

Blueprint

Authentication for e-government

July 2003

E-government Unit
State Services Commission



Purpose

This document is the Online Authentication blueprint for the detailed design and scoping work that the E-government Unit will carry out, in conjunction with agencies and key stakeholders, by early 2004.

The blueprint:

- provides a background to online authentication;
- outlines the policy work that has been completed to date;
- summarises the decisions made by Cabinet about online authentication in June 2003; and
- illustrates the conceptual model for online authentication.

Preamble

Online authentication

To use some government services, you need to prove who you are. You also need to know that you are dealing with a real government agency. The process of proving who you are and establishing the authenticity of the agency is called authentication. The E-government Unit is looking for ways, acceptable to New Zealanders, to authenticate people and agencies so that the types of government service that require authentication can be provided online.

Why online authentication is important

*“By June 2007, networks and Internet technologies will be integral to the **delivery** of government information, services and processes.”¹*

Currently, individuals need to prove who they are to access more than one third of all government services. Increasingly government services are being provided online. The government portal - www.govt.nz - helps you find over 1,000 services provided by central and local government agencies. With more services from more government agencies becoming available online in the next few years, it is also important to ensure that the privacy of individuals is maintained and the security of information is protected.

You can use most existing online services without any kind of authentication, including getting access to a vast amount of information that is freely available online, such as education review reports on schools, health and safety information or the opening hours of your local public library. However, to deliver some kinds of government services online, agencies need a way of ensuring that these services - delivered over the Internet - are going to the right person. This will be achieved by electronically verifying that people are who they say they are and that their privacy is protected. Online authentication also means that you can check and be confident that the Internet site you are using is a genuine New Zealand government agency website.

This is what we mean by **online authentication**.

¹ E-government mission (see <http://www.e-government.govt.nz/docs/e-gov-strategy-june-2003>).

Some everyday authentication examples

There is nothing new about having to prove your identity in order to access information or services. Here are some examples of authentication methods commonly used in every day life.

Joining a library

In order to borrow books or other material from your local library you usually require a library card. In some areas, your library card can give you access to online library services, such as reserving books. When applying for a library card, you usually have to fill out a form and supply the librarian with some independent evidence of your address details (e.g. a bank statement) with your address on it. This confirms that you live in the area and are entitled to use the library's services.

Internet (online) banking

Increasing numbers of New Zealanders are using the Internet for online banking. It is a very convenient process, allowing you to manage your money when you want to. In order for you to carry out online banking, you must first talk to your bank about obtaining access to your bank accounts and services over the Internet. Most banks require you to prove your identity, usually by supplying personal information and your account details. For most banks, once they are sure of your identity, you are then provided with a Customer ID number and a temporary password to use once to login for services at the bank's website. This information is usually posted to your home address. You are prompted to choose your own password for future use the first time you successfully log into the bank's secure website.

Applying for a passport

Every New Zealand citizen is entitled to apply for a New Zealand passport. Passports are valuable items, and therefore evidence must be provided to ensure you are who you say you are. A passport application requires filling in a form with a lot of personal information. Your application has to include an original copy of your birth certification or citizenship certificate as proof of your New Zealand citizenship. The application forms require a person who knows you (your "witness") to fill out and sign a section confirming your identity. The witness also has to sign your photo as extra proof of your identity. These measures all help to authenticate your application.

Principles

Over the past few years the E-government Unit 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. We have analysed which services provided by government agencies in New Zealand require or are likely to require online authentication. We have also looked at overseas examples of online authentication both for government and commercial services.

You can read more about the work so far on the e-government website (see www.e-government.govt.nz/authentication/). As a result of this work, in April 2002 Cabinet established a set of policy and implementation principles to guide the development of online authentication.

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 & 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 minimized.

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.

Design Assumptions

The principles were the basis for the conceptual design work that was carried out by the E-government Unit in late 2002. Four options that represented the possible ways to achieve a consistent approach to online authentication were developed. These conceptual models were analysed to determine the implications for the public and for the government agencies providing services via the Internet. Feedback from the public was also sought to determine what type of authentication system people would prefer to use.

