

Authentication for e-government
Government Logon Service Design Overview
Initial Implementation - Design Blueprint

The E-government Unit; State Services Commission
New Zealand

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.

Background

What is the purpose of this document?

The New Zealand All-of-government authentication model currently comprises two inter-related but separate services; the Government Logon Service and the Identity Verification Service. The Government Logon Service is currently being built and the Identity Verification Service is in the design stage.

This document provides a high-level overview of the Government Logon Service. An accompanying document will be developed for the Identity Verification Service once the design stage has been completed.

This document:

- reviews the core concepts of authentication used in the New Zealand programme
- outlines the design for the Government Logon Service
- summarises the principles approved by Government for All-of-government authentication and its initial implementation.

What is the All-of-government Authentication programme?

To use some government services, people need to verify who they are. People also need to know that they are dealing with a real government agency. The process of establishing, to the required level of satisfaction, the identity of one (or more) of the parties in a transaction is called 'authentication'.

The All-of-Government Authentication Programme aims to standardise authentication for New Zealand government online services. The State Service Commission initiated the programme in 2000 as a means to facilitate the increasing volume of e-transactions between people and government agencies. For more

details, see www.e-government.govt.nz/authentication/. A two page 'Fact Sheet' that provides answers to frequently asked questions is available at: <http://www.e-government.govt.nz/programme/docs/authentication.pdf>

What stage is the programme at?

The current phase of the All-of-Government Authentication programme, started in July 2004 and scheduled to complete in early 2006, includes:

- the initial implementation of the 'Government Logon Service' to up to four government agencies
- developing standards for the overall authentication process
- policy work on privacy, and future legal implications
- researching and developing ways in which electronic identity of individuals can be managed to create the Identity Verification Service
- supporting review bodies and privacy impact assessments
- further work to confirm the estimated costs and benefits of rolling out the Government Logon Service to other government agencies.

Core concepts for NZ online authentication

This section:

- describes the organizational actors of the All-of-government Authentication model
- describes the generic authentication processes that underpins the model
- introduces some core concepts like 'keys'
- outlines the Government Logon Service processes.

Introduction

In April 2004, the Design and Scoping phase of the Authentication project produced several key documents, including:

- *Authentication Best Practice Framework*
(<http://www.e.govt.nz/docs/authentication-bpf/index.html>)
- *Summary of Business Processes*
(<http://www.e.govt.nz/docs/authent-processes-200312/index.html>)
- *Online Authentication: Security*
(<http://www.e.govt.nz/docs/authent-security-200307/index.html>)

These deliverables identified two core concepts for the Authentication Project:

- **actors** – the specific participants in the authentication process
- **verification and confirmation of identity processes** – separating authentication into two discrete components.

These core concepts are detailed below.

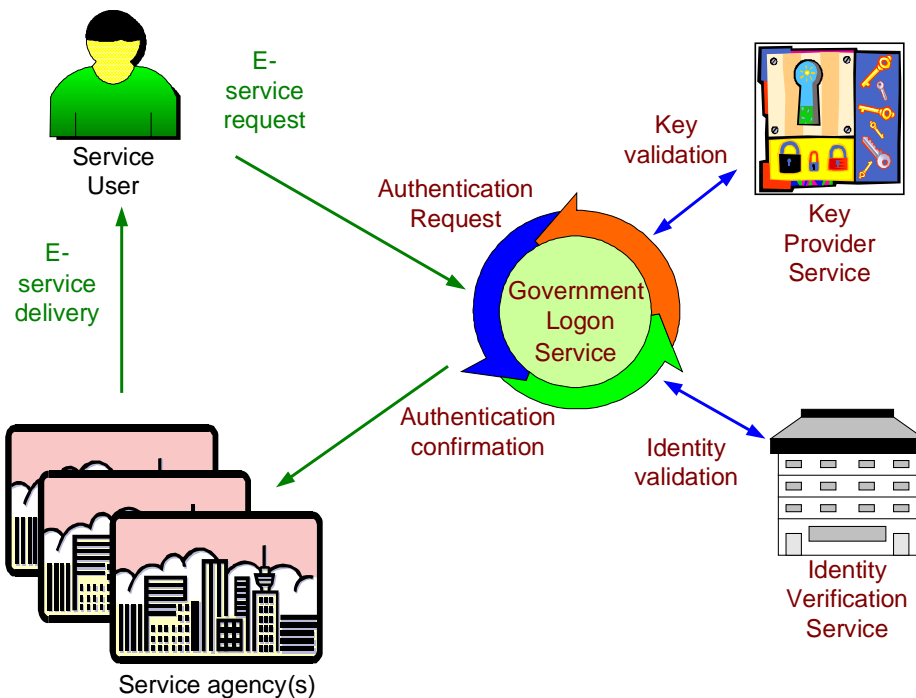


Figure 1: All-of-government authentication participants

Who are the actors?

