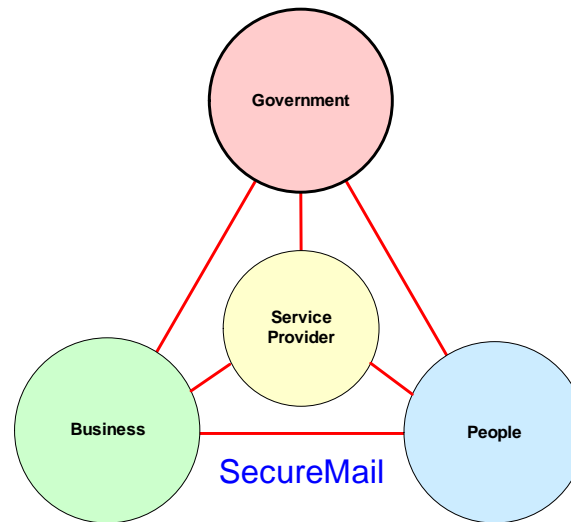


SecureMail: Blueprint

for people

May 2004



E-government Unit
State Services Commission

STATE SERVICES COMMISSION
Te Komihana O Ngā Tari Kāwanatanga



Purpose

The purpose of this blueprint is to provide **people** with an introduction to SecureMail and a high level discussion of some of the key business, legal and technical topics for its deployment and use. This blueprint is one of a set of four high-level documents intended for government agencies, service providers, businesses and people.

Background

SecureMail is an extension of an existing E-government initiative, known as SEEMail. SEEMail has been operating since 2000 and is used by over forty agencies as an approved means for the secure exchange of email and attachments over the Internet within New Zealand.

Many communications between government, businesses and people include personal in-confidence information. Communicating such information over the Internet requires sufficient security to protect the privacy and rights of an individual as well as the integrity of an organisation. SecureMail has been designed to meet this need.

Used appropriately, SecureMail provides a high level of assurance that:

- The FROM: address has not been faked (spoofed)
- No unauthorised person has read or altered the message.

An analogy is that SecureMail provides the option to send a message on letterhead paper in a sealed envelope, where previously all messages were typically sent as a postcard.

Benefits of SecureMail

Government is encouraging the use of SecureMail by people so that agencies can securely exchange messages with them.

The benefits for people using SecureMail are expected to include:

- **Convenience** - SecureMail will be an easier way for government, businesses and people to send a message, where previously they have used letters and other channels because of security concerns. Some message types that are expected to use SecureMail include:
 - *Replies* from organisations (government or business) in response to enquiries relating to personal information;
 - *Notifications*
 - from government, such as official results or reminders;
 - from business, such as statements or payslips;
 - *Transactional messages*
 - from business, as part of a business process, such as interaction with a supplier: purchase orders ⇒ invoices ⇒ remittance advices ⇒ receipt;
 - from government, as part of a process such as completing a form: form ⇒ receipt ⇒ service.

- **Improved security** – People using SecureMail will have a high level of assurance that messages are being sent and received with greater security than normal Internet email because:
 - The FROM: address has not been faked (spoofed);
 - No unauthorised person has read or altered the message.
- **Better spam control** – There is an increasing volume of messages with faked FROM: addresses generated by spammers or automated viruses. SecureMail provides a high level of assurance that the FROM: address has not been faked, meaning filters and automated rules can be applied in highly effective ways. People will be able to:
 - identify unauthenticated messages from outside of SecureMail.
 - prioritise authenticated SecureMail messages over the rest, thereby improving response times – conversely, organisations will be able to prioritise authenticated SecureMail messages, thereby improving performance for their clients.

Isn't SecureMail just email?

SecureMail involves more than using ordinary email over the Internet. SecureMail specifies, and audits against requirements that provide a high degree of security and ensure interoperability.

Security: Many communications between government, businesses and people include personal in-confidence information. The government handles and transmits such information using security standards mandated by the government's security policy manual, Security in the Government Sector (SIGS).

SecureMail specifies a set of security requirements to ensure that messages are communicated in accordance with SIGS. These requirements are imposed on any service provider who handles SecureMail.

Interoperability: SecureMail specifies a set of requirements and certifies each organisation's system, to ensure that all organisations using SecureMail are able to securely exchange messages without issue.

Auditing: The SecureMail system undergoes regular automated tests to ensure ongoing interoperability and security.

