Codes

There is a variety of laws and codes that relate to different agencies and sectors, and which may be relevant to the deployment of a specific authentication solution. For example, some agencies have special statutory authority to collect or retain specific information; other agencies can impose specific penalties in cases where an individual falsely provides information. Any specific legislative provisions of this nature may need to be considered in the design of an agency's authentication solution. The Electronic Transaction Act 2002 may also impact on the agency's legislation.

The legislation that applies more generally to agencies and which requires consideration includes:

- the Privacy Act, the Human Rights Act, the archives legislation (Archives Act, Local Government Act and the forthcoming Public Records Act), Fair Trading Act, Consumers Guarantee Act, the Electronic Transactions Act, and the NZ Bill of Rights Act;
- evidence law, such as the Evidence Amendment Act (No 2) 1980 and the draft Evidence Code currently being formulated as legislation by the Ministry of Justice. The new Code is likely to be more facilitative of online authentication and transactions than the current evidence law; and
- crimes legislation, particularly the Crimes Amendment Act introduced in 2003 which includes provision for computer crimes.

Other areas that may need consideration, depending on the nature of any design and development work, include:

- the rules around obtaining ID credential information – for example, the requirement for search warrants or non-party discovery rules;
- legislating for the validity/certainty of online transactions – the sufficiency of digital signatures for the solution – particularly if the solution is to be able to be extended to Government-to-business transactions; and
- very often, non-statutory law such as the laws of contract, evidence, tort (such as negligence) will be relevant.

Legal Robustness/Feasibility

Authentication is required where a party to a transaction needs to have certainty about the identity of the other party. For most agencies, this certainty extends beyond being sure at the time the transaction takes place, to having an audit trail that provides the basis for action in the event that it is subsequently determined that there is something unusual about the transaction.

Allocation of liability if things go wrong can also be important. If, for example, there is a serious system failure or some other problem with the solution that leads to loss, it is important that all parties know who can and cannot be held liable for any wrongdoing, and what the implications of that liability are.

In general, these concerns can be handled either through statute (i.e. legislation defining liabilities and the extent of each type of liability), via existing law such as the law of negligence and/or through contract (such as a contract between the Client and the service agency).

Many existing online services, such as Internet banking, rely on the latter option and ask that individuals accept terms and conditions as part of registering for an online service. The precise nature of the terms and conditions will vary from agency to agency but, if you are relying on a contract, you should consider including the following:

- information about rights, responsibilities and obligations;
- specification of the liability that either party can incur;
- a description of the services that can be accessed using the authentication solution;
- an outline of how the solution works, in terms of equipment that the user requires;
- any charging information;
- advice regarding dispute procedures;
- any specific privacy matters that are relevant;
- an explanation of cancellation or suspension processes; and
- full contact information for your agency.

If you are relying on contract to ensure the legal certainty of your solution you should seek advice from your legal department before developing terms and conditions. In these cases it is also important to ensure that you have implemented procedures to ensure that a record of the acceptance of terms and conditions is maintained in all cases.

An important aspect is to make sure that the way in which the contract is agreed to by the individual is sufficiently robust for evidential purposes. For example, while it is desirable from a practical perspective to have a contract agreed by a simple on-line “click-accept”, that may not be sufficient for legal purposes.

The Ministry of Economic Development has guidelines available which will assist agencies in implementing solutions based on the Electronic Transactions Act.

In some cases an agency may need either to enact some new legislation or to amend existing legislation in order to lawfully operate its authentication solution. For example, a service provided by an agency may specify particular procedures for verifying identity in its enabling legislation. This does not apply to most agencies, but again you should seek advice from your legal department to be sure. They can also check whether the Electronic Transactions Act 2002 automatically extends the agency’s restrictive legislation to enable an online solution.

Authentication of Guardians and Trustees

Many individuals, for a raft of different reasons, have another person undertake transactions with government agencies on their behalf.

For example:

- an individual living overseas may nominate an agent to manage their affairs;
- guardians often transact on behalf of their children; and
- on occasion, power of attorney is exercised for individuals who are unable to act for themselves.

Where there is a level of demand, an agency delivering online authenticated services will need to consider allowing guardians and trustees access to the online service. Care needs to be taken in implementing processes for authenticating a guardian or trustee. Establishing the relationship between an individual and their guardian or trustee should always be completed carefully, and consideration be given to doing this offline.

Similar care needs to be taken to ensure that there is a gatekeeping process before removing a guardian or trustee's access privileges, but equally to ensure that access is removed quickly in cases where the agency is satisfied that the guardianship/trustee relationship no longer exists.

Notes:

05 Implimenting Authentication

5

This section describes and provides guidelines for implementing online authentication solutions. It provides detailed information on implementation options for the concepts covered in the earlier sections of this document and focuses on positioning towards an all-of-government approach.

Readers are reminded that any implementation should be undertaken using sound project management methodologies and with appropriate project audit in place.

Authentication Technologies

In spite of the many advances in computer hardware, software and encryption there are relatively few techniques available to authenticate an individual. We can generally class the techniques as members of one of three groups:

- Secret – Something you know;
- Biometric – Something you are; and
- Token – Something you have.

Each of these groups has subgroups as well.

Refer to **Authentication Scorecard - RSA Security** and **Authentication Reference Guide - Secure Computing'*** for further information about authentication technologies from an industry perspective. **These references are only included to provide readers with additional information related to authentication, and are not intended as Standards, Compliance or Best Practice Framework initiatives.*

Secret

The oldest and most pervasive authentication technique is the Shared Secret. An entity proves its identity to an authenticating party by demonstrating that they and that party both know a common or shared secret.

Secret Type I (Shared Secret): Secret Type I authentication requires two parties to share a common secret. The authentication is performed by the party wishing to be authenticated sending a secret to the authenticating party. The authenticating party checks that the secret is the same as the secret registered for that party and grants or denies authentication accordingly.

Refer to **Usernames and Passwords** section for specific discussion about this type of Shared Secret authentication technology

This type of authentication is distinguished by the fact that both parties must know the shared secret before authentication can be performed (although it is often modified using a one-way transformation before storage by the authenticating party).

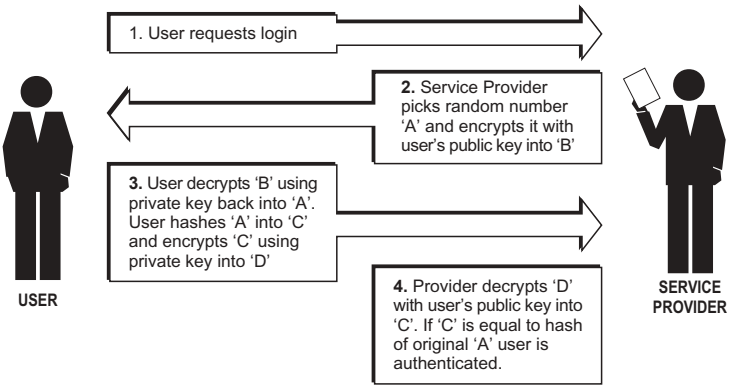
Usernames and passwords are the most common form of Type I shared secrets and by far the most common form of authentication used on computer systems today.

The greatest flaw of this type of authentication lies in the fact that the first entity must communicate or transmit the shared secret and therefore lose control of it. The secret may be susceptible to interception during transmission, by suborning the authentication party or by another party masquerading as the authenticating party.

Secret Type II: Type II secret authentication requires the first party, the party wishing to be authenticated, to have a secret. The second authenticating party does not have the secret, but has other information

that is mathematically related to the first party's secret. This related information does not disclose anything about the original secret, but does allow someone to prove if the secret has been used.

The common example of Type II Secret Authentication employs Public Key cryptography.



Biometric

Like all systems the authenticity of the biometric is reliant upon certain controls being in place, e.g. physical security over the facial recognition camera system and personnel security relating to its maintenance staff.

Biometric authentication uses the physical characteristics of an individual to prove their identity. Like secret authentication, there are two general classes of biometric authentication.

Biometric Type 1: This type of authentication includes voice and handwriting recognition. The feature that distinguishes Type I Biometrics is that the physical characteristic being measured can easily change; for instance a person's voice may change significantly due to health conditions or emotional state.

Biometric Type 2: This authentication technique uses those physical characteristics of a person that do not **generally** change. Type II techniques include fingerprint or face recognition, iris and retina scanning and hand geometry measurement.

Token Authentication

Brute Force Attack – a technique used by Internet hackers to attempt access to a protected system. This attack requires trying all (or a large fraction of all) possible values till the right value is found; also called an exhaustive search.

This is where an individual must present a physical token to prove their identity. Passports, drivers' licences and credit cards are typical tokens used with this type of authentication. Tokens generally incorporate some anti-counterfeiting features such as watermarks or other features that are difficult to reproduce. Note that not all types of tokens are useful in electronic authentication systems.

Portable electronic devices including USB flash drives, smart-cards, or PCMCIA cards are considered to be authentication tokens. In fact, these devices are really just storage devices used for Secret Authentication (typically Secret Type II). The advantage of these devices is that they

typically provide relatively secure storage for the secret and, resistance against brute force attacks. Some token devices also incorporate a digital signature as an anti-counterfeiting feature.

Another type of token is the time-based authentication token for one-time reply to a computer, generated one-time challenge, the token being protected by a PIN and allocated to a specific user for additional security.

Usernames and Passwords

Usernames and passwords are the most common technique used for authentication in online transactions, and require a closer examination.

The technique has both good and bad features:

Good features include:

- most people understand and are comfortable with usernames and passwords;
- it is very simple; and
- it requires no special hardware or software on the client system.

Less desirable features include:

- browser password managers can save usernames and passwords on a person's computer;
- people often mismanage passwords; and
- username and password systems can be subject to simple brute force attacks or simple guessing.

The username/password scheme relies on randomness of both username and password to make it difficult to guess the correct combination of characters to authenticate as a specific individual. This randomness is usually measured as entropy. Currently, 128 bits of entropy is considered 'cryptographically adequate' for securing information.*

Note that the current Windows password is stored in 7-character lots. Thus an 8-character password is broken into a 7-character and 1-character password in the password file. Brute force breaking of a single character is very simple, thus the veracity of 8 or 9-character passwords over 7-character is suspect.