These are the actors in the all-of-government authentication model:

- **service user** – the person who interacts with agencies to access services via the Internet. A service user is also referred to as an agency’s customer.
- **key provider** – an organisation accredited to issue and manage client logons; when requested by a legitimate agency, the key provider confirms that a key is valid and current. The key may be referred to a ‘logon’.
- **service agency** – the agency that delivers the online service to the client after verifying their eligibility
- **government logon service** – the web site which acts as an intermediary between the service user and service agency, through which authentication transactions pass
- **identity verification service** – manages and holds ID credentials (*The exact shape of this service is being designed and will not be operational in this Initial Implementation phase*).

What are the generic authentication process steps?

These are the two main steps in the authentication process:

- Evidence of identity
- Confirming identity

Evidence of identity

The first step in authentication is a 'one off' process whereby an individual provides evidence to register or establish their identity. Producing a birth certificate and/or having trusted people in the community sign a photo are common examples. Registering an identity may result in the creation of an 'identity (ID) credential' like a passport. A person's ID credential is:

- a recorded set of verified identity attributes
 - unique to each person
 - only presented to prove one's identity.

For Initial Implementation, the evidence of identity process remains with the service agency.

Confirming identity

The second step in authentication is a repeated process, which involves using an authentication method to confirm identity. An authentication method is commonly called a 'key' or 'logon'. A common online example is using a username and password to verify your identity when accessing your Internet banking service. The service confirms users' identity using a 'key' (or 'logon'), such as a username/password or a digital certificate.

What are Keys?

As noted, the term 'key' is used as a metaphor for an authentication method like a username or digital certificate. A key is used as:

- a convenient means for a service user to demonstrate ownership of identity
- presented to access a service that needs to identify its users

The key itself, does not contain any identity details.

For the Government Logon Service, keys are assigned a unique Key Serial Number. The Key Serial Number for a particular key is always the same one.

The Key Serial Number is then extended to create a Modified Key Serial Number. Each Modified Key Serial Number for a particular Key Serial Number is modified to reflect the agency where it will be used. This means that Modified Key Serial Numbers are unique for each key-agency combination. This is explained further in the design section.

What are the Government Logon Processes?

The Government Logon Service design uses the two process steps described above and breaks them out into the following three sub-processes:

1. registration
 - a. evidence of identity is established
 - b. a key is issued
2. first-time service – service agencies verify identity for users' first access and link identity data and the key details
3. repeat service – service agencies confirm the identity of users' for ongoing accesses.

The Initial Implementation phase for the Government Logon Service is only concerned with steps 1b, 2 and 3.

Later phases will establish an Identity Verification Service to manage and hold electronic identity credentials. This Identity Verification Service will address 1a, but for this phase of the project, identity management will remain the responsibility of the service agency.

It should also be noted that service entitlement and authorisation, the mechanisms for letting people use a particular service or any aspect of a service after verifying their identity, are outside of the scope of the All-of-government Authentication Service. Entitlement and authorisation functions continue to remain with the service agency.

Until the Identity Verification Service is available, agencies are encouraged to consult the following published documents to help standardise the identity management process:

- *Evidence of Identity Framework*
(http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Framework-Index?OpenDocument)
- *Authentication for E-government: Best Practice Framework for Authentication*
(<http://www.e.govt.nz/docs/authentication-bpf/index.htm>).

Government Logon Service development

This section reviews the scope, objectives and design of the Initial Implementation of the Government Logon Service.

What is the Government Logon Service?

The Government Logon Service is an initiative to provide a private, secure and convenient service to people using government services over the Internet. The Government Logon Service will allow people to more conveniently access government online services by using a single logon – for instance, a username / password. It will be like having a unique key that opens many government service doors. However, if they wish, people will still be able to use different keys for different services.