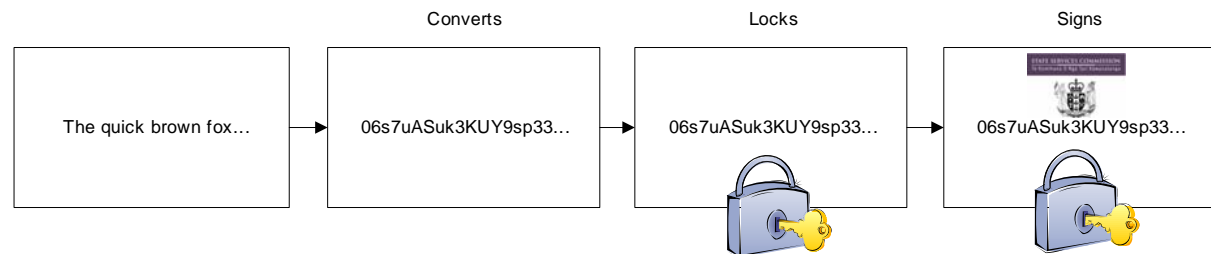
Any service provider who handles SecureMail is audited on a regular basis, to ensure compliance with their security obligations.

How does SecureMail protect a message?

SecureMail uses Internet security standards (S/MIME) to secure messages sent over the Internet between government, businesses and service providers that are SecureMail capable.

SecureMail performs the following actions for a sending organisation:

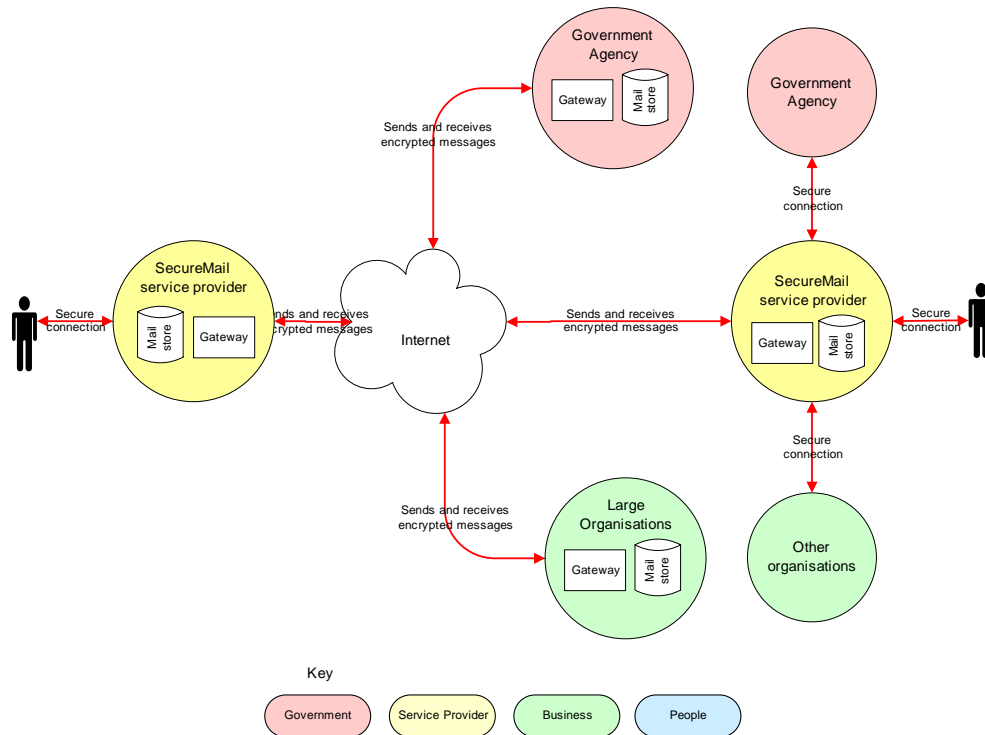
- **Converts the message** from plain text to secret code so that it can only be read by the receiving organisation;
- **Locks the message** so that any tampering can be detected; and
- **Signs the message** by the sending organisation so that the origin of the message can be proven.



SecureMail performs the following actions for a receiving organisation:

- **Checks the signature** matches the sending organisation's signature;
- **Checks the lock** to ensure the message has not been read or altered; and
- **Converts the message** from secret code back to plain text.

SecureMail system



This diagram demonstrates how the SecureMail system operates. For simplicity, multiple instances of each organisation are not shown.

On the left, it shows a person, who uses a secure connection provided by their service provider, to access a mail storage facility, and a SecureMail gateway.

On the right, the diagram shows a range of receivers.

On the top right, a large government agency can use its own Gateway to send/receive secure messages over the Internet, without any service provider intervention. Smaller government agencies send/receive secure messages via a service provider.

On the bottom right, the diagram shows how businesses and people can send/receive secure messages using a SecureMail service provider or via their own Gateway.

One configuration option for SecureMail is to only have a single government Service Provider. Effectively, this option would require the establishment of a centralised all-of-government webmail service. This option is not currently being considered, but is included for completeness.

