

New Zealand Secure Email Requirements v1.0

These requirements are PROVISIONAL – still subject to formal consultation and amendment with the Secure Email community.

Sections in **YELLOW** are highlighted as areas that will probably require greater discussion with the Secure Email community.

Sections transferred from the SEEMail Requirements, have been amended with “track changes” on, to assist the SEEMail community in noting the differences.

Any enquiries should be directed to email: securemail@ssc.govt.nz or write to:

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

10 April 2005

Version 1.0

Contents

Introduction	7
Background	7
Purpose	8
Further information:	10
Definitions	11
SecureMail Definitions	11
Technical Definitions	11
Generic Gateway Requirements	11
RFC Requirements	11
Implementation Requirements	11
Integration Requirements	11
Interoperability Requirements	11
Security Requirements	11
Trigger Word Requirements	11
Certificate Handling Requirements	11
Certificate Handling Requirements (cont)	11
LDAP Requirements	11
Secure Email Sending Requirements	11
S/MIME Sending Requirements	11
Secure Email Receiving Requirements	11
S/MIME Receiving Requirements	11
Timekeeping Requirements	11
Agency-Specific Requirements	11
Gateway Administrator Notification	11
Diagnostics	11
Record Keeping Requirements	11
SEEMail Requirements	11
SEEMail Participating Agency Requirements	11
Security Requirements	11
Exception Requirements	11
SEEMail Gateway Requirements	11
SEEMail Trigger Words	11
SecureMail Requirements	11
SecureMail Gateway Requirements	11
SecureMail Trigger Words	11
SecureMail – Generic Service Provider Requirements	11

Sovereignty Requirements 11

Accreditation Requirements 11

Security Requirements 11

User Authentication Requirements 11

Duty of Care Requirements 11

Timekeeping Requirements 11

Minimum Customer Service Requirements 11

Contact Information Requirements 11

Reporting Requirements 11

Lawful Interception Requirements 11

SecureMail – Mail Service Provider Requirements 11

 Authentication Requirements 11

 Mail Service Provision Requirements 11

 Minimum Customer Service Requirements 11

 Value-Added Service Requirements 11

 Minimum Customer Training Requirements 11

Certification Authority (CA) Requirements 11

 Security Requirements 11

 Certificate Requirements 11

 LDAP updates 11

Participating Agency Requirements 11

 Principles 11

 Lawful Requirements 11

 Interoperability Requirements 11

 Security Requirements 11

 Certificate Requirements 11

 Documentation and Training Recommendations 11

 Postmaster Configuration 11

 Notification Requirements 11

 ETA Requirements 11

Centralised Infrastructure Requirements 11

 LDAP Server Requirements 11

 LDAP Service Provision Requirements 11

 SMARTS Server Requirements 11

Deleted requirements 11

 Listserve Requirements 11

Introduction

Background

In 2000, the New Zealand government implemented Internet security standards (S/MIME) to secure messages sent over the Internet between government agencies. SEEMail is currently used by over forty government agencies as a means for the secure exchange of email and attachments using the Internet.

In 2004, the E-government Unit initiated a project, SecureMail, to extend the SEEMail concept, to include secure email communications between government, businesses and people. The SecureMail project has developed a set of complementary requirements, to enable the functioning of SecureMail, alongside SEEMail.

These requirements fit within a wider set of requirements termed the 'New Zealand Secure Email' system, which describe the centralised infrastructure and relationships between the parts of the system.

