



## **Secure Electronic Environment (S.E.E.) Mail**

### **BUSINESS REQUIREMENTS**

**19<sup>th</sup> November 2002**

**Version 2.2**

**Document Purpose:**

This document describes the business requirements that a Gateway must meet, to be able to exchange, block and report upon messages sent between S.E.E. Mail Participating Agencies.

**Key S.E.E. Mail documents:**

Definitions

Business Requirements (this document)

Site Certification process

Product/Supplier Accreditation Process

Tests

**Further information:**

Refer to [www.see.govt.nz](http://www.see.govt.nz) for further information regarding the Secure Electronic Environment (S.E.E.)

Throughout this document the terms “[S\*\*MAIL]”, “[IN CONFID\*NC\*]”, “[S\*NSITV\*]” and “[R\*STRICT\*D]” are used. This enables the document to be e-mailed from a S.E.E. participating Agency to any non-S.E.E. organisation. Before using this document “\*” should be globally replaced with “E”

**Revision Information:**

v2.1	-	Incorporates	“Trusted	Server”	concept.
v2.1a	-	Updated	to	reference	SIGS.
v2.2 - Updated to use existing government security classifications instead of XSEEMAIL					

**Key words:**

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. (<http://www.ietf.org/rfc/rfc2119.txt?number=2119>)

MUST is typically used where non-compliance with the requirement would impact all SEEMAIL Agencies.

SHOULD is typically used where non-compliance with the requirement would only impact the implementing SEEMAIL Agency.

**Contents**

1 High Level Requirements .....5

1.1 Applicable RFCs 5

1.2 Agency Requirements 5

1.3 Implementation Requirements 6

1.4 Integration Requirements 6

1.5 Integration Requirements 6

1.6 Listserve Requirements 6

1.7 Interoperability Requirements 7

1.8 Scalability Requirements 7

1.9 Security Requirements 7

2 Implementation Details .....8

2.1 SEEMAIL Business Rules 8

2.2 Link Setup 9

2.3 Operational Requirements 9

2.4 Security Requirements 9

2.5 Self-signed Certificates 9

2.6 Certificate Naming Conventions 10

2.7 CRL Distribution Points 11

2.8 Certificate Processing 11

2.9 Sending 14

2.10 Receiving 15

2.11 Trusted Server Functionality 16

2.12 Administrator Notification 16

2.13 Documentation and Training Rules: 16

2.14 Diagnostics 17

2.15 LDAP Server Functionality 17

APPENDIX A: Guidelines for Agencies Choosing a SEEMAIL vendor .....18

Flexibility 18

Ease of Use 18

Support 18

Relationship Management 19

APPENDIX B: Guidelines for Agencies Choosing a SEEMAIL CA .....19



## High Level Requirements

Key to symbols used throughout this document:

- \* - Business requirement
- † - RFC requirement (our interpretation)
- ‡ - Government Security requirement (SIGD or GCSB)

## Applicable RFCs

1.1.1 Gateways **MUST** be compliant with the following RFCs:

RFC2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, <http://www.imc.org/rfc2459>

RFC2632 S/MIME Version 3 Certificate Handling, <http://www.imc.org/rfc2632>

RFC2633 S/MIME Version 3 Message Specification, <http://www.imc.org/rfc2633>

1.1.2 Compliance with the following RFCs is encouraged and partial compliance is required to meet S.E.E. Business requirements:

RFC2634 Enhanced Security Services for S/MIME, <http://www.imc.org/rfc2634>

RFC3183 Domain Security Services using S/MIME, <http://www.imc.org/rfc3183>

1.1.3 Where Gateways fail to interoperate, then the S.E.E. Steering Group will make a final decision, using the following order of precedence is:

S.E.E. Mail business requirements

RFC compliance

Product implementations

1.1.4 Wherever possible, Gateways **SHOULD** utilise the RFC specifications in the same manner as desktop clients.

1.1.5 Note that in certain circumstances, the S.E.E. Mail business requirements will be mandatory (**MUST**), even though the RFC only specifies an optional compliance (**SHOULD**).