Most common username password systems use a derivation of an individual's name as the username. The algorithm for generating usernames from names is generally trivial and provides at most a few bits of entropy. This leaves the password as the only significant test for authentication. The question is "how good is that test"?

There are approximately one and a half million English words. This gives about 19 bits of entropy in the entire language; using words 8 characters or less will have probably no more than 15 bits of entropy.

Entropy - Randomness or lack of organisation in a situation. A totally entropic situation is unpredictable.

A random 8-character string (letters only, single case) has about 40 bits of entropy. A random 8-character string of mixed case, numbers and special characters will provide at most 56 bits of entropy.

Only if you have a completely random username and password, each with 9 characters, will you come close to having 128 bits of entropy. Username and password requirements like these are unlikely to survive 'sociability testing' in ordinary user groups. For example: reducing the opportunity for

**(Ref: Arjen K. Lenstra and Eric R. Verheul. Selecting Cryptographic Key Sizes. J Cryptology, Aug 2001 [p 37, 217].)*

individuals to guess another person's password or to break the encryption code based on knowledge of that person.

Mitigating low quality passwords: The use of lower quality passwords can be acceptable in authentication systems that incorporate features to prevent brute force attacks.

By allowing only a small number of failed login attempts, even short, low entropy passwords are difficult to guess and may provide suitable authentication assurance.

One time password schemes: The term "One time password" refers to a number of systems that use a system of changing passwords at every transaction, to prevent passwords from being stolen. The most common of these systems uses a password-generating device (a token), which displays a string of letters or numbers that change frequently. The system, which is actually a variation of Secret Type II, uses a secret mathematically combined with the current time to generate the current password. The password-generating token typically resembles a key fob, but can also be implemented in software to run on a computer or handheld PDA.

Writing down passwords: One practice that is broadly discouraged is writing down passwords. However the idea deserves more consideration than it is generally given.

The reason the practice is discouraged is because of the threat that the written passwords will be discovered by a malicious person who will then be able to falsely authenticate himself or herself as the owner of the password.

This is a threat, but it ignores the fact that almost all adults are adept at managing pieces of paper in a secure manner. Most people have spent their lives knowing how to store valuable paper (currency) in a secure manner (in their purse or wallet).

If users can be taught to treat a written password in the same way they would treat a $100 note, the risk of losing passwords in this manner would probably be reduced to an acceptable level.

People can also easily learn to write passwords in a secure manner inside, for instance, a diary full of people's addresses. A relatively high-quality eight-character password such as "Jnh4senZ" could be written as a name and address like:

John Smith 14 Albatross Grove Wellington, NZ

In a similar fashion, existing names in a diary could be used to generate high-quality passwords that could be easily referenced by a user. These methods all have a very low risk of being compromised.

Username/Password Policy

Refer to the **Advisory Roles** section for information about GCSB's role.

The Government Communications Security Bureau (GCSB) offers guidance in their publication "New Zealand Security of Information Technology Publication 204 - Authentication Services And Mechanisms".

This publication contains detailed information on password formats, including lengths and acceptable characters.

User education related to passwords

In any username/password authentication system, the security and integrity of the system relies on the actions of the user. For this reason it is important to establish well-defined and promoted user education programmes. These should include educating the user about the following points:

- Don't use easy-to-guess passwords or the same password for multiple accounts.
- Create passwords that combine alpha, numeric and special characters (such as *) — which makes them harder to guess or crack — and change them frequently.
- Do not save passwords on your system, where they can be copied. Instead, key them in every time you log in.
- Passwords should not be shared with any other person. Persons known to the user are the most likely to commit identity fraud.
- If you have to record your password somewhere, ensure it is stored in a secure place and following the guidelines in the previous section 'Writing down passwords'.
- Never give out your password to any party that has initiated a call or email to you. For example, fraudulent emails or phone calls from persons claiming to be from your bank and asking for your PIN number.
- Periodically check your account information and check when the account was last accessed. Investigate any transactions that appear suspicious or unfamiliar.
- If you suspect someone has compromised your password, contact the agency as soon as possible. This will allow for use of your account to be suspended until the suspicion is confirmed.
- If possible, install virus protection software on any computer that you use to enter your password or access your account.
- Before conducting any transaction online, ensure you understand what privacy and security protection the vendor has put in place. This includes encryption of passwords across public networks (the Internet) and whether or not the other party is retaining your password.
- Ensure users terminate any active sessions when they are finished, or require them to use an appropriate security mechanism, for example a password-protected screensaver.

Digital Certificates

The use of Digital Certificates and Public Key Infrastructure [PKI] is an example of a Secret Type II authentication. Public Key cryptography employs the mathematical relationship between two very large prime numbers to provide a mechanism where one number transforms a block of data (a secret) in such a way that the other number must be used to transform it back into its original form. The first number, called the private

For information on Secret Type II authentication, refer to section **Authentication Technologies - Secret**

key, is kept secret by its owner. The second number, the public key, can be freely distributed to anyone you wish to share secrets with.

PKI refers to the use of public and private keys, together with infrastructure, to create, verify and revoke keys in a distributed environment. This may include a 3rd party service provider of a registration process and agreed contractual service performance requirements.

Some PKI implementations also use a physical container for the private key such as a Smart Card, a flash memory device or devices that communicate using Radio Frequency (RF) or Infra Red (IR). These containers typically provide protection for the private keys stored inside by requiring a password or PIN to access the keys. Smart Cards protect the key further by making it unreadable; it can only be used to perform cryptographic operations on the card itself.

A digital certificate comprises the public key, and information identifying the holder of the corresponding private key, all of which is digitally signed by a trusted certificate issuer called a Certification Authority [CA], for example Verisign or Thawte.

The private key can also be stored on a person's computer, typically using encryption based on a password to reduce the risk of theft.

A private key approach provides secure authentication (and other cryptographic functions) by virtue of having a large secret, typically 1024 bits in today's applications. Guessing this secret using brute force systems is considered impractical using commercially available computers.

Digital Certificates and the use of private and public keys are well supported by common browsers, web servers, application servers and LDAP servers.

However, a private key approach is not without it's faults. In particular, the task of managing a large number of private and public keys is time consuming and expensive. The infrastructure required to securely create, distribute and manage keys for individuals (and computers) is particularly expensive to establish and operate. Strict procedural enforcement, physical security and detailed auditing are required.

There is another very large problem related to the management of private keys. Unless the private key is stored in a physical container that provides strong security, such as a Smart Card, it can be subject to theft. Even if the private key is encrypted using a password, it is susceptible to relatively simple brute force dictionary attacks. Even worse, it is easy (and tempting) for a user to store a private key on their computer without protecting it with a password. It would be relatively simple for another person to walk up to their computer and authenticate themselves using this type of unprotected Key.

Using secure private key containers like a smart card is an expensive proposition. Each user would require a smart card (costing from approximately $10-$30) and would also need a device attached to their computer to read the card. Costs of smart card readers start at approximately $50. The cost of such an implementation across the general public would be significant.

Many users also have a variety of conceptual problems when attempting to use a certificate approach to authentication. These problems include the failure to understand the difference between their login password and the password to access their private key, and confusion resulting from having multiple private keys installed on their computer.

So, when should Digital Certificates be used or avoided?

Avoid Digital Certificates if:

- your users may not be sophisticated in their understanding of computers; or
- you have a group of users without a support infrastructure; or
- you support a very large group of users.

Consider Digital Certificates if:

- you have a requirement for strong authentication (where you are protecting valuable resources); or
- your users are authenticating from computers that are configuration managed; or
- you already have a key management and help desk infrastructure.

Refer to section **Implementing Non-Repudiation** for discussion about strong authentication and the need to ensure that robust technologies are supported by appropriate processes.

Multi-Factor Authentication

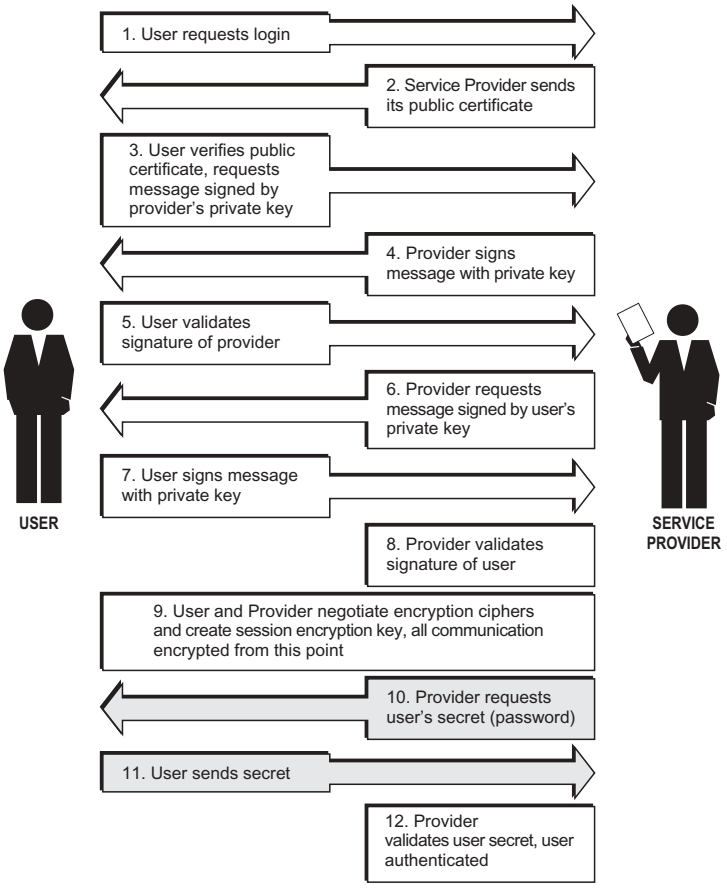
When authentication is used to protect more valuable resources, a single authentication technique may not be sufficient. In these cases it is common to use two-factor authentication. Most two-factor authentication schemes employ two different techniques, one of them usually Secret Type I.

When considering multi-factor authentication and increased security, selecting a method from each of the categories to form your multiple factors is recommended. For example, combining the selection of a password (something you know) and notification via cell phone (something you have).