Purpose

This document describes the New Zealand Secure Email system, and outlines the requirements for each of its components and interfaces, specifically:

- Gateway Requirements
 - SEEMail Gateway Requirements – Any Gateway sending IN-CONFIDENCE and SENSITIVE email in accordance with SEEMail business requirements
 - SecureMail Gateway Requirements – Any Gateway sending IN-CONFIDENCE email in accordance with SecureMail business requirements
 - Interface between SEEMail and SecureMail Gateways (note: it is possible for a single Gateway to be certified for both SEEMail and SecureMail)
- Certification Authority (CA) Requirements
- Participating Agency Requirements
 - SEEMail Accreditation Requirements – Government agencies bound by SIGS and sending IN-CONFIDENCE and SENSITIVE email in accordance with SEEMail business requirements
 - SecureMail Accreditation Requirements – Any agency sending IN-CONFIDENCE email in accordance with SecureMail business requirements
- Interoperability Reference Test Requirements

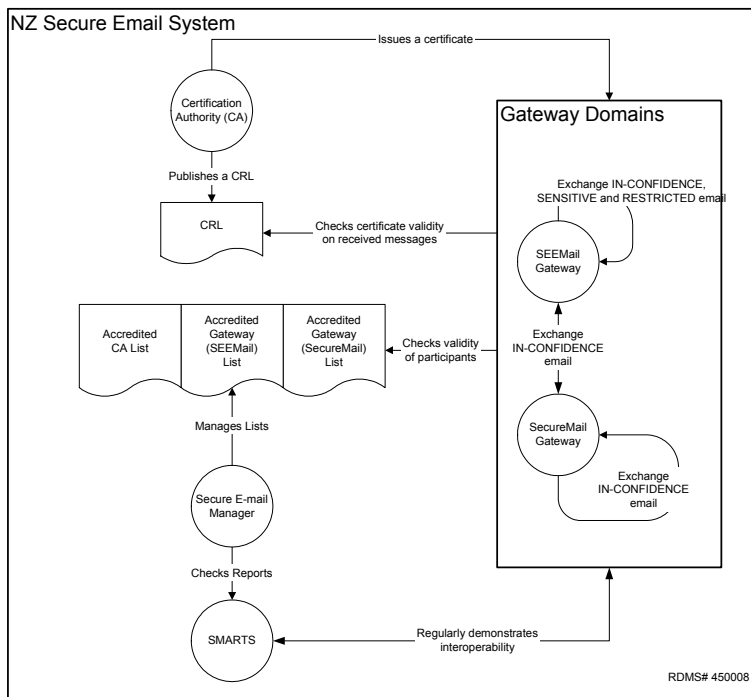
Formatted: Bullets and Numbering

Formatted

Formatted

Formatted: Bullets and Numbering

Formatted



Further information:

Requirement annotations: Key to symbols used throughout this document:

- {B Req} - Business requirement
- {RFC} - RFC requirement (our interpretation)
- {S Req} - Government Security requirement (SIGD or GCSB)

RFC Key words: The 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.

Note that in certain circumstances, the Secure Email business requirements will be mandatory (MUST), even though the RFC only specifies an optional compliance (SHOULD).

Revision Information: This document is based upon the SEEMail Business Requirements v2.5.

Definitions

SecureMail Definitions

Accreditation Authority	Accredits SecureMail Vendors, products and Gateways for compliance with the SecureMail requirements.
Administrator	Administers the SecureMail Directory and acts as the Accreditation Authority and the Certificate Authority.
Business	An entity in any form (e.g. company, incorporated society, partnership, sole trader, trust) that carries on business or business-like activities.
Gateway	A system that secures and processes messages to the SecureMail standard.
GSP - Gateway Service Provider	A Business that provides Gateway services.
Government Agency	Departments, Crown entities, and any organisation within the State sector.
Individual	A natural person.
Interception Agency	A Government Agency that have interception and search/seizure powers.
ISP – Internet Service Provider	A Business that provides Internet services.
Mail Server	A server that processes and stores email.
MSP - Mail Service Provider	A Business that provides Mail services.
Organisation	A Government Agency or Business.
Plain-text message	A message that is not encrypted.
Regulator	A Government Agency that regulates the Administrator and sets policy, standards and measures compliance with those policies and standards.
Role	Different legal personas that a person can take on (e.g. individual, trustee, etc).
SecureMail environment	The environment complying with the SecureMail requirements for security