## Agency Requirements

The Gateway **MUST NOT** adversely impact on the functionality of existing systems, including virus checking and content filtering software. Specifically the Gateway **MUST**:

- Permit transmission of existing non-secure e-mail;
- Permit secure e-mails containing attachments;
- Permit secure e-mails being transmitted to multiple user recipients;
- Permit transmission of individual-to-individual S/MIME messages

Each SEEMAIL Agency must be confident that:

- a) All SEEMAIL messages are secured;

A message with a SEEMAIL trigger word<sup>1</sup> will only ever be sent securely ;  
All messages between SEEMAIL Agencies authenticate the sending agency;  
Incoming and outgoing messages must be automatically suspended when the Gateway is not operational.

The Recipient in a SEEMAIL Agency must be confident that:

- a) The message is from the sending SEEMAIL Agency<sup>2</sup> as claimed;  
No one outside the sending SEEMAIL Agency has read the message;  
No one outside the sending SEEMAIL Agency has altered the message.

The Sender in a SEEMAIL Agency must be confident that:

- a) The message can only be read by the receiving SEEMAIL Agency;
- b) No one outside the receiving SEEMAIL Agency can read the message in transit;
- c) No one outside the receiving SEEMAIL Agency can alter the message.

## Implementation Requirements

The Gateway MUST require minimal implementation effort by existing SEEMAIL Agencies.

The Gateway MUST behave in a consistent and predictable manner.

The Gateway MUST notify relevant parties on exceptions.

## Integration Requirements

The Gateway MUST require no client software customisation.

The Gateway MUST support common e-mail client software.

## Integration Requirements

The Gateway MUST be able to utilise X.509 v3 certificates from any major certificate authority vendor.

The Gateway SHOULD operate on multiple platforms, such as Windows NT and Unix.

## Listserve Requirements

The Gateway MUST permit the exchange of non-secure e-mail among list-serve groups of individuals; some of whom are members of Participating Agencies and some of whom are members of non-Participating Agencies.

---

<sup>1</sup> Current SEEMAIL trigger words are “[S\*\*MAIL]”, “[IN CONFID\*NC\*]”, “[S\*NSITV\*]” and “[R\*STRICT\*D]”

<sup>2</sup> The definition of a SEEMAIL Agency is a Participating Agency who uses SEEMAIL and has current site certification.

The Gateway MUST allow the exchange of secure e-mail among list-serve groups of individuals; who are all members of Participating Agencies.

The Gateway MUST function with non-S.E.E. list-serves.

## Interoperability Requirements

The Gateway MUST interoperate with all other Accredited Software in all Participating Agencies, in a manner that complies with these business requirements.

The Gateway MUST gracefully handle ALL functions indicated in this document as being potentially supported by a communicating gateway, whether mandatory (MUST) or optional (SHOULD), i.e. the Gateway must not cause a communicating Gateway to have to be configured with optional functions switched-off because the first Gateway cannot handle the optional functions without crashing or exhibiting some other undesirable behaviour.

## Scalability Requirements

The Gateway MUST be scalable to interoperate with all Participating Agencies, up to the number of Eligible Agencies.

As per RFC822, Section 4.7.5, User-Defined-Fields:

Individual users of network mail are free to define and use additional header fields. Such fields must have names which are not already used in the current specification or in any definitions of extension-fields, and the overall syntax of these user-defined-fields must conform to this specification's rules for delimiting and folding fields. Due to the extension-field publishing process, the name of a user-defined-field may be pre-empted.

‡ The Gateway SHOULD be able to tag messages with an “X-SEEMAIL-Version” field, identifying the current SEEMAIL version e.g. “X-SEEMAIL-Version: 2.0”.

## Security Requirements

A Participating Agency MUST comply with the minimum security standards dictated by the Security In the Government Sector (SIGS) manual<sup>3</sup> and New Zealand Security of Information Technology (NZSIT) publications<sup>4</sup>.

### 1.1.6 A Participating Agency MUST

Apply a structured risk management approach

Conduct risk assessments

Avoid default installations

Test and install security patches

Review audit logs

Review applications' security coding

Maintain security documentation

---

<sup>3</sup> [www.security.govt.nz/sigs/](http://www.security.govt.nz/sigs/)

<sup>4</sup> [www.gcsb.govt.nz/nzsit/](http://www.gcsb.govt.nz/nzsit/)

A Participating Agency MUST ensure at all times it is able to pass Site Certification tests.

A Participating Agency MUST be able to add a security classification label to messages.

A Participating Agency MUST be able to recover quickly from key compromise.

A Participating Agency MUST have real time access to the logging and analysis of faults, alerts and intrusions.

A Participating Agency SHOULD be aware when their Gateway fails and how this appears to Senders.