Multi-factor authentication may also allow agencies to provide a single strength or method of authentication for the majority of their Clients. When a minority of the overall user group require more sensitive or valuable transactions, these Clients are re-authenticated using a stronger authentication method. This would allow agencies to provide simpler and cheaper authentication methods to the majority of their Clients, and to provide more complicated, and possibly more expensive, methods only as and when required.

Several products support the use of three or more factors for circumstances where the need for very high authentication is required.

A Simplified Example of Multi-Factor Authentication, Secret Type I and Public key, using SSL



Supporting Infrastructure

As important to the actual authentication technique is the supporting infrastructure that facilitates the registration and storage of authenticating information and the actual authentication exchanges.

Directories: The most common way to store authentication information today is in a directory. Directories using the Lightweight Directory Access Protocol [LDAP] are the most common type and provide fast, hierarchical retrieval of user authentication information. LDAP directories have fine-grain access control capabilities to protect information. They can also reference information in different directories – aiding integration. Most directory products are highly scalable and support replication allowing high availability solutions.

Directory servers can also act as the actual authenticating agent. Most can directly authenticate an individual using either username/password or a digital certificate.

SSL: Secure Sockets Layer, and also Transport Layer Security – (TLS), provides a secure transport mechanism for exchanging authentication information. It protects information in transit using encryption as well as identifying both parties in the communication. Most Web Servers and Directories natively support SSL communications.

Identity Management Systems [IMS]: Many vendors provide solution packages that combine the features of a Directory Server with software (typically a web-based application) to facilitate the provisioning of individuals in an authentication system. The principal features of these products are to provide support for self-registration of users (note the lack of EOI), and support for automatically dealing with lost passwords (note lack of evidence).

Identity Management Systems typically need strong supporting processes and possibly customisation to meet the requirements of New Zealand Government agencies.

Note that the security of the Identity Management System needs to be on a par with the overall security requirements of the resources you are protecting.

Access Control Systems: A system that provides control, to varying degrees of granularity, over the resources that an individual can access, is called an Access Control System. There are a number of Access Control products that specifically support websites and online applications. Most of these products either include an authentication system or depend on an LDAP directory to perform authentication.

Data Formats

Data format is an important consideration in any information system.

Authentication relies upon the establishment of Evidence of Identity and the verification of related identity attributes. The schema for storing and exchanging these attributes requires particular consideration given the potential for this data to be used across agency boundaries. In particular, the move towards achieving the goals of the E-government Strategy includes an increased likelihood of name and address data being relied upon across government agencies.

For this reason, readers are referred to the 'xNAL Guidelines'. xNAL is a structured XML language for representing names and addresses.

The xNAL Guidelines were written for the NZ e-Government XML Name and Address Working Group and maintained as part of the e-GIF.

Agencies should also give serious consideration to ensuring that the character set used in their system is appropriate to meet their business needs. For example, the use of Unicode may assist agencies in accurately recording Client name data in particular ethnic scripts, macrons and accents.

The *xNAL Guidelines* are available from the **E-government Website.** Information about e-GIF can also be found at this website.

Notes:

06 Implementation Considerations

6

This section contains important considerations related to implementing authentication solutions. It includes considerations related to an all-of-government approach to establishing Evidence of Identity and to online authentication, and contains advice regarding the selection of products and services.

Evidence of Identity Framework

The Evidence of Identity [EOI] Framework is currently being developed to provide a best practice guide for establishing the identity of individuals who wish to transact with government agencies. When the EOI Framework is finalised it will provide a standard for agencies to follow in establishing EOI, and is therefore directly relevant to any agency implementing an authentication solution.

The Framework has been developed because:

- Agencies currently take different approaches to EOI. This causes confusion for individuals who are asked for different combinations of EOI by different agencies. Consistency of processes, based on the level of risk associated with particular types of transactions, is needed to avoid this confusion.
- A robust and consistent approach to EOI across government will assist in protecting individuals against theft or fraudulent use of their identities, and against personal or public loss of money through identity fraud.
- The E-Government Unit has recently been working on the issue of online authentication of identity. A robust framework for verification of identity is a critical component of any authentication process in the online environment.
- Identity fraud is a growing problem and implementation of a consistent approach to EOI is likely to have a positive effect on identity fraud. Overseas figures show a significant increase in the number of identity fraud victims in recent years.

The EOI Framework is currently at final draft/consultation stage and, when finalised, will be made available in full for agencies to adopt.

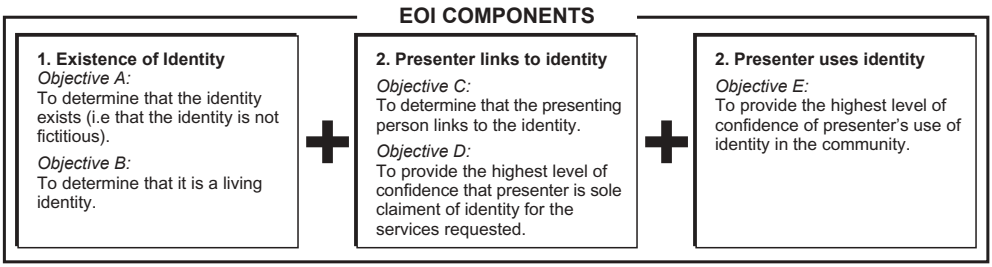
Extracted from the Draft Evidence of Identity Framework – December 2003 Version 0.6

The draft EOI Framework consists of four elements:

- the specification of the components necessary to establish identity to a sufficient level of confidence, and the objectives that must be met to achieve these components;
- the principles underpinning both the development of the EOI Framework and the subsequent application of it by agencies;
- the processes required to meet the EOI objectives outlined in the Framework; and
- business rules for using the Framework.

The draft EOI Framework was developed by a cross-agency working party made up of representatives from the Department of Internal Affairs, E-government Unit, Ministry of Social Development, Land Transport Safety Authority, New Zealand Immigration Service, Inland Revenue Department, NZ Police, Ministry of Education, Accident Compensation Corporation, Electoral Office, Ministry of Fisheries and the Combined Law Agency Group.

The Framework outlines a number of objectives that, if met, provide confidence in the identity of individuals. It is essential that all of the objectives, shown in the diagram below, are met, as each relates to a different aspect of identity.



EOI Components. (extracted from the draft 'Evidence of Identity Framework' by the Cross Agency Evidence of Identity Project on 10 September 2003)

Using the Framework

This section is based on the **Draft Evidence of Identity Framework – December 2003 Version 0.6.** When finalised, the EOI Framework will be available for agencies to use.

Given that there are varying levels of risk involved in government transactions, the level of confidence required to establish an individual's identity, depending on the transaction being undertaken, varies. Individual agencies are responsible for determining what risk level is applicable to the services/transactions they deliver. To do this agencies must first assess the transaction against the following categories to determine the relevant level of confidence:

The categories in the draft EOI Framework are aligned with the Trust Levels set out in section **Trust Levels** of this Framework.

Category Zero – Anonymous Service/Transaction, which does not require the individual to be identified;

Category One – Pseudonymous Service/Transaction, which does not require the individual to be identified, but does mean the agency requires some contact details for the individual (such as physical address or email address);

Category Two – Identified Service/Transaction, which requires the individual to be specifically identified;

Category Three – Verified Service/Transaction, which requires the individual to be specifically identified AND the identification data for that person to be verified.

The draft EOI Framework then sets out the concept of two different confidence-level processes for EOI:

1. **Confidence Level A**

   Should be followed for transactions requiring individuals to be identified.

2. **Confidence Level B**

   Should be followed for transactions of greater risk, where greater verification of an individual's identity is required.

It is expected that agencies will apply Confidence Level A for Category Two transactions and Confidence Level B for Category Three transactions.

For example:

Objective A – To determine that the identity exists can be established to Confidence Level A by sighting a full birth record, or a Passport or Firearms Licence. A higher Confidence Level B can be established by the agency gaining consent from the individual to request verification from the custodian

of the primary data, or by sighting the document and verifying the document is genuine.

The draft EOI Framework provides guidance on how each of the five objectives can be met to the required Confidence Level.

Separation of Authentication and Authorisation

The EGU Authentication Project has drawn a clear distinction between Authentication and Authorisation. While some people are quick to observe the close relationship between the two, the strategic vision for e-government in New Zealand means that care should be taken not to integrate them.

The section below sets out other reasons for separating authentication and provides advice about achieving that separation.

The June 2003 Cabinet directive relating to online authentication formalised the need for authentication and authorisation to be separated. See the **e-government website** for a summary of this directive.

Reasons for separating Authentication, Authorisation and Access Control

In addition to strategic drivers, there are four practical reasons for keeping Authentication, Authorisation and Access Control separate.

Modularity: One of the most important reasons to separate Authentication from Authorisation and Access Control is to promote modular system design.

Modularity means that something is designed and constructed in a manner to allow flexibility and variety in its use.

There are many benefits to using an Authentication/Authorisation/Access Control system that is modular. The first and most obvious advantage is future compatibility with an all-of-government authentication system. Other benefits include:

- easier integration with existing application authorisation and access control systems;
- simpler system troubleshooting and maintenance;
- more options for performance upgrades; and
- it makes system changes easier as requirements change.

Cost: By separating authentication from authorisation and access control, there will be more flexibility to use the authentication directory, without having to duplicate your entire infrastructure.

Scalability, performance, availability: The authentication system is often the keystone of a larger access control system. It is often the performance-limiting element of that system as well. By separating the authentication from authorisation and access control, system designers have more flexibility to implement this portion in a more robust manner to provide performance and high availability.

An integrated Authentication, Authorisation and Access Control system will typically be more expensive to scale to the same degree (due to licence and hardware costs). The Authorisation and Access Control elements do not always support distributed or replicated operation as well as the Authentication portion.

Effort: Keeping the Authentication system mitigates the level of effort that the agency will need to expend in the future to switch to the use of the all-of-government authentication solution.

Keeping Authentication Separate in Practice

This section explains how the proposition that authentication be kept separate from authorisation and access control can be applied.