	and interoperability.
SecureMail mailbox	A mailbox within a domain name recorded in the Directory.
SecureMail Membership Agreement	The agreement that sets out the obligations of the Administrator and all Organisations with Gateways.
SecureMail Service Provider	Provides Gateways and/or SecureMail mailboxes.
SecureMail standards	The standards to which an Organisation with a Gateway must comply.
SecureMail user	An Organisation or Individual that uses the SecureMail environment.
SecureMail Vendor	Provides SecureMail software and support.
Service Agency	The Government agency responsible for delivering an e-service to a person.
Service Provider	A Business that provides a Gateway and/or Mail Service.

Technical Definitions

Certificate	A Digital Certificate is a digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. A Digital Certificate is a data structure used in a public key system to bind a particular, authenticated individual to a particular public key.
Certificate Authority	Issues Certificates to Government Agencies, SecureMail Service Providers and Businesses that have an accredited Gateway.
Directory	Records the domain names, digital certificates and public keys of all Government Agencies, SecureMail Service Providers and Businesses that can use SecureMail.
Domain name	A name following the standard used to locate an organisation or other entity on the Internet, based on RFC1034, RFC1035.

Encrypted message	A message that has been encrypted.
e-GIF standards	The New Zealand E-government Interoperability Framework, accessible at www.e-government.govt.nz/docs/e-gif-v-2/index.html .
Gateway	A combination of hardware and software that encrypts messages with the receiving organisation's Public Key and digitally signs them with the sending organisation's Private Key.
NZSIT	The New Zealand Security Information Technology standards issued by the Government Communications and Security Bureau, accessible at www.gcsb.govt.nz/nzsit/index.htm .
Private Key	A logical key that is kept secret to one Organisation and has a corresponding Public Key. It is used to unlock SecureMail messages encrypted with the Organisation's Public Key and to digitally sign SecureMail messages sent by the Organisation's Gateway.
Public Key	A logical key belonging to one Organisation, that is made publicly available and has a corresponding Private Key. It is used to encrypt plain text messages to be sent to the Organisation that holds the corresponding Private Key and may be used to check the digital signature of a SecureMail message sent by that Organisation is valid.
SIGS	The Security In Government Sector manual (2002) issued by the Department of Prime Minister and Cabinet, accessible at www.security.govt.nz/sigs/index.html .
SMARTS	SecureMail Automated Reference Test Server, which tests the interoperability of Gateways.
S/MIME	Secure Multipurpose Internet Mail Extensions.
SSL	Secure Sockets Layer.
VPN	Virtual Private Network.

Generic Gateway Requirements

RFC Requirements	
<p>Note: The following requirements refer to a Gateway and its functions. It is acceptable to implement Secure Email functionality in a system using non-Gateway components – such an implementation will be reviewed on a case-by-case basis. Site certification (SMARTS) tests the overall system functionality.</p>	
1.	<p>The Gateway MUST be compliant with the following RFCs:</p> <ul style="list-style-type: none"> • RFC2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.imc.org/rfc2459 • RFC3850 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling, http://www.imc.org/rfc3850 • RFC3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification, http://www.imc.org/rfc3851 <p>NOTE: Compliance with the following RFCs is encouraged and partial compliance is required to meet Secure Email business requirements:</p> <ul style="list-style-type: none"> • RFC2634 Enhanced Security Services for S/MIME, http://www.imc.org/rfc2634 • RFC3183 Domain Security Services using S/MIME, http://www.imc.org/rfc3183
2.	<p>The Gateway SHOULD wherever possible utilise the RFC specifications in the same manner as desktop clients.</p>
Implementation Requirements	
3.	<p>The Gateway MUST behave in a consistent and predictable manner.</p>
4.	<p>The Gateway MUST support secure emails containing attachments.</p>
5.	<p>The Gateway MUST support secure emails transmitted to multiple user recipients.</p>
6.	<p>The Gateway MUST be scalable to interoperate with all Secure Email agencies.</p>
7.	<p>The Gateway MUST allow asynchronous setup and maintenance of Secure Email links. {B Req}</p>
8.	<p>The Gateway MUST require minimal implementation effort by existing Secure</p>