Using SecureMail

To be able to send messages using SecureMail, a person will need to get access to a SecureMail mailbox and register their new email address with organisations they wish to securely communicate with.

Getting access

Getting access to a SecureMail mailbox is possible by several means, including

- obtaining one from a service provider; or
- using one provided by another organisation (e.g. employer); or
- using someone else's.

Option 1 - obtaining a SecureMail mailbox from a service provider – a person will need to obtain a SecureMail mailbox from an accredited SecureMail service provider. Note: Many people may have an ISP that is an accredited SecureMail service provider, in which case their ISP may be able to upgrade their existing mailbox to a SecureMail mailbox.

Your SecureMail service provider will require you to comply with a range of requirements, including:

- using a secure connection from your computer or business to the SecureMail service provider;
- protecting the security of your username and password.

Option 2 - using one provided by another organisation – some organisations may provide a SecureMail mailbox. The organisation providing the SecureMail mailbox will probably set a policy on its use.

For example, an employer may provide a SecureMail mailbox for work purposes only, because the email address contains the organisation's name. Alternatively, they may allow it to be used for personal use. In such situations, it is recommended that personal messages be classified with [PERSONAL] in the subject line. A better option is if they provide two SecureMail mailboxes, one for business and one for personal.

Option 3 – using someone else's – some people may share a SecureMail mailbox.

SecureMail does not identify the person who sent the email – it authenticates the FROM: address. If the email address has been registered with an organisation, then the person who has registered, will be liable for any transactions carried out, using that email address.

Organisations may ask a person if they share their SecureMail mailbox with anyone else (eg family member). If they do so, it may restrict the kinds of transaction that the organisation is prepared to do with the person through that email address.

Verify SecureMail address

A person who is an existing customer of an organisation and who wishes to use SecureMail to communicate will need to confirm the organisation has SecureMail, and then contact the organisation prior to sending a SecureMail message.

The person will probably have to go through a “change-of-address” process to confirm identity before they can change their contact information (from a postal address, to an email address).

The level of identification required may depend on the particular type of transaction to be carried out. In some cases, providing a form of photo ID may be required. The person's SecureMail service provider might choose to provide a service to simplify this process.

Using SecureMail

A person's SecureMail mailbox can be used to send/receive ordinary messages and SecureMail messages.

Typically a person only has to send their message like normal. SecureMail knows which recipients are SecureMail capable and will automatically lock and sign the message before sending it. If the recipient does not have SecureMail, the message will be sent **without** security. This means messages to ordinary recipients can still be read or altered by a third person.

Accountability: SecureMail does not identify the person who sent the email – it authenticates the FROM: address. Some senders may share a SecureMail email address.

In some cases, depending on the nature of the transaction, an organisation may require the user to acknowledge they are the only person using the mailbox (ie it is not a mailbox to which other people have access).

An organisation may require strong authentication, to give a higher assurance of accountability - such an organisation will have to assist clients who require this.

Topics to consider

Authentication

It is important that people protect their SecureMail mailbox access and do not share it. If the SecureMail mailbox is used for high value or high-risk transactions, then a more secure form of authentication, other than username/password, may be necessary.

People cannot authenticate themselves solely by using their SecureMail address because SecureMail only authenticates the FROM: address, not the sender.

Accountability

People are responsible for all authorised use of a SecureMail mailbox. It is important to safeguard access to the mailbox by adequately protecting the username and password.

People should not access SecureMail through insecure public access points, unless they can use a form of strong authentication, not susceptible to theft/capture, such as a one-time-password token.

Delivery receipt

SecureMail will return a delivery receipt if requested. This indicates the message has been successfully delivered, unlocked and verified by the organisation responsible for handling the receiver's messages. This feature is not a read receipt – for an important transaction, the business may have to request an acknowledgement from the receiver, that the message has come to the recipient's attention.

SecureMail Principles

A set of policy and implementation principles was used to guide the development of SecureMail:

Policy principles:

- **Security** - suitable protection must be provided for information provided by both people and the Crown.
- **Acceptability** – ensuring that the proposed 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 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 security required for government to people (G2P) transactions will vary based upon the nature of the information.

Implementation principles:

- **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 are considered, and as far as possible avoiding ‘vendor capture’.
- **Risk-based approach** – providing an approach based on agreed security 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** – 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.

Further Information

SecureMail Project

Further background reading, as well as more detailed information and progress updates, are available on the e-government website (<http://www.e-government.govt.nz/securemail/>).

Specific questions can be emailed to securemail@ssc.govt.nz or posted:

Attn: SecureMail 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.

More information about the E-government Unit (www.e-government.govt.nz) and the State Services Commission (www.ssc.govt.nz) is available online.