Product Selection: The first and best way to keep the authentication system modular is through careful product selection:

- Don't purchase features not needed. Most common web and application servers provide native authorisation and access control features. Use these rather than buying a product with rich authorisation features.
- Don't purchase inflexible products. Select only products that allow flexible and modular use of your directory or system.

Lazy Implementation: Even if an integrated authentication/authorisation system is purchased, not all features may be required. Implement only the features that are currently required rather than creating a complex and comprehensive infrastructure that revolves around your current tools.

Application Writing: When developing online applications, agencies can ease a later transition to a separate authentication system through intelligent software architecture. The most important feature required is modularity. Ensure that portions of the software that deal with authentication, authorisation and access control are logically detached from each other. This could be assisted by providing programmers with standard API's that carry out the authentication and authorisation functions.

Also, see the section **Guide for selecting Authentication Products and Services** that looks at product selection more closely.

This allows simpler modification in the future, if required.

Avoid modelling software elements on features of the authentication or authorisation systems. Rather, base software on business processes and objects, and use isolated software elements to interface to your authentication infrastructure.

System Design: The overall system design should reflect a modular approach. The desired long-term objective is to have adequate separation between the authentication and authorisation elements. This objective should be considered when designing directory structures of database schemas, and a separation of different types of data implemented (for example, identity data could be separated from access data).

An alternative would be the inclusion of a tiered architecture or layer above the directory or database that would implement the separation process or logic for relying applications. Specific implementation would depend on existing or developed infrastructure agency resources and requirements.

There are a number of pitfalls to avoid when designing your system:

- avoid monolithic products that keep authorisation and authentication data closely coupled;
- avoid writing code that performs authentication or authorisation. Ensure your developers have experience and understand the risks involved; and

- Agencies should remember to ensure that the user ID scheme in their authentication solution is sophisticated enough to allow for the future use of user ID's across other agencies/services.
- Provide application programmers with APIs/services/modules that carry out authentication and authorisation, this separation and modularity will simplify integration to authentication sources/services external to the agency.

Guide for Selecting Authentication Products and Services

This section provides guidance about selecting product sets that will fulfil your current access control requirements, but not prevent migration to an all-of-government authentication system in the future.

System Selection

The following criteria can be used to evaluate authentication and access control products.

Functional Requirements for Forward Compatibility

- Any product selected today for authentication or access control should work with any LDAP v3 directory, or at least be certified to work with the market-leading directories.
- The system must be configurable to resist brute force attacks by limiting the number of failed authentications.
- The system should provide considerable flexibility in how it can map on to directory hierarchies and user schemas. The system should not force the use of a particular schema. It should map on to any directory containing a minimum of user information.
- User identity and user authorisation information must be logically separate. They must be able to reside in different directories.
- An Application Programming Interface [API] may be required to facilitate future integration with a foreign directory system.

Standards

- Lightweight Directory Access Protocol [LDAP] v3 is the current standard for directories to hold user authentication information.
- Security Assertion Mark-up Language [SAML] defines a standard for communicating information about authentication, authorisation and access control.
- SSL v3 is the current specification for the Secure Sockets Layer. Closely related is the Transport Layer Security v1 standard, derived from SSL v3.

Implementation Tips

The following tips are suggestions that agencies may wish to adopt to 'future proof' their authentication solutions:

- Keep a minimum amount of information in your LDAP 'person' entity. If additional information is required consider (for user management, access control, etc.) using a different LDAP directory tree.

These points are presented as guidance for agencies and are NOT mandatory standards

- Don't misuse fields in a standard LDAP structure; it is better to extend the schema.
- Plan ahead with user names. Recognise that, if you migrate to all-of-government authentication, you may have user id clashes. These can be minimised by salting user ID's with organisational information.
- Don't co-locate authentication and authorisation or access control information.

Security

Security is an important part of an Authentication infrastructure. While we talk about ensuring that only the correct individual can be authenticated for online access, the protection of the online resources and the authentication system itself are equally important.

In this section we look at four different areas of security concern: Operational Security; Infrastructure Security; Application Security; and Governance.

For further information on Risk Management, refer to section – **Risk Assessment for Authenticated Online Services.**

N.B. This section provides only an overview of security related to Authentication Systems. The actual security requirements for any given implementation must be assessed and managed through a comprehensive Risk Management process. This section simply provides background information on areas of security that are commonly addressed in a Risk Management plan.

Operational

There are many aspects to Operational security that need to be addressed. They include user support, intrusion detection and prevention, system access and procedural support.

User Support: Any system that supports a large number of users will meet some common challenges. The most common is lost or forgotten passwords. An agency must ensure that the processes surrounding the issuing, re-issuing and resetting of passwords all meet the same EOI criteria and resist 'social engineering'.

It is good practice to ensure that periodic quality assurance and audit reviews take place when the system has been operationalised.

Help desk procedures must be designed so as to ensure that a malicious individual could not discover information about another legitimate user. These procedures should be frequently reviewed and audited for compliance.

Intrusion Detection and Prevention: Like any high-value information asset, an authentication/access control system will require active measures to detect and repel malicious attacks. An intrusion detection and prevention system should be configured in anticipation of attempts to steal or insert user identities, to falsely authenticate an individual, or to deny services.

System Access: Access to authentication/authorisation systems and information must be controlled like any high-value business asset. This includes access to the physical systems, management consoles and system backups.

Procedural Support: High-value transactions that occur online should require complementary procedures to provide validation. For instance,

transactions exceeding a certain limit might require an alternate form of confirmation, such as a telephone call.

At a minimum, users should receive feedback about online transactions using alternate means such as a posted confirmation. This provides a means for fraudulent activity to be detected.

Infrastructure

The security structure component of an online system must be incorporated into the design of the online environment and supporting infrastructure, rather than be added like a new feature.

Design features in an online infrastructure include segregated Demilitarised Zones [DMZ] for isolating different functions and information, firewalls, intrusion detection/prevention systems, disaster preparation and consolidation, and analysis of logging information.

Any online infrastructure should be subject to regular vulnerability assessment and be an actively managed component in a security management framework.

Application

Good quality application security can be one of the more difficult goals to achieve. Applications are subject to a variety of attacks; SQL injection, URL bypassing, hidden field manipulations, and various encoding attacks, are just a sample. Most business application programmers do not have the training or experience to write bullet-proof web applications.

SQL injection is the name for a general class of attacks that can allow nefarious users to retrieve data, alter server settings, or even take over your server if you're not careful. SQL injection is not a SQL Server problem, but a problem with improperly written applications.

Consider adopting one of the following three steps to mitigate this threat:

1. Do not attempt to write authentication or access control software. Rely on the features of a third party authentication and access control system for this functionality. These products generally have been subject to intense security scrutiny and review, and provide fine-grained access control to static resources.

Organise your application in a hierarchical fashion to ensure that portions that include user forms or that do database transactions can only be reached with prior user authentication.

2. Use stateful error handling. This can be used to detect and thwart repeated attempts to penetrate application security.

3. Have a qualified third party analyse and security test your application software on a regular basis.

Governance

The growing importance of information systems to organisations, and the risks arising from this increased dependency, make appropriate and effective information privacy and security governance a significant aspect of overall governance.

For example, the Ministry of Health and ACC ‘Health Information Management Code of Practice’, notes that governance should focus on strategic alignment, leadership and the structures that ensure appropriate

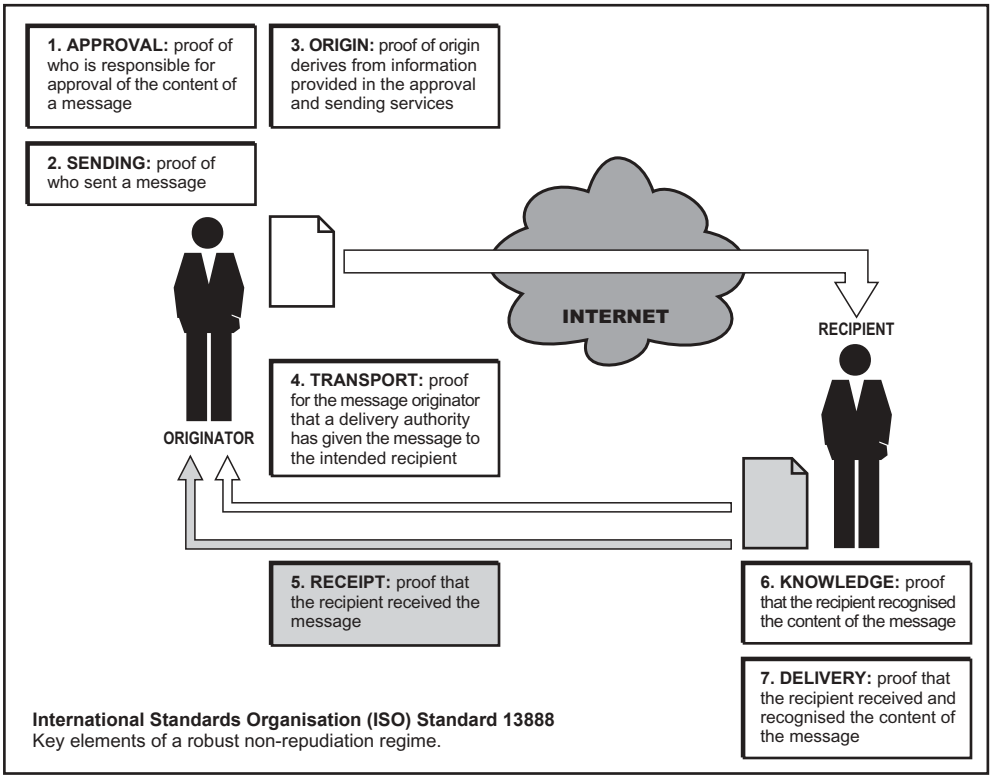
standards, policies and procedures are developed, adopted, implemented and maintained.

For some solutions, governance could be provided through a formal governance committee. While for smaller, less mission-critical systems, governance could appropriately be provided by line management.

Implementing Non-Repudiation

This section provides guidance and considerations around implementing non-repudiative applications. It is based on the objectives of non-repudiation and is technology neutral. How the properties are implemented is up to the agency, based on their specific requirements such as those listed in the Non-Repudiation section of this document, and is provided as concepts to be included in any intended design.