	Email Agencies.	
Integration Requirements		
9.	The Gateway MUST not impact on the functionality of existing systems, including virus checking and content filtering software.	
10.	The Gateway MUST require no client software customisation.	
11.	The Gateway MUST not impact the transmission of email to non-secure recipients.	
12.	The Gateway MUST not impact on the transmission of individual-to-individual S/MIME emails.	
<u>13.</u>	<u>The Gateway MUST not impact on the transmission of listserve emails.</u>	<u>New</u>
14.	The Gateway MUST support common email client software.	
15.	The Gateway MUST be able to utilise X.509 v3 certificates from any Secure Email accredited Certification Authority.	
16.	The Gateway MAY support more than one Secure Email domain.	
Interoperability Requirements		
17.	The Gateway MUST interoperate with all other Accredited Software in all Participating Agencies, in a manner that complies with these business requirements.	
18.	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.	
<u>19.</u>	<u>The Gateway MUST be able to interface with SMARTS (Secure eMail Automated Reference Test Server) to test interoperability and security.</u>	<u>New</u>
<u>20.</u>	<u>The Gateway SHOULD allow the Gateway Administrator to manually initiate SMARTS testing.</u>	<u>New</u>

21.	<p><u>The Gateway MUST automatically perform SMARTS testing, at least once per month.</u></p> <p><u>Note: It is suggested that the Gateway perform SMARTS testing at system start time, and then once a month from that date/time, to ensure all Gateways do not attempt to test simultaneously.</u></p>	New
Security Requirements		
22.	The Gateway MUST check the authenticity of any message before relying on it. {B Req}	
23.	The Gateway MUST only send email using an approved algorithm. {S Req}	
24.	The Gateway MUST support the following approved algorithms: Triple-DES, RSA-1024/2048 and SHA-1. {S Req}	
25.	The Gateway SHOULD support the following approved algorithm: Advanced Encryption Standard (AES) with 128, 192 and 256-bit key lengths. {S Req}	
26.	The Gateway MUST always use the highest approved encryption algorithm supported by both Gateways. {S Req}	
27.	The Gateway crypto modules MUST be FIPS140 evaluated. {S Req}	
28.	The Gateway 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. {S Req}	
Trigger Word Requirements		
29.	The Gateway MUST handle an email containing trigger word(s) consistently. {B Req}	
30.	The Gateway MUST only recognise trigger word(s) in UPPER case {B Req}	Amended
31.	The Gateway MUST only recognise trigger word(s) bounded by square brackets {B Req}	Amended
32.	The Gateway MUST recognise trigger word(s) in either the email SUBJECT or email BODY. {B Req}	