The Government Logon Service will:

- make it easier for New Zealanders to take advantage of the benefits of transacting electronically with government
- lower the overall cost to government, by building one service for multiple agencies
- enhance security by allowing faster, more effective upgrades, from a central service provider, in response to ever-evolving security threats.

During current initial implementation phase, up to four agencies will take up the Government Logon Service.

Registration, first-time and repeat service

This section outlines the design for the three major processes in the Government Logon Service, concluding with a diagram showing the separation of information held by actors throughout the processes.

How will registration work?

Registration means service users getting customer records and keys to use services. For the Initial Implementation, service users establish customer records with each participating service agency. Each agency uses its own registration process, based on advice in the *Best Practice Framework* and the draft *Evidence of Identity* standards. (Future implementations will establish centralised identity management services so that service users do not have to register separately with each agency.)

As illustrated below, the process is explained in two steps: agencies create customer records based on details from the service user; and transparently to (separately from?) the agency, service users request and receive keys from a key provider.

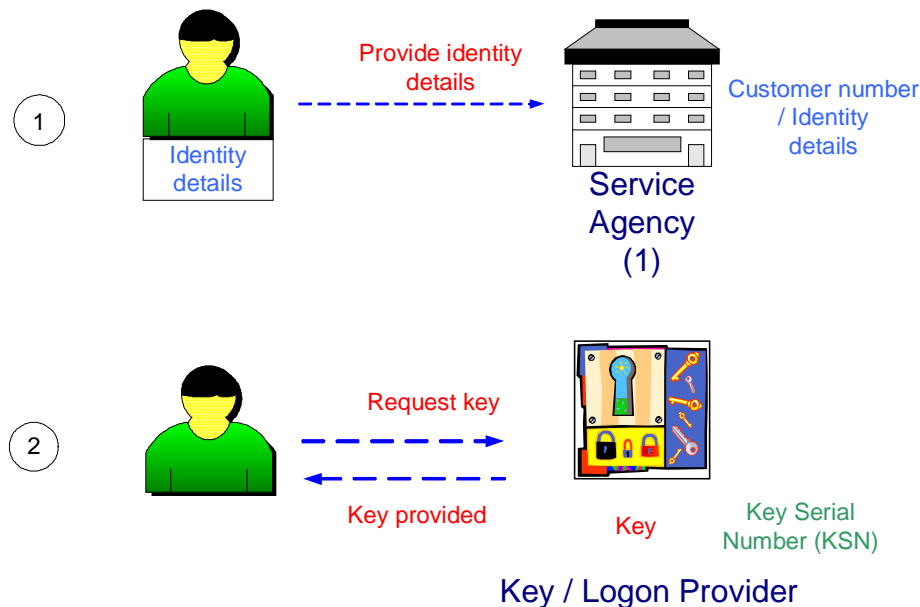


Figure 2: Registration—Customer Record and Logon

The two steps:

- 1 Establish a customer (service agency) identity record – Service users provide service agencies with details that confirm identity, and with further information that enables agencies to determine service eligibility or resource access. Agencies create a unique customer record for each service user.
- 2 Provide a Key – Service users provide Key Providers with sufficient details for the Key Providers to create and administer keys (including for example, details for managing passwords). For the purposes of issuing the key, no evidence of identity process is required. This is the main differentiation from other authentication models. The Key Provider also associates a Key Serial Number for the key.

How does first-time service work?

The first time a client accesses a service, the agency links a client's key to their customer records. The Government Logon Service achieves this by the use of Modified Key Serial Numbers, which are unique to each key-agency combination. As illustrated below, the process involves six steps, from the client requesting access to a service to the service agency storing the Modified Key Serial Numbers.