The following diagram, based on the International Standards Organisation (ISO) Standard 13888, outlines the key elements of a robust non-repudiation regime. Any design needs to consider each of the individual elements and how they will be implemented and combined to achieve a robust non-repudiation application.



International Standards Organisation (ISO) Standard 13888
Key elements of a robust non-repudiation regime.

Properties of Non-Repudiation

The following properties (based on the report "Non-repudiation in Practise" - http://dsns.csie.nctu.edu.tw/iwap/proceedings/proceedings/sessionD/6.pdf.) can be derived and must be satisfied to support non-repudiation for online transactions. The first two properties would support non-repudiation of submission, while the last two properties could achieve non-repudiation of receipt.

1. Transactions and customers must be tightly bound. Each transaction must be bound to a Client via an acceptable authentication mechanism and the Client must be authenticated prior to the agency actioning the transaction request. The authentication mechanism should be strong enough to uniquely hold the Client accountable for initiating the transactions as a result of authentication.

2. Transactions must be difficult to forge. Additional security measures and mechanisms should be tightly coupled with the authentication mechanism to prevent transactions from being forged.

3. Transactions must be unalterable. After a transaction is initiated, its contents (including user ID, date and time, and transaction details) cannot be altered without detection while in transit to maintain transaction integrity and allow future verifications if and whenever necessary. It must ensure that the transaction is unaltered and logged after it is committed and confirmed.

4. Transactions must be verifiable. Logs must be archived and properly protected to prevent unauthorised alteration. Whenever there is a repudiation dispute, transaction logs, along with other logs or data, can be retrieved to verify the initiator, date and time, transaction history, and so on.

Relevance to Agencies

Because of the complexities surrounding non-repudiation, it is important for agencies to accurately determine their requirements, in particular any risk mitigation measures. In the majority of situations, non-repudiation is directly related to risk management and the consequences to an agency if a client repudiates a transaction.

Some issues to consider:

- do the advantages and costs related to providing a service that requires non-repudiation online, compare positively to the cost of implementing a totally non-repudiative solution? Do the benefits outweigh the costs?
- is the cost of implementing a non-repudiation solution less than the consequences of a client repudiating a transaction? Does the risk warrant the costs of implementation?
- implications for client privacy, ease of use and compliance with legislative and other legal requirements should also be considerations in determining a solution;
- the ideal for an electronic transaction is to achieve a high-level of non-repudiation. The reality is that, as with any form of offline contract, achieving 100% non-repudiation without the risk of failed litigation and prohibitive costs may not be possible. However, particularly for

transactions where the ability to sue or prosecute is important, non-repudiation is an important consideration;

- achieving a high level of non-repudiation requires not only technical considerations, but also policy, legal and human resource capabilities that can hold up to external scrutiny, possibly by a judicial authority. Non-repudiation is achieved through a combination of robust technical and policy processes;
- achieving non-repudiation for electronic transactions may not require a totally technical solution. Consideration should be given to parts of the process that can safely be completed online, and then completion offline when required. For example, requiring the client to appear in person to complete and sign the application after completing any pre-requisite requirements; and
- there is a requirement that each of the properties or parts of a transaction requiring non-repudiation should be balanced. For example, the electronic or technical parts of the transaction should not be stronger than the manual parts, and vice versa. The degree of non-repudiation a transaction achieves will be dependent on its weakest part or property.

Because of the issues listed above, there is no single solution to satisfy all agencies. Apparent risks, costs, available resources, existing and planned infrastructure, and transaction requirements may, all differ between agencies. Agencies need to determine their own requirements for non-repudiation and balance these against the drivers for providing services online.

Public Key Infrastructure [PKI] for non-repudiation

For further information related to PKI implementations refer to publication: *Secure Electronic Environment (S.E.E) - Paper 14 International and New Zealand PKI Experience Accross Government*, available from the **e-government website.**

Public Key Infrastructure is a common solution for implementing systems requiring non-repudiation. When PKI was initially introduced it was promoted as the solution to authenticating parties to a transaction over the Internet, and was said to offer robust non-repudiation. Subsequent implementations of PKI infrastructure internationally have had mixed results. The common characteristics of successful implementations are: *(Based on the report – Australian Security Forum – Position Statement on PKI of the Australian Security Industry, November 2003)*

- parties to the transaction tend to deal with one another in a well-defined context. The use of the digital certificates and keys is tightly constrained and single purposed, and the types of available transactions are limited (for example Landonline);
- they tend to operate under existing terms and conditions, with previous well-defined contractual and legal liability arrangements;
- there is usually a recognised authority over the domain of the transactions, which can take responsibility for registered digital certificate holders;
- the deployment of digital certificates is tightly coupled with (or embedded in) specific types of applications, for example smart cards or tokens, and senders and receivers typically use the specific forms and/or special-purpose application software;
- front-end registration processes are not onerous and are fit for the intended purpose, rather than seeking to standardise general-purpose evidence of identity rules as if all certificates were equivalent;

- there is a relatively high transaction volume, to make the benefits of replacing previous paper transactions worthwhile, because implementations often deliver most value when used for automating paperless routine transactions between parties who have an existing business relationship;
- the digital certificates are based on representing membership of some well-defined community, for example a credit card scheme, professional association or employment, as opposed to strictly identity.

Implementing systems outside of the characteristics above may lead to issues and problems that have frequently been associated with PKI. These include complex legal and liability issues, the need for clients to undergo multiple, onerous identity checks, lack of good e-service applications, responsibility of the owner to understand and monitor digital certificates, and international differences in identification standards.

Successful PKI implementations tend to be characterised by systems designed to replace paper-based transactions between parties with an existing pre-defined and well-developed relationship, pre-defined legal and liability arrangements governed by an existing authority, and within a limited transaction scope.

Mitigating Agency Authentication Risks

How can users be certain that the site they have connected to is the one they really want? It is generally accepted that there is no single technical or process oriented solution that can provide a robust agency authentication mechanism by itself. Agency authentication requires a combination of technical and process solutions, regular monitoring and updating. Constant advances in technology and developments in 'hacker' methodology mean that any solution needs to be regularly monitored and kept up to date. The latest identified risks and exposed weaknesses must be addressed and applied to the agency authentication solution. To provide security to their Internet applications, agencies need to implement additional technical layers and establish processes that will provide the additional security appropriate for their online transactions.

The concept of Agency Authentication is detailed in the Concepts section of this document – refer to **Agency Authentication.**

It is recommended that any agency authentication solution address the three following areas:

1. Pre-transaction These are the pre-cursor events to an online transaction between a Client and agency. The focus is on building awareness of the problem, achieving user education and providing an infrastructure that will support a robust agency authentication solution.

2. Current-transaction These are the events that occur during an online transaction between a Client and agency. The focus is on establishing the identity (authenticity) of both parties.

3. Post-transaction. These are the events that occur after an online transaction between a Client and agency has been completed. The focus is on the Client and agency implementing processes that will assist in identifying any fraudulent activity that has taken place. It will assist in monitoring the system to identify any patterns in activity that may cause suspicion and have gone previously un-noticed.

The guidelines, where possible, are described in a technology-neutral manner and focus on the objectives, not the technical or implementation details.

1. Pre-transaction guidelines:

- **User education:** Information should be provided to both Clients and agency staff. This would include increasing their knowledge of how to identify and mitigate risks. The 'human factor' and general complacency are some of the main vulnerabilities related to agency authentication that will require either:
  - a comprehensive education programme; or
  - less reliance being placed on the user to correctly understand the security options in place and/or to follow complicated procedures.

For example: how to check the agency name matches the name on the certificate or to check the 'padlock'. This should also include information on how to handle any error messages or information instructing the Client to return to the agency site at a later time (a common strategy used by hackers to delay users after they have stolen their passwords or access codes).

- **Website design:** The agency website design requires consideration of its appearance for the individual agency and all-of-government. Providing the Client with a consistent experience with individual agency websites, and across all government online initiatives, will assist the Client in being able to identify less competent fraudulent websites.

This would include:

- displaying the agency logo;
- displaying legitimate contact details (such as 0800 number);
- being written in an appropriate style for that agency;
- providing a consistent user experience, especially in relation to asking for a Client's username and password;
- being consistent in relation to when a username and password is asked for during a transaction assists Clients in identifying possible fraudulent requests to provide their password details to a fake website.

- **Secure Socket Layer [SSL] certificates:** SSL server certificates are the industry standard for authenticating servers. For example, the use of an SSL certificate by the agency server that the Client's browser would check whenever logging on to the agency site. More recently, vulnerabilities in the use of SSL certificates have been exposed. The majority of these relate to the 'human factor' and users' lack of understanding of their use and security flaws in SSL design. Although vulnerable, the use of SSL certificates combined with user education should be the minimum standard for all agencies.

When referring to SSL, readers are reminded that Transport Layer Security [TLS] version 1 now supersedes SSL version 3 and is practically identical. To ensure future developments of TLS are included in future design considerations, both should be referred to when investigating options in this area.

The SSL server certificate that agencies use should be purchased only from an internationally recognised Certification Authority such as Thawte or Verisign. SSL server certificates issued by a recognised Certification Authority will be automatically recognised by any of the popular web

browsers. The use of locally generated or self-signed certificates is strongly discouraged. Self-generated certificates will be queried by the browser, adding a further step and decision that has to be taken by the user.

An additional benefit to using SSL during user authentication is the encryption that SSL provides. This means that a user's identity and password will not be subject to interception in transit.

- **End User control:** Part of the difficulty in ensuring the integrity of an online transaction is the lack of end user control. This ranges from varying degrees of technical knowledge on the part of the client, to different browser configurations and operating systems. Options for gaining some control or consistency at the Client end include:
  - the use of hardware devices (such as tokens); or
  - using installed software at the Client end capable of encapsulating technology solutions for agency authentication, without reliance on the Client to operate it and follow correct procedures.

Examples of the latter include software installed on a token that is capable of providing a secure agency authentication mechanism or a PKI capable token that hides the complexity of the authentication process from the Client.