Cabinet considered the results of the analysis and the outcome of the public consultation in June 2003 when it made a decision to proceed with designing an all-of-government authentication solution. As part of its decision, Cabinet agreed that the design work should focus on a centralised approach with limited information exchange and that privacy and security should be key considerations.

Cabinet directed that the design and scoping work cover **all** online services where an individual person is transacting with a government agency and there is a need to prove who they are. This means that the solution will have to work for people resident or temporarily in New Zealand, as well as for people living overseas who use New Zealand government services. It also means that the solution will need to cater for people who access online government services for professional or business reasons as well as those accessing services for personal reasons.

You can read more about Cabinet's decision on the e-government website (see www.e-government.govt.nz/authentication/).

Design assumptions for online authentication

The conceptual model selected by Cabinet is underpinned by the following design assumptions:

- the public should be able to choose whether or not to access services that require authentication over the Internet (the 'opt-in' policy principle);
- authentication (verifying identity) must be handled independently from authorisation (access to services);
- the all-of-government model does not require national ID cards, digital certificates or the exchange of biometric data at the time of transaction (consistent with authentication principles such as technology-neutral, affordability and acceptability);
- existing agency-based identification numbers, for example Inland Revenue Department numbers or National Health Index numbers, will not need to be replaced;
- service agencies will continue to determine entitlement to a service rather than determination becoming a function of the authentication agency. The authentication agency role should be to issue and verify credentials and store identity details provided at registration;
- some transactions require greater security than others. For this reason, some service agencies will continue to require strict processes, such as requiring you to apply in person, before you can receive these types of service. For example obtaining a firearms license;
- some transactions require less security than others. For example, getting general information about government services such as obtaining agency brochures. For this reason, authentication is not required for some transactions; and
- that *Security in the Government Sector* (SIGS)² will provide the basis for the security framework with particular consideration being given to confidentiality, authenticity, non-repudiation, integrity and availability.

² Security in the Government Sector (SIGS) (see <http://www.security.govt.nz/sigs/index.html>).

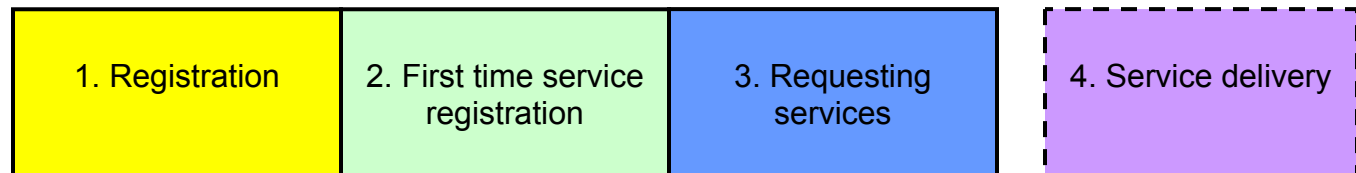
Conceptual Model

A conceptual model provides a high-level picture of how a system and process would work. It does not describe the detail of the systems and processes required to implement the model.

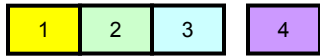
The conceptual model for online authentication illustrates a consistent way for people to identify themselves online when they want to access government services. It is important to remember that online authentication is about verifying who is applying for a service rather than whether or not the person is actually entitled to receive the service.

The diagram below shows the four processes that make up the online authentication conceptual model.

