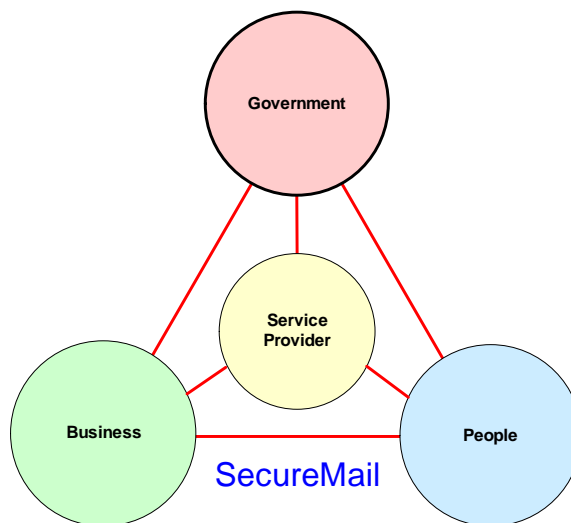


SecureMail: Blueprint

for businesses

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 **businesses** 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 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.

The case for SecureMail

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

For a business, the value proposition for providing SecureMail is anticipated to be:

- **Convenience** - SecureMail will be an easier way for government, people and business 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:
 - *Adhoc messages* from customers, such as enquiries for personal information;
 - *Notifications* to customers, such as statements or personalised promotions; and
 - *Transactional messages*, as part of a process, such as interaction with a supplier: purchase orders ⇒ invoices ⇒ remittance advices ⇒ receipt.
- **Automation of tasks** – SecureMail will help enable the development of new transactional applications. Processing of structured messages (such as invoices) can be integrated with business applications, potentially reducing the time staff spend on routine tasks.
- **Improved Service for customers** – SecureMail offers several opportunities for a business to improve service:

- 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. A business will be able to prioritise authenticated SecureMail messages over the rest, where appropriate.
- A business will be able to assure its customers that messages are being sent and received with greater security than normal Internet email.

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.

Interoperability: The secure exchange of email over the Internet is defined by a number of Internet standards, but many commercially available products, referred to as Gateways, do not work with each other (interoperate). SecureMail specifies a set of requirements to ensure that Gateways will interoperate. There is an accreditation process to ensure Gateway vendors and their products meet the SecureMail requirements.

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.

Auditing: Gateways are certified after installation, to ensure they meet SecureMail security and interoperability requirements. Certification is performed using an automated test facility. In addition, each Gateway must regularly perform automated tests to ensure ongoing interoperability and security.

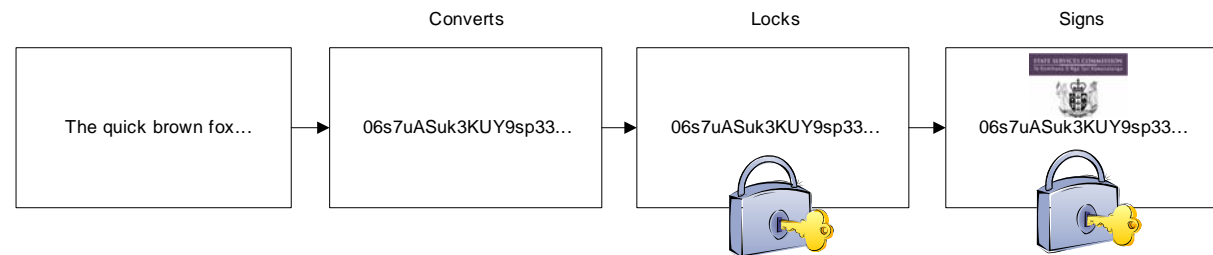
Any service provider who handles SecureMail will be audited on a regular basis, to ensure compliance with their security obligations.

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:

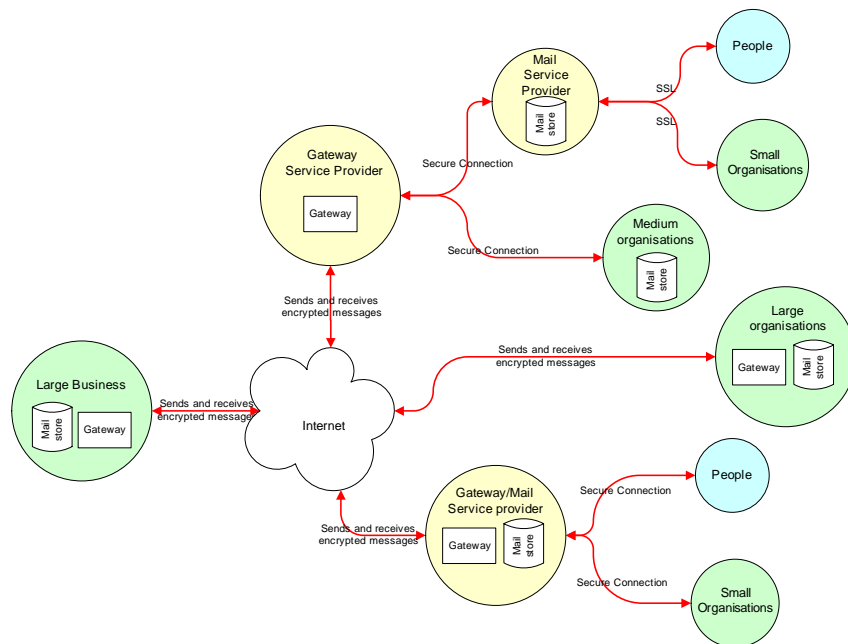
- **Converts the message** from plain text to secret code so that it can only be read by the receiving organisation;
- **Locks the message** so that any tampering can be detected; and
- **Signs the message** by the sending organisation so that the origin of the message can be proven.



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 will work for a business. For simplicity, multiple instances of each organisation are not shown.

On the left, it shows a large business using its own Gateway to send/receive SecureMail messages to the Internet. Other technical configurations for small and medium businesses are represented on the right of the diagram.

On the right, the diagram shows three types of receivers:

On the top right, a **Gateway Service Provider** provides a Gateway to a Mail Service Provider, who in turn provides mail store services to lots of people and small organisations. In addition, the Gateway Service Provider offers a gateway service to medium organisations with their own mail store.

On the bottom right, a **Gateway/Mail Service Provider** provides their own Gateway and mail store services to many people and small businesses.

On the middle right, the diagram also shows how a large organisation can use its own Gateway to send/receive secure messages over the Internet, without any service provider intervention.

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.

SecureMail deployment – an overview

Before deploying SecureMail, a business will need to consider:

- **Business and legal topics:** There will be legal and business topics to consider from a business's use of SecureMail for communicating with government, businesses and people.
- **Business processes:** A business's existing processes may need to be re-designed to work with SecureMail.
- **Technical architecture:** A business's existing technical architecture may need to be reconfigured to work with SecureMail.

To use SecureMail, a business will need to organise access, by installing its own Gateway, contracting the service from a Gateway Service Provider or obtaining a SecureMail mailbox from a Mail Service Provider.

- **OPTION 1: Own Gateway:** A business requiring its own Gateway will need to:
 - **Acquire a Gateway:** Select, install and test an accredited SecureMail Gateway. Gateways can be acquired from SecureMail accredited vendors. Once installed, the Gateway must pass site certification tests. Gateways also need to perform regular automated testing and to be upgraded in a timely fashion, as amendments to the SecureMail requirements are notified;
 - **Join SecureMail:** A business will need to sign the SecureMail Membership Agreement. This Agreement sets out the terms that apply to using SecureMail, such as complying with the SecureMail requirements;

- **OPTION 2: Contracted Gateway:** A business can use the service of a Gateway Service Provider. The Gateway Service Provider will impose SecureMail requirements for security and interoperability on the business.
- **OPTION 3: Obtaining a SecureMail mailbox:** A business can obtain a SecureMail mailbox from an accredited SecureMail service provider. Note: Many businesses may have an ISP that is an accredited SecureMail service provider, in which case, their ISP may be able to upgrade their mailbox to a SecureMail mailbox.

To deploy SecureMail, a business will need to:

- **Comply with SecureMail requirements:** Be responsible for maintaining security and interoperability in accordance with the SecureMail Membership Agreement or those terms that their Service Provider imposes on them.
- **Impose SecureMail requirements:** Impose applicable SecureMail requirements on employees and contractors, and ensure relevant security matters are reported and actioned.

To operate SecureMail, a business will need to:

- **Continue to comply with SecureMail requirements:** Continue to maintain security and interoperability in accordance with the SecureMail Membership Agreement or those terms that their Service Provider imposes on them. Where a business has its own Gateway, deploying SecureMail will also place an obligation on a business to undertake regular testing of their Gateway and to upgrade their Gateway in a timely fashion, as amendments to the SecureMail requirements are notified.

Business topics to consider

Before deploying SecureMail a business will need to consider how SecureMail will impact on its business processes. Some of the topics that need to be considered are outlined below. The topics fall into three categories:

- Topics related to using SecureMail for dealing with customers;
- Topics related to having a SecureMail Gateway; and
- Topics related to providing SecureMail for personal use, to staff and contractors.

Issues related to using SecureMail for dealing with customers

Verify SecureMail address

Existing customers who wish to use SecureMail to communicate with a business will have to go through a process to change their contact information (from a postal address, to an email address).