- **Consider physical layer security:** This option may not be viable for most online transactions. It is unlikely to be available in all areas. If the infrastructure and network are available, a possible alternative is to use dedicated lines across a network either not connected as part of, or operated separately from, the Internet. The viability of this option depends on agency location and the provision of a suitable network, which is unlikely to be available outside the main centres.

2. Current-transaction guidelines:

This section provides guidance regarding measures that will support agency authentication during transaction.

- **Shared secret (Challenge and response):** This involves the agency authenticating itself to the Client by providing information known only to the agency and the Client at the time of transaction. There are many variants on this theme. Each should include displaying information to the Client that only the agency and Client would know. Examples include:
  - the last transaction date and time;
  - a pre-determined shared secret;
  - displaying a pre-selected graphic; or
  - displaying the Client's full name and address as a greeting.

The purpose is to mitigate against phishing techniques by showing the Client that the agency has information that the fraudulent website would not have access to. To mitigate against 'man-in-the-middle' attacks, this information would have to be provided across a channel other than the Internet. For more information on using other channels refer to 'Out of band considerations' in the sub-section below.

A basic process to implement shared secrets would involve the Client

accessing the agency site and providing a low security means of identifying themselves, for example a Client number or email address. The agency can then use this to locate the previously-shared secret and repeat it back to the Client across the pre-agreed channel.

- **Out of band considerations:** An 'out of band' solution may be an option for high-risk transactions or as an alternative to a purely technical solution. 'Out of band' usually involves some communication or transmission between the Client and the agency that is not reliant solely on the Internet for transmission. This approach mitigates 'man-in-the-middle' attacks and provides multi-factor authentication. Examples of 'out of band' include cellphones, SMS messaging, telephone call or, in more complex initiatives, token devices with one time pass code generators. There are many variants on the concept. These usually involve the Client logging into the agency and then being provided with an access code or identifiable information via a channel that only the agency would know. For example: the Client's cell phone number or email address that a 'man-in-the-middle' attack would not have access to. An 'out of band' solution involves a higher level of complexity and infrastructure that would have to be balanced against cost and the benefits being obtained.

- **Transaction agreements:** An option becoming more prevalent is the setting up of transaction agreements to protect against un-authorised access to services or financial transactions. Any transactions made outside these limits or times would trigger an exception process where the transaction may be delayed until an offline verification can be obtained from the Client. Examples of these would be immediate acceptance of transactions during office hours on certain days of the week, and the automatic delaying of transactions outside these agreed times until offline verification can be obtained.

- **Programming solutions to mitigate against fake websites** One technique used by hackers to implement fake websites includes using the legitimate website as a background and superimposing the fake site on to the legitimate website. From the Client's perspective the website looks real, acts appropriately, and contains the legitimate SSL padlock. The Client is then prompted to enter their details into the fake site, where the hacker obtains their authentication details. Some programming languages, for example JavaScript, have functions available, to detect if the section of the website is embedded in a frame and, if so, to push the legitimate section of the website to the front. This should prevent hackers from superimposing fake website sections over the top of legitimate ones.

3. Post-transaction guidelines

This section provides guidelines about events that can occur after a transaction has taken place to support agency authentication. The purpose of the events is to identify fraudulent activity that may have gone un-noticed by the Client and/or agency.

- **Provide account information to the Client:** The Client should be provided with regular and detailed transaction records to allow them to identify fraudulent activity.

- **Monitor account activity:** Periodic checking of account activity should be undertaken to identify exceptional behaviour that may indicate fraudulent

activity on a user account. For example, excessive transaction requests within a short period, or excessive service requests compared to previous behaviour.

With any type of agency authentication, the most important element is user education and awareness. Agencies are responsible for the protection of the user information that they hold. It is the responsibility of the user to assist in that protection.

General guide for Agency Authentication practices

It is not expected that all agencies should implement all of the individual guidelines. Determining which guidelines to implement is up to the individual agencies. A formal risk identification, assessment and management process, together with a cost benefit analysis, should provide input into the decision.

The following table is provided as a general guide for agencies when considering the agency authentication options.

GUIDELINES

RISK LEVEL	PRE-TRANSACTION	CURRENT-TRANSACTION	POST-TRANSACTION
MINOR	• Website design		
MODERATE	• All the above • User education • Secure Socket Layer [SSL] certificates	• Shared secret	• Provide account information to the client
MAJOR	• All the above • Consider control at the user end	• All the above • Out of band considerations • Programming solutions to mitigate against fake websites	• All the above
EXTREME	• All the above • Consider physical layer security	• All the above • Transaction agreements	• All the above • Monitor account activity

Interoperability

Interoperability is an important consideration for agencies currently implementing authentication solutions because of the planned strategic direction for all-of-government authentication. The following sections provide some guidance to implementers regarding how to achieve and maintain interoperability.

Standards

Standards compliance is one of the most important steps to ensuring interoperability. Adopt appropriate standards and ensure that you follow them.

There are existing and emerging standards in the areas of authentication and access control that stand out from the rest. These are:

LDAP v3 - common standard for directories. There are a large number of compliant implementations, including both commercial and open source.

A range of other standards may be relevant to specific implementation initiatives. Some of these standards are outlined in **Appendix C - List of Recommended standards.**

SAML - The Security Assertions Markup Language appears to be the best emerging standard for communicating authentication and authorisation information using XML. This work is based on the Organisation for the Advancement of Structured Information Standards (OASIS), a diverse industry group producing standards to facilitate electronic/Internet transactions.

SSL - Secure Sockets Layer provides an encrypted communications channel between the web server and the end user. SSL also authenticates the web server to the user. At a minimum, SSL should be used to encrypt the transmission of usernames and passwords when a user is authenticated.

Demonstration

Standards are an important part of maintaining interoperability, but are not a guarantee. Many standards, such as SAML, allow each vendor to define their own authentication assertions. This means use of SAML is not guaranteed to ensure interoperability between vendors' products.

The best way to ensure interoperability is by demonstration. When selecting authentication and authorisation products, ensure that a demonstration of interoperability is part of the selection process.

Approaches

A number of industry groups have attempted to define a set of standards and practices for web services, including authentication and authorisation.

OASIS, the Organisation for the Advancement of Structured Information Standards, may be one of the most universally accepted bodies. Their standards are frequently referenced by other bodies.

The Liberty Alliance Group is an organisation that promotes a de-centralised framework for web service interoperability, including authentication and authorisation.

Passport. Microsoft provides their .NET Passport Authentication service as an online authentication system to support web services. The dominating feature of this system is a single centralised authentication system, controlled by Microsoft, that supports a wide variety of customers.

Staff Training and Certification

The all-of-government strategy around authentication involves promoting consistency of user experience, and of system implementations across agencies. An important part of achieving this is developing and maintaining staff skills in individual agencies and across government. This is important, not only in providing a consistent service to Clients, but also in developing and increasing security awareness in the area of online authentication and information management in general.

The majority of government agencies have existing training and human resource initiatives focused on their core business and staff development. The areas of knowledge listed below are presented for consideration in agency training programmes and may already form part of an agency's training schedule. They should not be considered compulsory but, if

implemented, should provide a broad and stable skill set related to authentication systems and information technology that would promote consistency and transferable skills across government.

Staff involved in handling, supporting or the management of personal Client or agency information should also be specifically considered as candidates to undergo security vetting processes, and to obtain corresponding security level access.

Operational staff skills and knowledge

Operational staff should have knowledge of the correct procedures for obtaining, storing and handling Client information. In addition to any other training, consideration should be given to ensuring that staff have the opportunity to receive training in:

- the agency's own policy on Client privacy and information handling;
- State Services Commission - Code of Conduct for Public Servants;
- Privacy Act 1993;
- Official Information Act 1982;
- Human Rights Commission Act 1993;
- Archives Act 1957; and
- Security in the Government Sector (SIGS).

Training for other staff

Staff involved in IT management and infrastructure, and project management and advisory roles, may also require the following additional training when authenticated online services are implemented:

- Information Technology – Code of practice for information security management (AS/NZS ISO/IEC 17799:2001);
- Risk Management – (AS/NZS 4360:1999);
- Electronic Transaction Act 2002;
- Computer Crimes Act 2002;
- Security in the Government Sector; and
- Guidelines for Managing and Maintaining Major IT Projects.

Notes:

07 Advisory Roles

The following agencies have key roles in the provision of advisory services to government. This includes participating in the development, operation, application and ongoing maintenance of standards and guidelines and, in this case, the Best Practice Framework.

Archives New Zealand

Archives New Zealand is a Public Service Department whose functions are to ensure the creation, maintenance and disposal (destruction, or retention as archives) of government records.

A full and accurate record of government activity is fundamental to a well-functioning democracy since it provides the mechanism whereby the public sector can account for its decisions and actions to government and its citizens. Records also provide evidence for citizens to confirm or claim their rights and entitlements, as well as providing individual public servants with evidence to justify their decisions.

By administering the disposal provisions of the Archives Act 1957 and providing advice and assistance to agencies, Archives New Zealand ensures that there is ready access to vital evidence for both government and its citizens.

Archives New Zealand's standards, guides and other tools on a range of recordkeeping issues and activities are available on its Continuum website:

Website: http://www.archives.govt.nz/

Department of the Prime Minister and Cabinet

The Department of the Prime Minister and Cabinet (DPMC) is one of the three central agencies responsible for co-ordinating and managing public sector performance. The others are the State Services Commission and the Treasury.

The Department's overall area of responsibility is in helping to provide, at an administrative level, the “constitutional and institutional glue” that underlies our system of parliamentary democracy.

DPMC serves the Executive (the Governor-General, the Prime Minister and the Cabinet) through the provision of high quality impartial advice and support services that facilitate government decision-making at both strategic and operational levels.

A major role of the department is to help co-ordinate the work of the core public service departments and ministries – so that decision making takes account of all relevant viewpoints and is as coherent and complete as possible.

DPMC is the authority under which SIGS is published.

Website: http://www.dpmc.govt.nz/

E-government Unit (State Services Commission)

The State Services Commission supports the State Services Commissioner in the discharge of his statutory responsibilities, which are to:

- at the direction of the Prime Minister or request of a responsible Minister, perform the functions and exercise the powers that apply to the Public Service;
- under the various Statutes, provide consultation on, or concurrence in, the terms and conditions of employment of a chief executive.