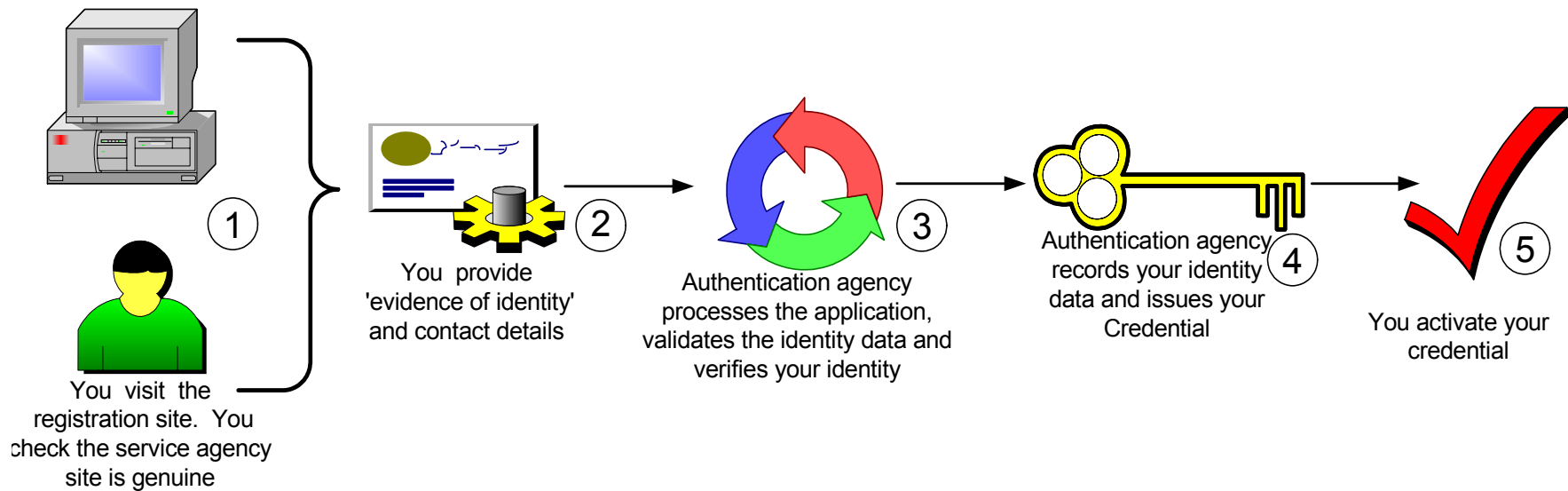
Online Authentication



1. Registration



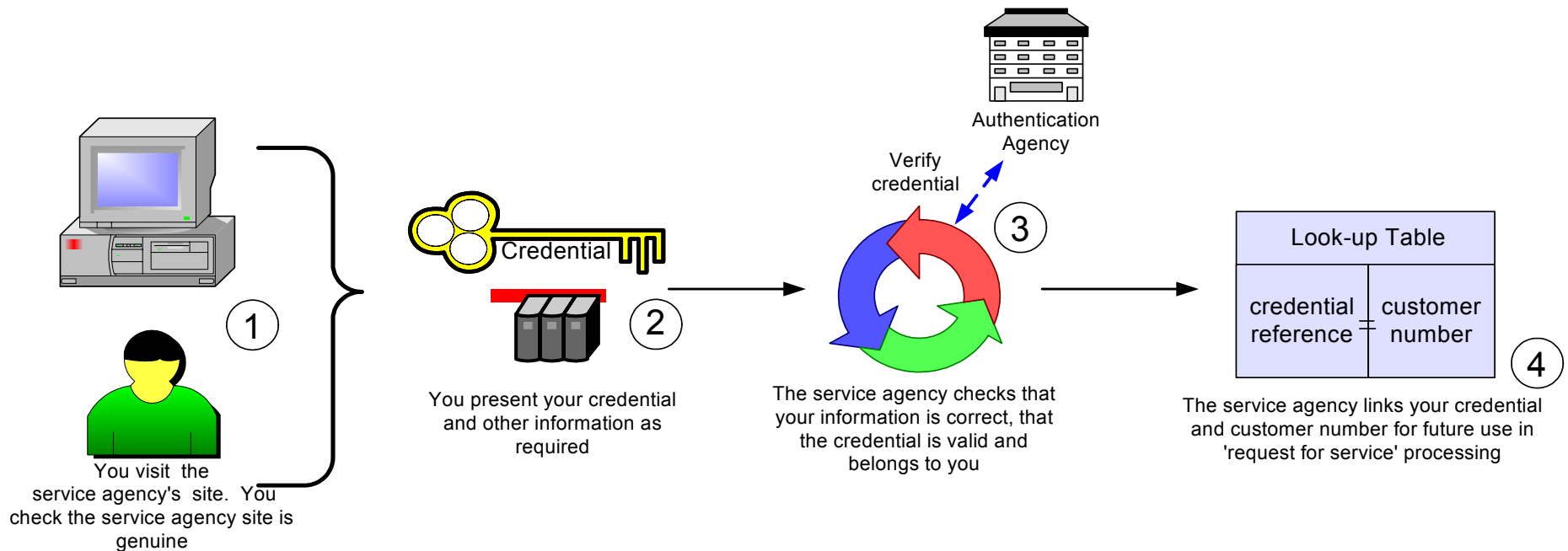
The first process described in the online authentication model is registering for a credential. This occurs once, the first time that you decide you want to access government services online.