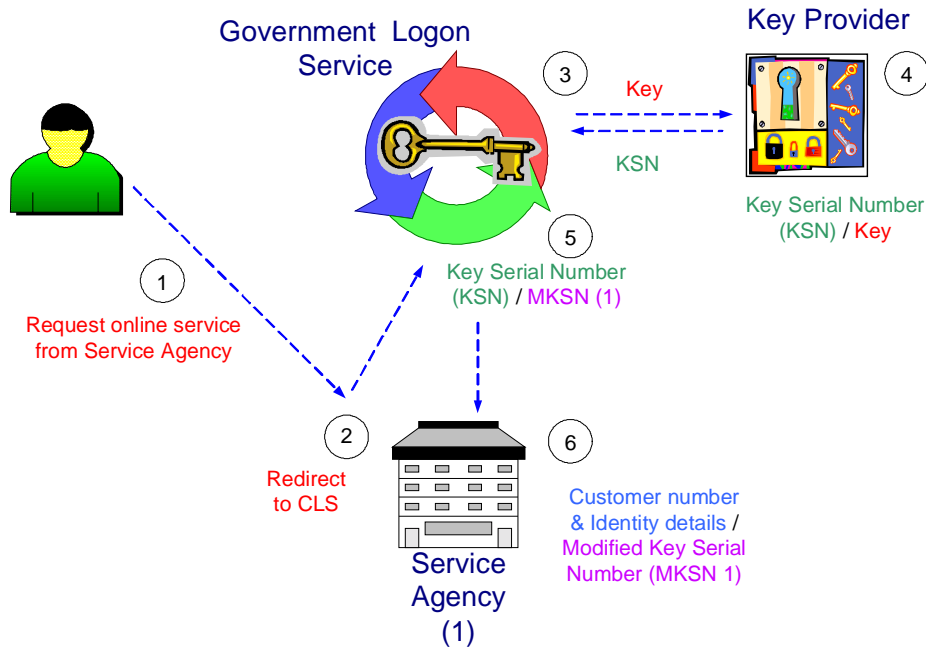


Figure 3: First-Time Service— linking identity with the Key

The steps required to link identity and the keys are as follows:

1. The service user requests an online service by accessing the service agency's website.
2. The agency may request details to determine eligibility for services or resources as well as to confirm identity.
After creation of the customer's record, the agency needs to link these details to the key that the service user will be using to access the service on an ongoing basis. They do this step by storing a 'token' to uniquely identify the first-time service transaction, and match the token to the Modified Key Serial Number generated by the Government Logon Service (in step 6).
To begin this process, the agency re-directs the service user to the Government Logon Service to logon.
3. The service user logs on by entering their key details, for example username and password, at the Government Logon Service website. The Government Logon Service sends a message to the key provider to validate the logon and requests its unique Key Serial Number.
4. The key provider validates the key and sends back the Key Serial Number along with attributes of the key such as its strength (which may determine which transactions are able to be undertaken with that key at service agencies).

5. The Government Logon Service creates a Modified Key Serial Number based on the Key Serial Number. The Modified Key Serial Number is unique for each user for each service agency. The Government Logon Service only sends the Modified Key Serial Number and associated key attributes to the service agency. Neither the actual key nor the Key Serial Number are sent.
6. The Service Agency receives and links the Modified Key Serial Number with the client's customer record that they created during the registration process. This permanent association lets the client repeatedly use the service without having to supply any further authentication details except for their key. The agency does not keep a record of the key, instead relying on its association with the Modified Key Serial Number to authenticate the service user for future transactions. The token used to enable this linkage is deleted.

How does repeat service work?

After the service agency has linked the customer record and key via a Modified Key Serial Number, the service user can transact with them on an ongoing basis. Because each Modified Key Serial Number is different, they cannot be used to match or exchange data across agencies. The agencies only have access to their Modified Key Serial Number – not the Key Serial Number associated with a particular Key.