## ***Implementation Details***

### **SEEMAIL Business Rules**

Core S.E.E. Mail functionality enables secure e-mail to be exchanged between Participating Agencies. This type of email is termed "SEEMAIL".

The Gateways of Eligible Agencies using SEEMAIL are certified, to ensure secure e-mail is handled consistently. The list of site certified Agencies will be made available in an LDAP 3.0 directory, indexed by DN and e-mail address. This is the SEEMAIL list.

With S.E.E. Mail version 2, functionality has been extended, so that secure e-mail can be exchanged with Trusted Agencies and Individuals<sup>5</sup> who are not site certified. These Agencies/Individuals will be contained within an Administrator approved list controlled by the sending agency. This is the 'TRUSTED' list.

Agencies using this extended functionality accept the risk that sensitive e-mail messages could be handled in an insecure manner by the receiving agency e.g. a staff member auto-forwards it to a Hotmail account, and therefore make their own business decision, according to SIGS guidelines, about who to trust and exchange keys with.

Note: Agencies may choose to maintain more than one 'TRUSTED' list to represent who can send/receive messages tagged "[IN CONFID\*NC\*]", "[S\*NSITV\*]" or "[R\*STRICT\*D]". This is outside the scope of S.E.E. Mail.

1.1.7 \* The trigger word WILL be one or more of "[S\*\*MAIL]", "[IN CONFID\*NC\*]", "[S\*NSITV\*]" or "[R\*STRICT\*D]"

\* The trigger word(s) MUST be recognised in any combination of UPPER or lower case e.g. [S\*\*mAiL].

\* Any combination of left-hand, right-hand square "[ " or squiggly "{ " brackets, including non-matching brackets MUST be recognised e.g. "{S\*\*mail}"

\* Mail containing the trigger word(s) must ONLY be delivered to:

- a) a Participating Agency, as defined in the SEEMAIL list;
- b) a Trusted Agency/Individual as defined in the TRUSTED list;

\* Gateways MUST handle a message containing the trigger word(s) consistently.

---

<sup>5</sup> Note: Currently most client e-mail software does not recognise the use of domain gateway signing. They typically warn that the sender's e-mail address (you@youragency.govt.nz) does not match the certificate e-mail address (domain-signing-authority@youragency.govt.nz). This may prevent replying to the sender. Outlook 2000 SR-1 with appropriate patches can work.

## Link Setup

- \* The Gateway **MUST** allow asynchronous setup and maintenance of SEEMAIL links.

## Operational Requirements

- \* A Participating Agency **MUST** comply with the S.E.E. PKI Certificate Policy v1.91 Operational Requirements, as detailed in Section 4.7 – Key Changeover:

Certificates must have an expiry date of no longer than THIRTEEN months after the issue date.

A new key pair must be generated for the replacement certificate if the existing key pair has been in use for FOUR years or more (i.e. key lifetime period must be no more than FIVE years).

## Security Requirements

⌘ A Participating Agency **MUST** place their Gateway inside a tightly configured firewall certified to EAL4 or better, or E3 or better on the UK ITSEC scale, and configured to allow only the protocols and commands required for the operation of the required service(s).

⌘ A Participating Agency **MUST** protect Gateway private keys at all times, from any unauthorised access, disclosure or tampering.

⌘ A Participating Agency **MUST** ensure all media used for the storage of Gateway private keys is sanitised by overwriting or degaussing as described in NZSIT207: Declassification of Storage Media, or destroyed before it is released from the Participating Agency's control.

⌘ Agencies **SHOULD** request a public key pair created with a hardware key pair or seed generator.

\* Gateways **MUST** check the authenticity of any message before relying on it.

⌘ Gateways **MUST** only send messages using an approved algorithm.

⌘ Gateways **MUST** support the following approved algorithms: Triple-DES, RSA-1024/2048 and SHA-1.

⌘ Gateways **SHOULD** support the following approved algorithm: Advanced Encryption Standard (AES) with 128, 192 and 256-bit key lengths.

⌘ Gateways **MUST** always use the highest approved encryption algorithm supported by both Gateways.

⌘ Gateway crypto modules **MUST** be FIPS140 evaluated.

⌘ Gateways **SHOULD** be Common Criteria evaluated to an Evaluation Assurance Level (EAL) of 3 or higher, by the Australasian Information Security Evaluation Programme (AISEP) or equivalent.