The E-government Unit of the State Services Commission provides leadership and coordination of the electronic government programme. The Government's aim, under the E-government Strategy, is to create a public sector that is structured, resourced and managed to perform in a manner that meets the needs of New Zealanders in the information age and which increasingly delivers information and services using online capabilities.

Website:http://www.e-govt.govt.nz/

Government Communications Security Bureau

The Government Communications Security Bureau (GCSB) contributes to the security of New Zealand through the provision of timely foreign signals intelligence to Government and assisting Government departments and agencies to protect their electronic information resources and communications systems.

GCSB also operates the New Zealand Centre for Critical Infrastructure Protection (CCIP), which is dedicated to providing advice and support to protect New Zealand's critical infrastructure from cyber threats. CCIP has three main roles:

- providing 24 hour/7 day "watch and warn" advice to owners of critical infrastructure and government departments
- analysis and investigation of cyber attacks
- to work with critical infrastructure organisations and other sectors nationally and internationally to improve awareness and communications regarding information technology security

Website:http://www.gcsb.govt.nz

Identity Services (Department of Internal Affairs)

Department of Internal Affairs (Identity Services Business Group) is currently developing the Evidence of Identity Framework which is in the final draft/consultation phase.

For advice or information related to this area, refer to Department of Internal Affairs, Identity Services Business Group.

Website:http://www.dia.govt.nz/

Office of the Controller and Auditor-General

The Controller and Auditor-General is a statutory Officer created by Parliament in the Public Audit Act 2001. The Auditor-General is independent of executive government and is answerable to Parliament.

The Auditor-General is the auditor appointed by Parliament to audit all public entities (including the Crown Accounts, Government Departments, Crown entities, State-owned entities, Local Authorities and their subsidiaries, Statutory Boards and Other Public Bodies).

As Controller, the Auditor-General monitors and certifies whether the Government has the necessary authority from Parliament for its proposed daily expenditure. This authority – referred to as supply – has the following key elements:

- the purpose of the expenditure must be lawful;
- there must be an appropriation voted by Parliament; and
- there must be a warrant from the Governor-General.

Website:http://www.oag.govt.nz/

Office of the Ombudsmen

The Ombudsmen are independent Officers of Parliament. Their primary purpose is to inquire into complaints raised against New Zealand central, regional and local government organisations or agencies. They are independent review authorities and are accountable to Parliament, not the Government of the day. They have three main roles:

- under the Ombudsmen legislation, to investigate complaints received from members of the public;
- under the official information legislation to review, any decision to decline the release in part or full of official information held by a government agency; and
- under the Protected Disclosures Act 2000 (PDA), to act as the provider of information and guidance to those who have made or are considering making a protected disclosure and as an "appropriate authority" for the making of disclosures pursuant to the Act.

Website:http://www.ombudsmen.govt.nz/

Office of the Privacy Commissioner

The Office of the Privacy Commissioner is an independent Crown Entity established by the Privacy Act 1993. The Privacy Commissioner:

- has a number of functions including investigating complaints and promoting, by education and publicity, an understanding and acceptance of the information privacy principles;
- has a team of investigating/complaints officers led by a manager for investigations, along with an enquiries team, which takes written and telephone and email enquiries;
- can issue codes of practice which may: modify the application of any of the information privacy principles; modify the application of

any of the public register privacy principles; or exempt any action from the principles;

- must have regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of the free flow of information and the recognition of the right of government and business to achieve their objectives efficiently;
- has a watch-dog role in relation to privacy; and
- monitors and reports on authorised information matching programmes. The Privacy Act places controls on statutory information matching programmes implemented in the public sector.

Website:http://www.privacy.org.nz

Standards New Zealand

Standards New Zealand is the operating arm of the Standards Council, a Crown entity established under the Standards Act 1988. The Standards Council, an appointed body with representatives from all sectors of the community, oversees the development and adoption of Standards and standards-related products.

Elements of the Standards New Zealand role include:

- facilitating the development and delivery of standards-related products by partnering with government, industry and consumer sectors;
- promoting the use of standards in the interest of the economy and community; and
- being the New Zealand member body of the International Organisation for Standardization (ISO) and the International Electro technical Commission (IEC).

Website:http://www.standards.co.nz

Health and Disability Sector

Agencies from the Health and Disability Sector should be aware of the specific codes, guidelines and standards that may apply to them.

For these agencies, ongoing compliance with existing sector authentication standards should be a primary consideration, and agencies should liaise with the Ministry of Health to obtain current information regarding specific Health and Disability Sector requirements.

Website:http://www.moh.govt.nz

Appendix A: Legal Advice Regarding Evidence Requirements

This appendix presents general legal advice regarding evidence requirements in relation online to authentication.

For some transactions, the ability to prosecute an individual for a crime relating to an authenticated online transaction is particularly important. While the transaction itself is the most important process, the secondary need to prosecute for fraud is important too.

Many of the issues detailed in the Legal issues section of this document, such as breach of contract, usually require a much lower level of evidence in court than is required for prosecutions. The evidence for prosecutions is based on "beyond reasonable doubt" which comes close to 100% proof. Where there may only be a need to prosecute in a small number of cases, an authentication solution should be designed to accommodate that need. Legal advice should be obtained in the early design stages to ensure legal requirements are met.

A significant issue with prosecutions based on online authentication is proving that the person presenting as Jane Doe is in fact Jane Doe. Where someone has signed something in handwriting, their identity can be readily established (if there is a forgery that can be readily established too). The on-line equivalent is more difficult as, with current practically available technology such as PIN numbers and digital certificates, often all that can be established is that someone used Jane Doe's PIN or digital certificate. Because there are genuine situations where keys can be misused, for example digital certificates in an office environment, an accused person may be able successfully to claim that it's not proven against him or her that it was he or she that used the digital certificate.

There are some solutions that minimise these risks and it is important for implementing agencies to get advice early on, along with input from other stakeholders such as security, privacy, and IT experts.

Those implementing the systems should take into account:

- the widened provisions to cover computer crimes, introduced in the Crimes Amendment Act 2003;
- the fact that other evidence is often available, and being able conclusively to prove the authentication will not always be essential. For example, the fraudster gets the money paid into his account, and that could be enough evidence to succeed on a prosecution. Therefore the agency may decide to adopt the online authentication solution even though it comes with some risks.

Meeting court evidence needs will often be important, even if the need to prosecute is not a significant driver. The following information is available:

- PD 0008:2003 – Legal admissibility and evidential weight of information stored electronically (available from the British Standards Institute www.bsi.org.uk)
- HB 171-2003 – Guidelines for the management of IT evidence (available from Standards Australia www.standards.com.au)

Appendix B - Reference Standards and Guidelines for NZ Information Systems

Due to the large and complex nature of this table it can only be viewed on the accompanying CD-Rom or E-government website.

Appendix C - List of Recommended Standards

Information technology – Code of practice for information security management – AS/NZ ISO/IEC 17799:2001

"This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organisation. It is intended to provide a common basis for developing organisational security standards and effective security management practice and to provide confidence in inter-organisational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations" – AS/NZ ISO/IEC 17799:2001

Risk Management – AS/NZS 4360:1999*

"This draft standard was prepared by the Joint Standards Australia/Standards New Zealand Committee on Risk Management as a revision of AS/NZS 4360:1995 Risk Management. Accordingly it retains the objective of providing a generic framework for establishing the context, identification, analysis, evaluation, treatment, monitoring and communication of risk." - AS/NZS 4360:1999

*Currently under revision. New version due for release in June/July 2004

Information security risk management guidelines – HB 231:2000

Handbook version of AS/NZ 4360 – intended for use as a reference document by three audiences:

- Managers accountable for the management of information security;
- Personnel who are responsible for initiating, implementing and/or monitoring generic risk management systems within their organisations; and
- Personnel who are responsible for initiating, implementing and/or maintaining information security within their organisation.

Security In Government Sector – (SIGS)

This manual is issued by the Interdepartmental Committee on Security in accordance with its terms of reference. It replaces the manual "Security in Government Departments" issued in 1994, and incorporates the revised security classification system approved by Cabinet on 18 December 2000.

New Zealand E-government Interoperability Framework (NZ e-GIF)

This document is designed to assist agency senior managers, business managers and information technology professionals to make decisions about ICT that will enhance their organisation's ability to work with other agencies in the e-government environment.

Appendix D - References

There is a vast array of reference material relating to authentication. Set out below are details of documents that agencies may find particularly helpful and which have been referenced within this Framework.

Secure Electronic Commerce – Building the Infrastructure for Digital Signatures and Encryption – Second Edition

Warwick Ford and Michael S. Baum
Prentice Hall 2001 – New Jersey

Non-Repudiation in Practice

Chii-Ren Tsai
Available online at: http://dsns.csie.edu.tw/iwap/proceedings/sessionD/6.pdf

Accessed 29 February 2004.

Authentication Reference Guide – Secure Computing

Available online at: http://www.securecomputing.com/pdf/authentication.pdf

A guide to leading industry authentication methods from passwords to digital certificates to biometrics. Their pros and cons and deciding which method is best for you.

This reference is included to provide readers with additional information only related to authentication and is not intended as a Standards, Compliance or Best Practice Framework.

The Authentication Scorecard – RSA Security.

Available online at:
http://www.rsasecurity.com/products/authentication/whitepapers/ASC_WP_0403.pdf

Provides information on authentication technologies and issues to consider when comparing them.

This reference is included to provide readers with additional information only related to authentication and is not intended as a Standards, Compliance or Best Practice Framework.

Appendix E - Glossary of Terms

Access Control: This is how authorised privileges are provided to an individual. It is the mechanism that controls at a low level, what actions an individual can perform, or will be performed on their behalf. Authorisation gives permission for an activity; Access Control conducts the activity.

Assertion: A statement or premise that is taken as being correct or true.

Attribute: An individual piece of information.

Authenticate: To give legal validity to, to render valid, to establish the validity of.