A business may require the mailbox holder to identify him or herself to a level sufficient for a particular type of transaction to be carried out, such as providing a form of photo ID. The mailbox holder's Mail Service Provider might choose to provide a service to simplify this process.

Customer accountability

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

In some cases, depending on the nature of the transaction, a business may require the customer to acknowledge they are the only person using the mailbox (ie it is not a mailbox to which other people have access). The customer's Mail Service Provider might choose to provide a service to simplify this process.

A business may require strong authentication, to give a higher assurance of accountability - such a business will have to assist customers who require this.

Staff obligations

Staff are responsible for all authorised use of a SecureMail mailbox. It is important to safeguard access to the mailbox 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.

Value added services

A business is free to develop value-added services as they see fit. Such services must not compromise SecureMail. In some situations, such as developing structured message formats, then a business will be encouraged to develop standards for the whole of New Zealand.

Service Level Expectation

The Internet has raised service level expectations about messages. Customer expectations need to be carefully managed to ensure realistic targets for things such as response times.

A business may need a quality assurance process to ensure consistent style and content in communications sent via paper mail, and those sent via SecureMail.

Because people and business may find it easier to send emails than to write letters, the volume of correspondence may grow. This growth may highlight or exacerbate problems with existing business processes or infrastructure.

Prioritisation of SecureMail

A business may prioritise SecureMail messages (which are likely to have a very low junk email ratio because of the authentication of the sender's email address) over non-SecureMail messages, to deal with the increasing volume junk mail.

Education

A business will need to consider what extra information and support its staff and customers need to use this new technology. For instance, it may have to advise its customers not to access SecureMail through insecure public access points, unless they can use a more secure form of strong authentication.

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.

Topics related to having a Gateway

Contact Information

A business will need generic contact information, kept up-to-date with the SecureMail administrator. This information cannot contain personally identifiable information, but rather securemailadmin@business.co.nz and a phone number.

Gateway obligations

A business running their own Gateway will be expected to maintain compliance with the SecureMail interoperability and security requirements.

They will require staff with experience in the operational issues that arise if message encryption fails. For example, if a Gateway fails, then until a new Gateway is implemented, all the arriving encrypted messages cannot be delivered. A significant upstream queuing facility may be required to store incoming messages. If the agency's decryption key is lost, then messages are useless – there must be a robust process to ensure the key is backed up securely and available in a timely fashion when required.

Sovereignty

A business must ensure SecureMail messages from government are protected for the public interest and to preserve personal privacy. To ensure New Zealand laws protect such SecureMail messages, a business will not be able to use facilities outside of New Zealand to handle SecureMail, i.e. a business is only allowed to store such messages in New Zealand and send those messages over the New Zealand part of the Internet.

Mail server obligations

A business must ensure that any SecureMail message it sends, has an authenticated FROM: address and can be linked to an accountable sender.

SecureMail has minimum standards for authentication. A business must support

username/password access to a mailbox.

Online Authentication

It is expected that any authentication mechanism used within SecureMail will be consistent with the “*Best Practice Framework for Authentication*”.

Topics related to providing SecureMail for personal use, to staff and contractors

Personal Use

A business will need to determine how its employees and contractors will use SecureMail. For example, a business may allow SecureMail for personal use. In such situations, it is recommended a separate mailbox/email address be used e.g. myname@personaluse.business.co.nz AND that information be categorised with [PERSONAL].

Each business will need to make its own evaluation of the business issues around using SecureMail.

Legal topics to consider

Before deploying SecureMail a business will need to consider how SecureMail will impact on it from a legal perspective. Some of the legal topics that need to be considered are outlined below.

Electronic Transactions

A business will need to:

- obtain consent from its customers for communications involving legal requirements that are subject to the Electronic Transactions Act;
- determine the time at which the business and the addressee legally receive SecureMail messages; and
- if SecureMail messages are used to meet existing legal requirements, assess how to achieve this purpose.

Privacy

As with any communication, SecureMail messages and associated information, such as operation logs, will be subject to Privacy Act obligations.

Crimes

If an interception, copying, accessing or interference offence is committed in relation to SecureMail messages or the associated SecureMail environment, a business should take appropriate action.

Human Rights

A business that deploys SecureMail must continue to provide alternative communication channels.

Employees/Contractors

A business must ensure that obligations are imposed on employees and contractors through agreements. Some topics to consider include ensuring that they:

- are not permitted to use SecureMail for unlawful purposes; and
- understand whether they are allowed to use SecureMail for personal

purposes.

Liability

Situations in which liability could arise include such things as security breaches, misuse of the system by authorised people and failure to perform an agreed action.

A business needs to make its own evaluation of the legal issues around using SecureMail.

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.