## Self-signed Certificates

As per RFC2632, Section 2.3, (Self-signed certs need other mechanisms to establish trust. This is not scalable)

Agents **MAY** send CA certificates, that is, certificates that are self-signed and can be considered the "root" of other chains. Note that receiving agents **SHOULD NOT** simply trust any self-signed certificates as valid CAs, but **SHOULD** use some other mechanism to determine if this is a CA that should be trusted. Also note that in the case of DSA certificates the parameters may be located in the root certificate. This would require that the recipient possess the root certificate in order to perform a signature verification, and is a valid example of a case where transmitting the root certificate may be required.

⌚ Agencies MUST use a Certificate Authority (CA) issued certificate.<sup>6</sup> Agencies MUST NOT use a self-signed certificate for S.E.E. Mail.

## Certificate Naming Conventions

As per RFC2632, Section 3, Using Distinguished Names for Internet Mail -

End-entity certificates MAY contain an Internet mail address as described in [RFC-822]. The address must be an "addr-spec" as defined in Section 6.1 of that specification. The email address SHOULD be in the subjectAltName extension, and SHOULD NOT be in the subject distinguished name.

Receiving agents MUST recognize email addresses in the subjectAltName field. Receiving agents MUST recognize email addresses in the Distinguished Name field in the PKCS #9 emailAddress attribute.

As per RFC2632, Section 4.4.3, Subject Alternative Name Extension -

The subject alternative name extension is used in S/MIME as the preferred means to convey the RFC-822 email address(es) that correspond to the entity for this certificate. Any RFC-822 email addresses present MUST be encoded using the rfc822Name CHOICE of the GeneralName type. Since the SubjectAltName type is a SEQUENCE OF GeneralName, multiple RFC-822 email addresses MAY be present.

⌚ Agencies MUST use either:

- a) one DCA certificate (for encryption and signing)<sup>7</sup> OR
- b) one or more DCA certificate(s) (for encryption and signing) with multiple RFC822 DCA e-mail addresses for every unique domain in the Subject Alternative Name Extension of the certificate

As per RFC3183, Section 4.1, Domain Confidentiality Naming Conventions -

A DCA MUST be named 'domain-confidentiality-authority'. This name MUST appear in the 'common name (CN)' component of the subject field in the X.509 certificate. Additionally, if the certificate contains an RFC 822 address, this name MUST appear in the end entity part of the address, i.e., on the left-hand side of the '@' symbol.

Along with this naming convention, an additional naming rule is defined: the 'name mapping rule'. The name mapping rule states that for a DCA, the domain part of its name MUST be the same as, or an ascendant of (as defined in section 3.1.1), the domain name of the set of entities that it represents.

⌚ If a single DCA certificate is used for both signing and encrypting, Gateways MUST comply with RFC3183, Section 4.1 Domain Confidentiality Naming Conventions.

⌚ IF a Gateway uses separate certificates for signing and encryption, then the signing certificate MUST comply with RFC3183, Section 4.1 Domain Confidentiality Naming Conventions.

⌚ Gateways MUST ensure that the domain part of an e-mail MUST be the same as or an ascendant of, either the SubjectAltName.rfc822Name or PKCS#9 emailAddress in the signer's certificate.

As per RFC3183, Section 3.1.1 –

The following naming conventions are specified for agents generating signatures specified in this document:

---

<sup>6</sup> RFC2632, Section 2.3. Self-signed certs need other mechanisms to establish trust. This is not scalable

<sup>7</sup> Note: We are optionally allowing the use of domain-confidentiality-authority certificates for signing as well as encryption. This violates RFC3183, but as far as we know works with all the products we are using. In the longer term using two keys will be better, particularly when/if clients support domain-signing & encryption correctly.

- For a domain signature, an agent generating this signature MUST be named 'domain-signing-authority'
- ...
- This name shall appear as the 'common name (CN)' component of the subject field in the X.509 certificate. There MUST be only one CN component present. Additionally, if the certificate contains an RFC 822 address, this name shall appear in the end entity component of the address - on the left-hand side of the '@' symbol.

⌘ IF a Gateway uses separate certificates for signing and encryption, then the encryption certificate MUST comply with RFC3183, Section 3.1.1 Naming Conventions.

Gateways MUST generate a warning, if the addresses do not match or the certificate does not contain any email address.