33.	<p><u>The Gateway MUST recognise trigger word(s) in the following message encoding formats:</u></p> <ul style="list-style-type: none"> • <u>UNICODE UTF-7</u> • <u>RTF</u> • <u>HTML</u> <p>{B Req}</p>	New
34.	<p>The Gateway MAY recognise trigger word(s) in the email attachments, but this is an agency-specific feature (NOT part of Secure Email). {B Req}</p>	Amended
35.	<p><u>The Gateway MUST recognise the Delivery Receipt trigger word: RSVPDR.</u></p> <p>{B Req}</p>	New
<p>Certificate Handling Requirements</p>		
<p>Certificate handling errors are the most likely cause of disruption to secure email traffic. Therefore, the following certificate processing principles have been adopted:</p> <ul style="list-style-type: none"> • Fail safe • Allow for faulty implementations • Allow for transition issues (e.g. <u>a certificate expires while the message is in transit or two valid certificates with different public keys exist for the same domain name</u>) • Allow for the use of certificates from outside of S.E.E. Mail • Incoming messages will be delivered, even if there are certificate problems. The user is warned and can make a decision about relying on the information. • Outgoing messages will not be sent, if there are certificate problems, as there is a risk to security. Messages will be queued for future delivery. 		
36.	<p>The Gateway MUST verify whether the certificate is valid, and must verify whether any of the failures listed below have occurred. {RFC}</p> <p>As per RFC3850, Section 5 -</p> <p><i>Some of the many places where signature and certificate checking might fail include:</i></p> <ul style="list-style-type: none"> - <i>no Internet mail addresses in a certificate match the sender of a message, if the certificate contains at least one mail address</i> - <i>no certificate chain leads to a trusted CA</i> - <i>no ability to check the CRL for a certificate</i> - <i>an invalid CRL was received</i> - <i>the CRL being checked is expired</i> - <i>the certificate is expired</i> - <i>the certificate has been revoked</i> - <i>the certificate has not yet been issued (system date is earlier than issue date)</i> 	

Formatted: Bullets and Numbering

	<i>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.</i>	
37.	<p>Where a Gateway has two (or more) valid certificates for a domain name, the newest SHOULD be used for signing outgoing email. {B Req}</p> <p>Note: Because we do not operate a time stamping service, the validity is based on whether the certificate is valid when processing the message as opposed to whether the certificate was valid when the message was signed. Using the newest certificate reduces the chance of the certificate expiring while the message is in transit.</p>	New
38.	Where a Gateway has two (or more) valid certificates for a domain name, all MUST be available for decrypting incoming email. {B Req}	New
39.	The Gateway SHOULD cache CRLs until they expire. {B Req}	New
40.	<p>The Gateway SHOULD use the last cached CRL if the Certificate Distribution Point (CDP) is unavailable. {B Req}</p> <p>Note: This is a business continuity issue – mail should not fail because the CDP is unavailable. It is a low risk that the CDP would be unavailable because of a DOS attack, to allow a compromised key to be used.</p>	New
41.	The Gateway MUST handle certificates in a consistent manner, as specified in Table 1: Certificate Processing Behaviour {B Req}	

TABLE 1: Certificate Processing Behaviour

Other agency's certificate is ...	Sending a message (encrypting)	Receiving a message (verifying)
Valid	<ul style="list-style-type: none"> Deliver message. 	<ul style="list-style-type: none"> Deliver message.
Revoked / Suspended	<ul style="list-style-type: none"> Auto-discover valid public key certificate (LDAP). Success: Send message. Fail: Hold message. Notify Sender, Sender's Postmaster – SECURE DELIVERY DELAYED. 	<ul style="list-style-type: none"> Generate warning to Recipient: UNVERIFIED MESSAGE. Deliver message. Notify Recipient's Postmaster.
Untrusted / Unknown CA	<ul style="list-style-type: none"> Auto-discover valid public key certificate (LDAP). Success: Send message. Notify Recipient's Postmaster. Fail: Hold message. Notify 	<ul style="list-style-type: none"> Generate warning to Recipient: UNVERIFIED MESSAGE. Deliver message. Notify Recipient's Postmaster.

	Sender, Sender's Postmaster – SECURE DELIVERY DELAYED.	
Expired	<ul style="list-style-type: none"> Auto-discover valid public key certificate (LDAP). <p>Success: Send message. Fail: Hold message. Notify Sender, Sender's Postmaster – SECURE DELIVERY DELAYED.</p>	<ul style="list-style-type: none"> Generate warning to Recipient: UNVERIFIED MESSAGE. Deliver message. Notify Recipient's Postmaster.
Unknown Status (CRL unavailable)	<ul style="list-style-type: none"> Wait and try to retrieve certificate status later. <p>Success: Send message. Fail: Hold message. Notify Sender, Sender's Postmaster – SECURE DELIVERY DELAYED.</p>	<ul style="list-style-type: none"> Generate warning to Recipient: UNVERIFIED MESSAGE. Deliver message. Notify Recipient's Postmaster.