Authentication or Authentication of identity: The process of initially establishing that a person is genuinely who they say they are, and the process of establishing an authenticated online session between a government agency and an authenticated individual.

Authentication Strength: See Key Strength.

Authorisation: Whereas authentication is used to establish the identity of a party to a transaction, authorisation is used to determine what privileges that party will enjoy. With typical online applications, individuals are authorised to view/change information related to themselves and conduct transactions such as purchases, using their own resources.

Biometric: In the context of authentication, biometric refers to a physical characteristic of a person. For example, fingerprint, voice, DNA or physical appearance, such as facial image.

Brute Force Attack: A technique used by Internet hackers to attempt access to a protected system. This attack requires trying all (or a large fraction of all) possible values till the right value is found; also called an exhaustive search.

Cabinet Policy and Principles: For the purposes of this document, this refers to the April 2002, Cabinet-approved policy and implementation principles (the authentication principles) for online authentication and for the development of a consistent approach to government authentication [CAB Min (02) 12/2A refers].

Client or Individual: A person seeking to access a government service online.

Component: A component can be either hardware, software or a process that delivers a piece of functionality within a system. Related components can be grouped together to form a ‘subsystem’.

Digital Certificate: A digital certificate is an electronic means of establishing your credentials when doing business or other transactions on the Internet. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

Digital Signing: Refers to an attempt to mimic the offline act of a person applying their signature to a paper document. Involves applying a mathematical algorithm, usually stored on and as part of the user’s private key, to the contents of a body of text. This results in an encrypted version of the document (this is referred to as the ‘digitally signed’ document) that can only be decrypted by applying the user’s public key.

Directory: Directories provide hierarchical storage of information (as opposed to relational schema or designs, such as databases). The de facto standard for directories is LDAP V3. Directories are used to provide quick and efficient storage for information about people, services and applications.

e-GIF: E-government Interoperability Framework – a collection of policies and standards endorsed for New Zealand government information technology (IT) systems.

E-government Unit [EGU]: The New Zealand E-government Unit was established in July 2000 in the State Services Commission. The E-government Unit is working with government agencies to achieve the Government's vision for e-government.

Entropy:	A measure of randomness or lack of organisation in a situation. A totally entropic situation is unpredictable.
Evidence of Identity [EOI]:	See Identification.
Evidence of Identity Framework:	The Evidence of Identity Framework is being developed as a best practice guide for establishing the identity of individuals who wish to transact with government agencies. The framework is being developed by a cross agency working party.
Evidence of Identity strength:	EOI strength is the level of confidence an agency requires in any identity information provided by the user. For example, a utility bill with the user's name and address, or the user's passport and confirmation of the details from a third party.
Functional Equivalence:	For the purposes of this document, Functional Equivalence refers to the Cabinet and Policy Principles definition in that authentication requirements should be similar to those that apply to an existing transaction, except where the online nature of the transaction significantly changes the level of risk.
Government Agency:	A blanket term that includes departments, Crown entities, and any organisation within the State sector. Service agencies and the Authentication Agency are government agencies.
Granularity:	Refers to the 'level of detail' of any given subject. For example, if a subject is referred to as having 'fine granularity' it is considered to be defined to a high level of detail.
Hacker:	A person who understand the "ins and outs" of computers, networks, and the Internet in general. The term generally refers to a person who has intent to access a computer system without authorisation.
Human Factor:	For the purposes of this document, 'Human Factor' relates to issues surrounding Internet security and the influence of human behaviour on any security mitigation technique.
Identification Evidence of Identity [EOI]:	The process of associating identity data with a particular person.
Identity fraud:	To use the identity of a person without their express consent, for a purpose that the person is not aware of, and/or does not approve of. Generally for an illegal activity.
Identity Management System:	A vendor solution package that combines the features of a Directory Server with software (typically web-based application) to facilitate the provisioning of individuals in an authentication system. The principal features of these products are to provide support for self-registration of users and for automatically dealing with lost passwords.
IMS:	Refer to Identity Management System.
Information Sharing:	For the purposes of this document, Information Sharing relates to the sharing of individual personal information between multiple agencies. This is often deemed to be information matching and usually requires enabling legislation in order for agencies to operate this process.
Key:	A method used by an individual to authenticate their identity across the Internet. Examples of a 'Key' include username/password combinations, digital certificates and tokens.
Key Strength:	Key strength refers to the level of confidence that can be attributed to the presentation of any particular Key type. For instance username/memorised password is considered the weakest form of authentication. The use of a PIN/physical token is considered stronger. Service Agencies might set a minimum "key strength", then use this attribute to see if a Client's Key is suitable for the service.
LDAP:	Refer to Lightweight Directory Access Protocol.
Legal Liability:	The phrase that summarises where the responsibility will lie if/when failures/frauds in the system occur.
Liberty Alliance Project:	A group that promotes open technical specifications that support a range of network identity-based interactions. For further information, refer to *http://www.projectliberty.org*
Lightweight Directory Access Protocol:	A set of protocols used to access a hierarchical directory of information on a directory server. LDAP is considered to be lightweight because it is based on a simplified version

	of X.500 directories. Directories may contain phone numbers, electronic mail addresses, Public Keys, computer names and addresses, or any other information that can be conveniently arranged hierarchically.
Man-in-the-middle attack [MITM]:	A technique used by Internet hackers. It results in the hacker 'positioning' themselves between the user and the system they are transacting with. This allows them to monitor communications and obtain information transferred between the parties.
Multi-factor Authentication:	This is combining two or more authentication techniques together to form a stronger or more reliable level of authentication. This usually involves combining two or more of the following types: • Secret – something the person knows • Token – something the person has • Biometric – something the person is.
Non-repudiation:	The inability of a person or agency to legally repudiate (deny) its participation with an action or a piece of information.
OASIS:	Refer to Organisation for the Advancement of Structured Information Standards.
Online:	For the purposes of this document, this refers to transactions made across the Internet or across a network of computers.
Online Authentication:	The online process of an individual establishing that they are genuinely who they say they are, and the process of establishing an authenticated online session between a government agency and an authenticated individual.
Organisation for the Advancement of Structured Information Standards [OASIS]:	OASIS was founded in 1993 under the name SGML Open, as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). OASIS changed its name in 1998 to reflect an expanded scope of technical work, including the Extensible Markup Language (XML) and other related standards, in particular SAML. Refer to website for further information: *http://www.oasis-open.org/home/index.php*
Person:	An individual human being; man, woman or child.
Personal Information:	Information about an identifiable individual.
PIA – Privacy Impact Assessment:	A formal process to identify and assess privacy implications – in this case of an online authentication solution for government.
PIN:	Personal Identification Number – a PIN is usually a form of shared secret or password in the form of a series of numbers. Usually used in combination with other forms of authentication techniques.
Privacy:	The proper handling of personal information throughout its entire lifecycle, consistent with the requirements of the Privacy Act 1993. It can also mean the right of an individual not to be identified.
Pseudonym:	An arbitrary name chosen by an individual to identify themselves, e.g. a username.
Pseudonymous Transaction:	A transaction where the party who initiated the process does not provide any identity information.
Repudiation:	The rejection or renunciation of a duty or obligation – usually arising from a disputed transaction. A party to a transaction later claims the transaction or part of the transaction did not take place.
Role:	The actions and activities assigned to, or required, or expected of, a person or an entity.
SAML:	Security Assertion Markup Language – an XML-based framework for exchanging security information.
Secure Socket Layer [SSL]:	A protocol developed for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Also referred to as HTTPS.

Service Agency:	Government agency or agent responsible for delivering a service to a client – not the Authentication Agency.
SIGS:	Security In the Government Sector manual – the minimum standards for Government security. Refer to *http://www.security.govt.nz/sigs/index.html*
Single Sign-on:	The act of signing on once (providing a UserID and Password) thereby achieving access to multiple systems or e-services without having to re-establish the identity of the person.
SQL Injection:	SQL injection is the name for a general class of attacks that can allow nefarious users to retrieve data, alter server settings, or even take over your server if you're not careful. SQL injection is not a SQL Server problem, but a problem with improperly written applications.
SSL:	Refer to Secure Socket Layer.
State Services Commissioner:	The Office of State Services Commissioner is central to New Zealand's politically neutral, professional and permanent Public Service. The Commissioner has two separate roles: • As the holder of a statutory office the Commissioner acts independently in a range of matters to do with the operation of the Public Service; and • As Chief Executive of the State Services Commission, the department that supports the Commissioner in the performance of this role, the Commissioner is responsible to the Minister of State Services for the Commission's capability and performance.
Technology Neutrality:	For the purposes of this document, Technology Neutrality refers to the Cabinet and Policy Principles definition in that agencies are to ensure a range of technology options are considered, and as far as possible to avoid 'vendor capture'.
Token:	A physical device used in the authentication of an individual. A type of 'Key', usually held in the possession of the individual. Examples include USB tokens or smart cards.
Transaction Strength:	This is the level of confidence an agency requires in an online transaction. For example, a low strength transaction may only require an acknowledgement via email that a service request has been received; a high strength online transaction may require many of the factors related to non-repudiation of a transaction.
Transport Layer Security [TLS]:	The successor protocol to Secure Socket Layer [SSL], created by the Internet Engineering Task Force (IETF) for general communication authentication and encryption over TCP/IP networks. TLS version 1 is nearly identical with SSL version 3.
Trust Levels:	The Transaction Trust Levels (the 'Trust Levels') were developed to provide guidance to those agencies considering providing a service online, by enabling them to categorise transactions on a consistent basis. This was intended to ensure that transactions of a similar type are implemented using similar authentication solutions.
Unique Identifier:	For the purposes of this document, the definition of Unique Identifier is the interpretation as set out in the Privacy Act 1993. *"Unique Identifier" means an identifier – That is assigned to an individual by an agency for the purposes of the operations of the agency; and That uniquely identifies that individual in relation to that agency; - But, for the avoidance of doubt, does not include an individual's name used to identify that individual.*
User Name/Userid	A construction of letters and numbers that, in conjunction with a password, uniquely identifies a person.
Verification (of a key)	A process to confirm whether a key is appropriate to be used.
xNAL	NZ E-government extensible name and address language. For further information refer to 'xNAL Guidelines'.