## CRL Distribution Points

As per RFC2459, Section 4.2.1.14, CRL Distribution Points -

The CRL distribution points extension identifies how CRL information is obtained. The extension SHOULD be non-critical, but this profile recommends support for this extension by CAs and applications.

⌘ The certificate MUST contain a CRL distribution point to enable the Gateway to verify whether it has been revoked or not.

\* Participating Agencies MUST maintain a S.E.E. Manager list of trusted CA root-keys. Agencies MAY add other CA root-keys if they require.

\* Participating Agencies MUST implement S.E.E. Key server certificates, when they become available, on the next renewal of their key.

## Certificate Processing

### Principles:

Fail safe

Allow for faulty implementations

Allow for transition issues (e.g. certificate expires while message is in transit)

Allow for the use of certificates from outside of S.E.E. Mail

As per RFC2632, Section 5 -

Some of the many places where signature and certificate checking might fail include:

- no Internet mail addresses in a certificate match the sender of a message
- no certificate chain leads to a trusted CA
- no ability to check the CRL for a certificate
- an invalid CRL was received
- the CRL being checked is expired

- the certificate is expired
- the certificate has been revoked
- the certificate has not yet been issued (system date is earlier than issue date)

There are certainly other instances where a certificate may be invalid, and it is the responsibility of the processing software to check them all thoroughly, and to decide what to do if the check fails.

☞ Gateways **MUST** always verify whether the certificate is valid, and must verify whether any of the failures listed in 2.8.3 have occurred.

☞ Gateways **MUST** provide a meaningful notification capability for invalid instances, and use the S.E.E. Mail Messages (as defined in S.E.E. Mail Tests).

1.1.8 \* Gateways **SHOULD** handle certificates in a consistent manner, as follows:

Result abbreviations: S = Sender, R = Recipient, RA = Recipient Administrator, SA = Sender Administrator

Other agency's certificate is ...	Sending a message (encrypting)	Receiving a message (verifying)
<b>Valid</b>	Pass message through.	Pass message through.
<b>Revoked / Suspended</b>	Auto-discover valid public key certificate (LDAP).  Success: Pass message through. Fail: Hold message. Notify S, SA.	Generate hard warning to R: "Certificate revoked/suspended - message integrity uncertain". Deliver message.  Notify RA.
<b>Untrusted / Unknown CA</b>	Auto-discover valid public key certificate (LDAP).  Success: Pass message through. Fail: Hold message. Notify S, SA.	Generate hard warning to R: "Certificate unknown - message integrity uncertain". Deliver message.  Notify RA.
<b>Expired</b>	Auto-discover valid public key certificate (LDAP).  Success: Pass message through. Fail: Hold message. Notify S, SA.	Generate soft warning to R:  "Certificate expired - message integrity uncertain". Deliver message.  Notify RA.
<b>Unknown Status (CRL unavailable)</b>	Send message. Notify SA.	Generate soft warning to R:  "Certificate status could not be checked - message integrity uncertain". Deliver message.  Notify RA.

Refer to Administrator Notification section for other relevant information.

At this stage, digital time stamping is NOT required, i.e. we are not dealing with possibilities such as the malicious back-dating of messages to match an expired key that was obtained somehow.

As per RFC2459, Section 4.2.1.14, CRL Distribution Points -

The CRL distribution points extension identifies how CRL information is obtained. The extension SHOULD be non-critical, but this profile recommends support for this extension by CAs and applications.

1.1.9 † Gateways MUST be able to retrieve CRLs automatically from a CRL distribution point extension in the relevant certificate.

As per RFC2633, Section 4, 4. Certificate Processing -

A receiving agent MUST provide some certificate retrieval mechanism in order to gain access to certificates for recipients of digital envelopes. This memo does not cover how S/MIME agents handle certificates; only what they do after a certificate has been validated or rejected. S/MIME certification issues are covered in [CERT3].

At a minimum, for initial S/MIME deployment, a user agent could automatically generate a message to an intended recipient requesting that recipient's certificate in a signed return message. Receiving and sending agents SHOULD also provide a mechanism to allow a user to "store and protect" certificates for correspondents in such a way so as to guarantee their later retrieval.

As per RFC2632, Section 4 -

Receiving and sending agents SHOULD also provide a mechanism to allow a user to "store and protect" certificates for correspondents in such a way so as to guarantee their later retrieval. In many environments, it may be desirable to link the certificate retrieval/storage mechanisms together in some sort of certificate database. In its simplest form, a certificate database would be local to a particular user and would function in a similar way as a "address book" that stores a user's frequent correspondents. In this way, the certificate retrieval mechanism would be limited to the certificates that a user has stored (presumably from incoming messages). A comprehensive certificate retrieval/storage solution may combine two or more mechanisms to allow the greatest flexibility and utility to the user.