Certificate Handling Requirements (cont)		
42.	The Gateway MUST provide a meaningful notification capability for invalid instances, and use the standard Secure Email messages (as defined in Table 2). {RFC}	

TABLE 2: Secure Email Warning Messages

	The following text must be displayed as part of any Secure Email warning message.
Sending	SECURE DELIVERY FAILURE – Your message could not be delivered securely, therefore, it was not sent. [Code: 999, ...]
Sending	SECURE DELIVERY DELAYED – Your message could not be delivered securely. The system will try again in X hours. [Code: 999, ...]
Receiving	UNVERIFIED MESSAGE – The confidentiality, integrity and/or authenticity of this message could not be verified. [Code: 999, ...]
Receiving	SYSTEM FAILURE MESSAGE – A message has passed through the Secure Email rule set without being processed. [Code: 999, ...]
Receiving	SYSTEM WARNING MESSAGE – A verified message has been received with no X-HEADER field.

43.	The Gateway MUST support an automatic process for retrieving certificates, via	
-----	--	--

	<p>LDAP query. ▾</p> <p><u>Note: Refer to LDAP requirements for further details.</u></p>		<p>Deleted: The query SHOULD retrieve the certificate by setting a 'search base' to "C=NZ", filtering on the unique gateway email address, domain-confidentiality-authority@domainname and requesting the 'usercertificate' attribute to the entry that is found.</p>
44.	<p>The Gateway MUST support a signed email request as a mandatory fallback mechanism if an LDAP directory is unavailable. The request MUST be sent to a special email address i.e. domain-certificate-request@domainname. The subject line MUST be the email 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. {RFC}</p> <p><u>Note: The converse also applies, the Gateway MUST support receiving a certificate request to the special email address i.e. domain-certificate-request@domainname, and responding with a certificate attachment.</u></p>		
45.	<ul style="list-style-type: none"> For each unique domain <u>name</u>, the Gateway MUST support <u>one</u> DCA certificate (for encryption and signing). ▾ <p><u>Note: Sub-domains are also considered unique e.g. if there are two sub-domains, mail1.agency.govt.nz and mail2.agency.govt.nz, then each sub-domain will require a unique certificate.</u></p>	Amend	<p>Deleted: either {RFC}:¶</p> <p>Deleted: ; OR ¶ separate DCA certificates (one for encryption and one for signing)</p>
46.	<p>The Gateway MUST comply with RFC3183, Section 4.1 Domain Confidentiality Naming Conventions. {RFC}</p> <p><i>As per RFC3183, Section 4.1, Domain Confidentiality Naming Conventions -</i></p> <p><i>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.</i></p> <p><i>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.</i></p>	Amend	<p>Deleted: IF a single DCA certificate is used for both signing and encrypting,</p>
	▾	Delete	<p>Deleted: 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. {RFC}</p>
47.	<p>The Gateway MUST ensure that the domain part of an email MUST be the same as, either the SubjectAltName.rfc822Name or PKCS#9 emailAddress in the signer's certificate. {RFC}</p> <p><i>As per RFC2632, Section 4.4.3, Subject Alternative Name Extension -</i></p> <p><i>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</i></p>	Amended	<p>Deleted: or an ascendant of</p>

	<p>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.</p> <p>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.</p> <p>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.</p>	
	▼ -----	Delete
48.	<p>The Gateway MUST generate a warning, if the addresses do not match or the certificate does not contain any email address.</p>	
49.	<p>The Gateway MUST retrieve CRLs automatically from a CRL distribution point extension in the relevant certificate. {RFC}</p> <p>As per RFC2459, Section 4.2.1.14, CRL Distribution Points -</p> <p>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.</p>	
	▼ -----	Delete. same as following requirement
50.	<p>The Gateway <u>MUST</u> add or update its <u>operational</u> certificate store by detecting previously unknown but currently trusted domain certificates in email received. {RFC}</p> <p><u>As per RFC2632, Section 4 -</u></p> <p><u>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).</u></p> <p><u>Note: The intention is that the Gateway automatically loads new certificates from</u></p>	Amend