2. First time service registration



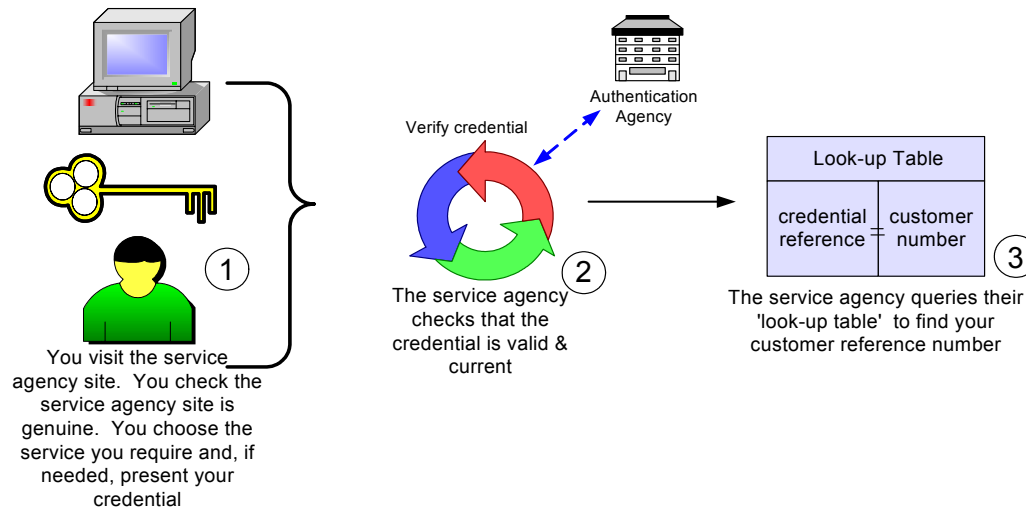
Once you have an authentication credential, you can let the service agencies you deal with know about your credential. You will have different “customer numbers” with the agencies you have already dealt with. Each agency needs to link your credential uniquely to the particular customer number that they use when they deal with you.