For instance, a secure Internet mail agent may resort to checking a centralised certificate retrieval mechanism for a certificate if it cannot be found in a user's local certificate storage/retrieval database.

1.1.10 † Gateways MUST provide a way to store and retrieve certificates it knows about, and hold them for later use.

1.1.11 † Gateways SHOULD add or update their certificate stores by detecting previously unknown but currently trusted domain certificates in e-mail received.

† Gateways MUST be capable of an automatic process for retrieving and using the appropriate certificate, for the following purposes:

- (a) When it wishes to send another Gateway an encrypted message and does not have a current certificate for that Gateway.
- (b) When it needs a new valid public key certificate from its CA

1.1.12 † An LDAP query to be the primary mechanism, as this is a standard, scaleable approach. The query SHOULD retrieve the certificate by setting a 'search base' to "C=NZ", filtering on the unique gateway e-mail address, domain-confidentiality-authority@agency.govt.nz and requesting the 'usercertificate' attribute to the entry that is found.

1.1.13 ¶ A signed e-mail request is a mandatory fallback mechanism if an LDAP directory is unavailable. The request MUST be sent to a special e-mail address i.e. domain-certificate-request@youragency.govt.nz. The subject line MUST be the e-mail address of the target certificate. The certificate MUST be returned as a commonly used binary encoded certificate attachment e.g. \*.cer or \*.crt OR a PKCS#7 container e.g. \*.p7b or \*.p7c.

¶ The administrator MUST be able to EITHER fully automate SEEMAIL key discovery if the Gateway can verify against the SEEMAIL List, OR require a manual approval step, dependant upon their preference.

As per RFC2632, Section 4.4.3, Subject Alternative Name Extension -

The subject alternative name extension is used in S/MIME as the preferred means to convey the RFC-822 email address(es) that correspond to the entity for this certificate. Any RFC-822 e-mail addresses present MUST be encoded using the rfc822Name CHOICE of the GeneralName type. Since the SubjectAltName type is a SEQUENCE OF GeneralName, multiple RFC-822 email addresses MAY be present.

¶ The Gateway MUST be able to load and utilise multiple RFC-822 e-mail addresses defined in a certificate.

As per RFC3183, Section 4.2 – Key Management for DCA Encryption

Gateways SHOULD support LDAP v3.0.

1.1.14 ¶ Gateways MUST support LDAP v3.0.

\* Gateways MUST be able to queue failed messages and send a warning message, to enable the administrator to manually repair the problem and release the queued messages, dependant upon the administrator's preference. Senders SHOULD be notified when an e-mail can not be delivered in a consistent manner to non S.E.E. delivery failures. e.g. Remote mail server is down, will keep trying for another 67 hours

Gateways SHOULD be able to store LDAP specifications for automatic certificate retrieval e.g.

The Gateway would store an LDAP specification for each trusted CA directory.

When the Gateway needs to use a certificate that is Expired, Revoked or Suspended it should use these LDAP specifications to attempt to auto-discover a renewed or re-issued certificate.

This procedure MAY also be used to discover non SEEMAIL domain security gateways, e.g. discovering a certificate for encryption as in 2.10.7

## Sending

\* Gateways MUST sign / encrypt all messages to an Agency, with no exceptions e.g. non-delivery response receipts, delivery receipts, etc.

As per RFC2632, Section 1, Overview -

...Before using a public key to provide security services, the S/MIME agent MUST certify that the public key is valid.

¶ Gateways MUST check that a public key is valid before using it to provide security services.

As per RFC2632, Section 4.2, Certificate Chain Validation -

In creating a user agent for secure messaging, certificate, CRL, and certificate chain validation SHOULD be highly automated while still acting in the best interests of the user. Certificate, CRL, and chain validation MUST be performed as per [KEYM] when validating a correspondent's public key. This is necessary before using a public key to provide security services such as: verifying a signature; encrypting a content-encryption key (ex:

RSA); or forming a pairwise symmetric key (ex: Diffie-Hellman) to be used to encrypt or decrypt a content-encryption key.

✧ Gateways MUST use a valid certificate to sign messages.