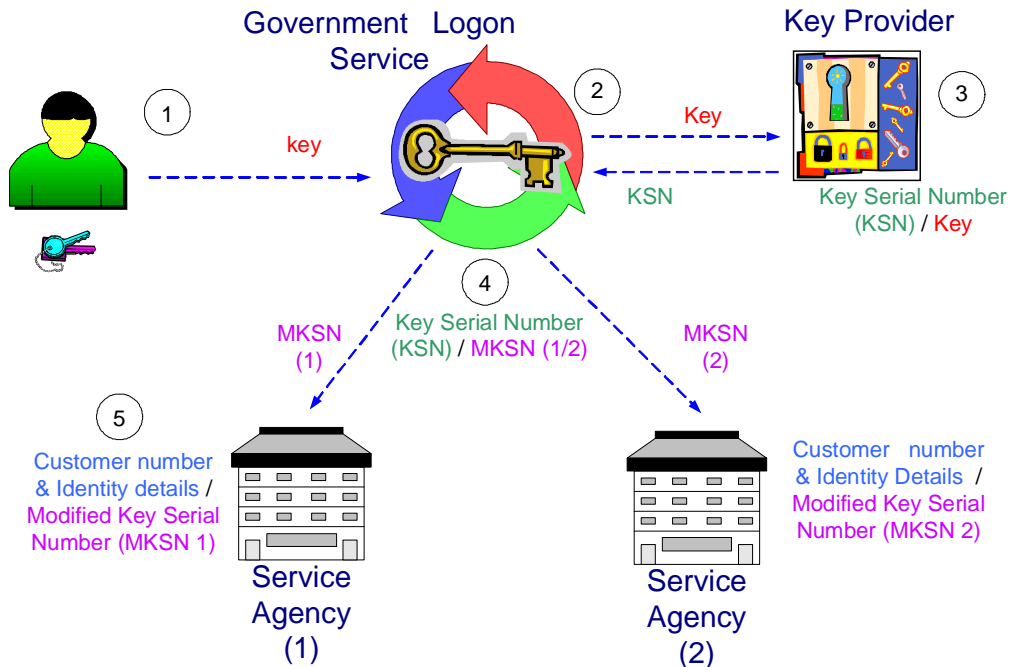


Figure 4: Repeat Service—using Modified Key Serial Numbers

The authentication steps for repeat access to a service are:

1. The service user electronically accesses a service agency, which redirects them to the Government Logon Service.

2. The service user logs on at the Government Logon Service website, The Government Logon Service sends a message to the Key Provider to validate the Key.
3. The Key Provider validates the key and sends back the Key Serial Number to the Government Logon Service.
4. The Government Logon Service sends the Modified Key Serial Number for that user -agency combination to the service agency.
5. The service agency matches the incoming Modified Key Serial Number with the service user's customer record and applies the appropriate authorisation and eligibility rules to provide the service user with controlled access to the online service.

How does the Government Logon Service design protect privacy?

Privacy is protected because the design separates the information held by each of the actors in the model. No one actor holds more than two pieces of information. The service user and the agency actually delivering the services only hold the identity data. The Government Logon Service does not hold any identity information. The following illustration shows how information is distributed among the actors.

	Key	KSN	MKSN	Identity
Key Provider	✓	✓		
Government Logon Service		✓	✓	
Service Agency			✓	✓
Service User	✓			✓

Figure 5: Who knows what?

The Government Logon Service design separates the main actors in the logon process and the information they hold. The use of derived serial numbers (Modified Key Serial Number) means limited sharing of information across actors, thus protecting the privacy of clients – a key design consideration.

Further Information

Online Authentication project – Initial Implementation

You can find further background reading on earlier phases of the Online Authentication project, 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

© Crown Copyright 2005 State Services Commission

Appendix 1: Approved policy principles for online authentication

Over the past few years State Services Commission 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. They have analysed which services provided by NZ government agencies require or are likely to require online authentication. They have also reviewed overseas examples of online authentication both for government and commercial services.

The State Services Commission's research led to a set of policy, implementation and design principles to guide the development of online authentication for NZ government. These are outlined in:

- an April 2002 Cabinet paper
(<http://www.e-government.govt.nz/authentication/cabinet-paper.asp>)
- a June 2003 Cabinet directive
(<http://www.e-government.govt.nz/authentication/cabinet-paper.asp>)

The principles from the paper and directive are listed below.

Policy principles

As per the April 2002 Cabinet paper, an NZ government online authentication solution must maintain:

- **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

As per the April 2002 Cabinet paper, any implementation of NZ government online authentication must demonstrate:

- **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 principles

As per the June 2003 Cabinet directive, any design for NZ government online authentication must include:

- **separate authentication and authorisation** – authentication (establishing/verifying identity) must remain separate from authorisation (access to/approval for services)
- **agency entitlement** – determination of entitlement to a service remains with the service agency
- **security based on SIGS** – Security in the Government Sector (SIGS) provides the security framework for authentication (see <http://www.security.govt.nz/sigs/index.html>).