Deleted: IF a Gateway uses separate certificates for signing and encryption, then the encryption certificate MUST comply with RFC3183, Section 3.1.1 Naming Conventions. {RFC}

As per RFC3183, Section 3.1.1 - ¶ The following naming conventions are specified for agents generating signatures specified in this document: ¶

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.

Deleted: The Gateway MUST store and retrieve certificates it receives, for later use. {RFC}

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.

Deleted: SHOULD

	<u>trusted CAs and they are available for immediate use.</u>	
51.	<p>The Gateway MUST be capable of an automatic process for retrieving and using the appropriate certificate, for the following purposes:</p> <ul style="list-style-type: none"> When it wishes to send another Gateway an encrypted message and does not have a current certificate for that Gateway. When it needs a new valid public key certificate from its CA <p>{RFC}</p> <p>As per RFC2633, Section 4, 4. Certificate Processing -</p> <p><i>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].</i></p> <p><i>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.</i></p> <p><i>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.</i></p> <p><i>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.</i></p>	
LDAP Requirements		
52.	<p>The Gateway MUST support LDAP v3.0. {RFC}</p> <p>As per RFC3183, Section 4.2 – Key Management for DCA Encryption</p> <p><i>Gateways SHOULD support LDAP v3.0.</i></p>	
53.	<p>The Gateway MUST support an LDAP query as the primary certificate retrieval mechanism. The query SHOULD retrieve the certificate by setting a 'search base' to "C=NZ", filtering on the unique gateway email address, domain-confidentiality-authority@domainname and requesting the 'usercertificate' attribute to the entry that is found. {RFC}</p>	
54.	<p>The Gateway MUST allow the administrator to fully automate <u>certificate discovery</u>.</p> <p><u>The Gateway MAY allow the administrator to require a manual approval step,</u> dependant upon their preference. {RFC}</p>	<p>Deleted: be able</p> <p>Deleted: EITHER</p> <p>Deleted: SEEMail key</p> <p>Deleted:</p> <p>Deleted: if the</p> <p>Deleted: can verify against the SEEMail List, OR</p>

	<p>As per RFC2632, Section 4.4.3, Subject Alternative Name Extension -</p> <p><i>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.</i></p>	
55.	<p><u>The Gateway MUST allow the administrator to fully automate certificate classification, if the Gateway can access the Accredited Gateway Lists (SEEMail, SecureMail).</u></p> <p><u>The Gateway MAY allow the administrator to require a manual approval step, dependant upon their preference. {RFC}</u></p> <p><i>Note: Classification is further advanced than discovery – once a certificate is discovered, it may be classified into a SEEMail or SecureMail list, depending upon the centralised accredited gateway lists.</i></p>	
56.	<p>The Gateway MUST be able to queue failed email and send a warning message, to enable the administrator to manually repair the problem and release the queued email, dependant upon the administrator’s preference. {B Req}</p>	
57.	<p>The Gateway SHOULD notify the sender when an email can not be delivered, in a consistent manner e.g. Remote mail server is down, will keep trying for another 67 hours {B Req}</p>	
58.	<p>The Gateway SHOULD be able to store LDAP specifications for automatic certificate retrieval e.g.</p> <ul style="list-style-type: none"> 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. ▼ 	
59.	<p><u>The gateway SHOULD allow an administrator to bypass CRL checking</u></p> <p><u>Note: This feature is required for DR purposes, when the CRL is not available. Ideally the options of CRL checking being turned off completely OR on a per certificate basis, should be offered.</u></p>	New

Deleted: This procedure MAY also be used to discover non SEEMail domain security gateways, e.g. discovering a certificate for encryption