✧ Gateways MUST use a valid certificate to encrypt messages.

As per RFC2632, Section 2.3, CertificateSet -

Sending agents SHOULD include any certificates for the user's public key(s) and associated issuer certificates. This increases the likelihood that the intended recipient can establish trust in the originator's public key(s). This is especially important when sending a message to recipients that may not have access to the sender's public key through any other means or when sending a signed message to a new recipient. The inclusion of certificates in outgoing messages can be omitted if S/MIME objects are sent within a group of correspondents that has established access to each other's certificates by some other means such as a shared directory or manual certificate distribution.

✧ Gateways MUST send a valid public key certificate with every signed message.

✧ Gateways MUST include the S/MIME capability attribute with every signed message.

✧ Gateways MUST be able to sign and/or encrypt e-mail to a non SEEMAIL entity if its certificate store contains a valid domain certificate for the recipient.

## Receiving

As per RFC2632, Section 2.3, CertificateSet -

Receiving agents MUST be able to handle an arbitrary number of certificates of arbitrary relationship to the message sender and to each other in arbitrary order. In many cases, the certificates included in a signed message may represent a chain of certification from the sender to a particular root. There may be, however, situations where the certificates in a signed message may be unrelated and included for convenience.

✧ Gateways MUST use the public key certificate sent with a signed message to verify the signature on that message.

As per RFC2632, Section 2.3, CertificateSet -

Receiving S/MIME agents SHOULD be able to handle messages without certificates using a database or directory lookup scheme.

✧ Receiving S/MIME gateways SHOULD be able to handle messages without certificates by retrieving the relevant certificates using a database or directory lookup scheme

As per RFC2633, Section 4.2, Incoming -

...certificates and CRLs SHOULD be cached for use in chain validation and optionally stored for later use...

✧ Gateways SHOULD determine if the public key certificate with a signed message, for a domain, is different from that in the key store, and update the local store.

As per RFC2633, Section 2.7.1 -

The list of capabilities SHOULD be stored for future use in creating messages...

✧ Gateways SHOULD cache S/MIME capabilities from received messages for future use.

\* Gateways SHOULD automatically determine the highest available encryption algorithm and key length from a received e-mail using the S/MIME capability attribute.

- \* Gateways MUST handle messages encrypted or signed with expired or revoked key pairs.
- \* Gateways MUST accept messages (including unsigned messages), encrypted with its DCA-public key, from an unknown source.
- \* Gateways MUST be able to strip DSA certificates from incoming e-mail where CN=domain-signing-authority.
- \* Gateways MUST be able to strip DCA certificates from incoming e-mail where CN=domain-confidentiality-authority.

## Trusted Server Functionality

- \* A Participating Agency MAY establish a "Trusted Listserv" ruleset, and use this as the basis to downgrade Warning 2B (unverified sender) from a HARD warning, to a SOFT warning.
- \* A Participating Agency MAY establish a "Trusted Server" ruleset, and use this as the basis to downgrade Warning 2B (unverified sender) from a HARD warning, to a SOFT warning. (This ruleset is typically used for agencies with external servers, wishing to receive e-mail status reports).

It is recommended that Participating Agencies reliably identify servers on their "Trusted e.g. by IP address rather than e-mail address alone.

## Administrator Notification

### Principles:

Implement notifications in such a way as to minimize the impact on service / performance e.g. don't send an error e-mail notification for every failed message

Implement notifications in such a way as to avoid loops e.g. don't send an error message to a sender administrator, if the message will create additional incorrect messages back to you.

\* Each Participating Agency MUST have a valid "postmaster@youragency.govt.nz" account, to send exception messages and accept notifications.

\* The Gateway MUST ensure exception / notification messages are addressed "from" a valid "postmaster@youragency.govt.nz" account.

\* The Gateway MUST ensure a rule for inbound messages, where the message is "from" postmaster, does not send an exception message (to avoid loops).

\* The Gateway SHOULD allow the administrator to specify audit log and/or e-mail notifications, and their frequency, as some failures could cause a log/mail notification storm.

\* The Gateway MUST ensure rules for inbound messages do not send exception messages to postmaster of the sending agency

## Documentation and Training Rules:

\* New Participating Agencies SHOULD provide user education material and publicise S.E.E. Mail when their agency joins.

---

8 This account has been defined by Government Website Design Guidelines, for technical e-mail purposes.

\* Participating Agencies SHOULD instruct new staff on the appropriate use of the SEEMAIL trigger words within 14 days of activating an e-mail account for them.