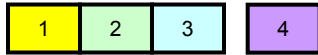
3. Requesting services



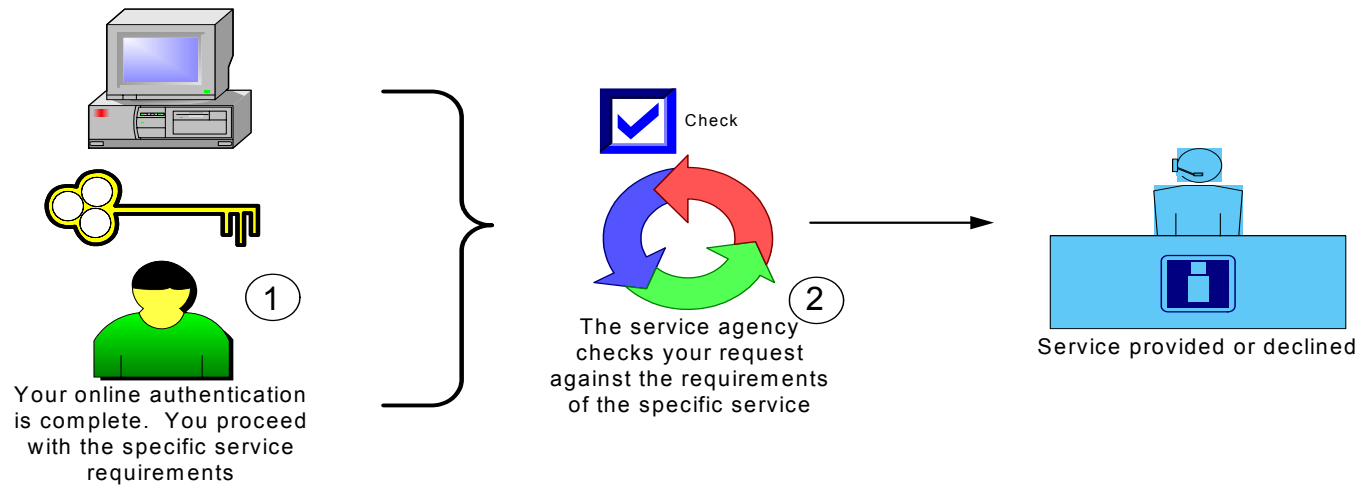
Before you can access a government service online, the service agency first needs to be sure that it really is you. They will ask you to present your credential and then check that it is valid. Once this step is complete, the service agency finds the customer number you previously linked to your credential.



4. Delivering services



The service agency applies their standard rules to decide whether or not you are entitled to receive the government service you are applying for.



Further Information

Online Authentication Project

You can find further background reading, as well as more detailed information and progress updates, on the e-government website (see www.e-government.govt.nz/authentication/).

If you have a specific question that you would like us to answer you can e-mail us at authentication@ssc.govt.nz or write to us at:

Attn: Authentication project team
E-government Unit
State Services Commission
PO Box 329
WELLINGTON

About us

The E-government Unit is a branch of the State Services Commission. It 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.

You can read more about the E-government Unit (www.e-government.govt.nz) and the State Services Commission (www.ssc.govt.nz) online.

Glossary

Authenticate	To give legal validity to, to render valid, to establish the validity of.
Authentication Agency	The government agency or agencies responsible for establishing the identity of the registering person and issuing that person with a credential to use when accessing services online. The authentication agency is not necessarily the same as the agency providing the service - the service agency .
Authorisation	Control of a person's access to an e-service or e-services.
Credential	A form of identification that can be used online which confirms you are who you say you are. Credentials are issued only after your identity has been authenticated in the registration process.
E-service(s)	A government service delivered electronically (i.e. over the Internet) to a person by a service agency . Only some e-services will require that a person will need to be appropriately authenticated .
Registration	The process of registering an identity of a person to be issued a credential to enable authentication for e-services .
Government Agency	A blanket term that includes departments, Crown entities, and any organisation within the State sector. Service agencies and Authentication Agency are government agencies.
Identity	A set of attributes, which together match to a person .
Identification	The process of associating identity data with a particular person .
Individual	A living person.
Opt-in	To choose to participate in something, such as an e-service.
Password	A word or phrase that only you know which can be used to gain access to some online government services. You will be able to get a password only when the authentication agency has established your identity.
Personal Information	Information about an identifiable individual .
Role	Different legal personas that a person can take on (e.g. individual, trustee, etc)
Service Agency	The Government agency responsible for delivering an e-service to a person .
Service-delivery information	Additional information (beyond a credential) required by a person so that they can access a specific e-service .
Service reference number	Customer number held by service agency (e.g. IRD number).
Verification	A step in the registration process, to confirm whether the person is who they claim to be.