\* Desired outcomes: Staff SHOULD know that:

- All e-mail between their Agency and a Participating Agency is signed and encrypted, and where to view the SEEMAIL list;
- A Participating Agency has been site certified, which means the handling of e-mail under different conditions has been tested and verified to work correctly;
- All e-mail between their Agency and an Trusted Agency/Individual is signed and encrypted, and where to view the TRUSTED list;
- A Trusted Agency/Individual has NOT been site certified, there is NO assurance as to the handling of e-mail once it has been received.
- Any e-mail with a SEEMAIL trigger word will only be sent, if it can be delivered signed and encrypted

\* A Participating Agency SHOULD update any applicable documentation and inform staff, when they create a secure relationship with a new Participating Agency or Trusted Agency/Individual.

## Diagnostics

\* Each Participating Agency, Supplier and Candidate MUST establish a “seemail-ping” automated e-mail responder for diagnostic purposes.

\* Seemail-ping MUST operate before any other SEEMAIL business rules and not invoke them.

\* The seemail-ping MUST auto-respond with a signed/encrypted reply to a message that is signed (and/or encrypted) using a domain certificate issued by a trusted CA.

\* Seemail-ping MUST respond with the SEEMAIL version number, gateway software name/version number and SHOULD respond with the list of SEEMAIL agencies it knows about

## LDAP Server Functionality

\* Each Participating Agency, Supplier and Candidate MUST provide and maintain a current certificate or certificate URL to the LDAP server.

\* The LDAP server WILL have a list of agencies as \*@domain

\* The LDAP server WILL have two lists: SEEMAIL and VENDOR

\* If a Participating Agency, Supplier and Candidate turns off or otherwise removes domain level e-mail security, they MUST be removed from the SEEMAIL LIST or VENDOR list.

## ***APPENDIX A: Guidelines for Agencies Choosing a SEEMAIL vendor***

The following areas will seriously impact the return on investment in a SEEMAIL system as they affect issues such as training, maintenance, system configuration, integration and of course future growth in user numbers. These issues can make the cost of ownership of a SEEMAIL system higher than the initial implementation cost and therefore need to be considered in the evaluation phase.

### **Flexibility**

Compliance with S.E.E. Mail business requirements – complies with all the MUSTs, and many of the SHOULDs

Interoperable with existing systems e.g.

Mail products, including (where appropriate) e-mail server and client software, web servers, virus scanning and content filtering software and firewall software

Encryption products or protocols, operating systems and web servers

Interfaces

Directory servers

Uses open, standard interfaces such as LDAP

SMTP functionality

SMTP mail relay in product (allows sending e-mail with reliance on other products)

Fully configurable SMTP input/output ports (if constraints, what constraints?)

Ability to interact with individual e-mail clients

Can exchange secure e-mail with individual-to-gateway

Can exchange secure e-mail with gateway-to-individual

Can handle individual signing and encryption

### **Ease of Use**

Simple management by non-technical personnel, who do not understand the intricacies of cryptographic algorithms, keys and signatures

Automates certificate management and secure links wherever possible

Intuitive interface

Sensible audit logging and error reporting (doesn't create notification "storms")

### **Support**

Availability of online support

Availability of support in Wellington

Availability of support in New Zealand  
Service levels of technical helpdesk  
Alert service for security / product updates

## Relationship Management

Any proposed contractual documentation  
Financial stability  
Reference sites, preferably another SEEMAIL site

### ***APPENDIX B: Guidelines for Agencies Choosing a SEEMAIL CA***

Participating Agencies SHOULD ensure that their CA provides at least a five-day overlap between certificate renewal and expiry of existing certificates, to provide sufficient time for old certificates to be renewed without incurring a significant outage.

Provide a full range of interfaces to the CRL e.g. file, LDAP or OCSP

Note: With regards LDAP, there is no guaranteed common LDAP schema standard for all CAs. For BaycorpID, a certificate is easily found in their directory by setting the 'search base' to c=NZ, filtering on the e-mail address (domain-confidentiality-authority@agency.govt.nz), then requesting the 'usercertificate' attribute of the entry that is found.

Provide a 'search base', 'filter spec', and certificate attribute name (e.g. 'usercertificate') by means of which certificates can be retrieved. (Note that the filter spec may be the entire distinguished name).