Secure Email Sending Requirements		
60.	<p><u>The Gateway MUST be able to tag email with an identifying Secure Email field, "X-NZ-Secure-email" field, indicating the message has been sent in compliance with these requirements {RFC}</u></p> <p><i>As per RFC822, Section 4.7.5, User-Defined-Fields:</i></p> <p><i>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.</i></p>	New
61.	<p>The Gateway SHOULD be able to tag email with an identifying Gateway Domain field, "X-SEEMail-Version" field, identifying the current SEEMail version e.g. "X-SEEMail-Version: 2.0". {RFC}</p>	
62.	<p>The Gateway MUST sign / encrypt all email to another Secure Email Agency, with no exceptions i.e. including non-delivery response receipts, delivery receipts, etc. {B Req}</p>	
63.	<p><u>The Gateway MUST sign / encrypt all email sent to other Gateways, from a Secure Email domain name, with no exceptions i.e. *@domainname {B Req}</u></p>	New
64.	<p><u>The Gateway MAY support more than one Secure Email domain name e.g. *@company1.domainname and *@company2.domainname.</u></p> <p><u>Note: Each Secure Email domain name will require a unique certificate.</u></p>	New
65.	<p><u>The gateway MUST ensure there is a 'rfc2822.FROM:' field ie blanks are not allowed.</u></p> <p><u>Note: This requirement is necessary to prevent internal Secure Email spoofing by sending a blank rfc2822.FROM field, and a spoofed rfc2822.Reply-To field – which some email clients will display as a "From:".</u></p>	New
66.	<p>The Gateway MUST authenticate outbound messages --- specifically that the 'RFC2822.FROM:' field in the message header matches the sender's 'RFC2822.FROM:' address, and is appropriate for the Sender's domain. The Sender must NOT be able to disable this feature.</p>	Amended

S/MIME Sending Requirements		
67.	<p>The Gateway MUST check that a certificate is valid before relying on it. {RFC}</p> <p><i>As per RFC2632, Section 1, Overview -</i> <i>...Before using a public key to provide security services, the S/MIME agent MUST certify that the public key is valid.</i></p>	
68.	<p>The Gateway MUST use a valid certificate to sign email. {RFC}</p>	
69.	<p>The Gateway MUST use a valid certificate to encrypt email. {RFC}</p> <p><i>As per RFC2632, Section 4.2, Certificate Chain Validation -</i> <i>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.</i></p>	
70.	<p>The Gateway MUST send a valid public key certificate with every signed email. {RFC}</p> <p><i>As per RFC2632, Section 2.3, CertificateSet -</i> <i>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.</i></p>	
71.	<p>The Gateway MUST include the S/MIME capability attribute with every signed email. {RFC}</p>	
72.	<p>The Gateway MUST be able to sign and/or encrypt email to a non Secure Email entity if its certificate store contains a valid domain certificate for the recipient. {RFC}</p>	
Secure Email Receiving Requirements		
73.	<p><u>The Gateway MUST provide a Delivery Report (DR), when requested by an authenticated sender, via a RSVPDR trigger word, IF the message can be</u></p>	<u>New</u>

	<p><u>delivered.</u></p> <p><i>The Receiving Gateway's associated action is:</i></p> <p><i>The message is delivered.</i></p> <p><i>A notification message is placed in the receiving Gateway's audit log noting the date / time / sender / subject / error.</i></p> <p><i>The authenticated Sender is sent a delivery receipt. They are provided with date / time / sender / receiver / subject / date received / time received.</i></p> <p><i>The delivery receipt wording MUST include: "Your message has been successfully delivered to the organisation responsible for handling the addressee's messages. This is not a read receipt."</i></p>	
74.	<p><u>The Gateway MUST provide a Non Delivery Report (NDR), for an authenticated sender, IF the message cannot be delivered.</u></p> <p><i>The Receiving Gateway's associated action is:</i></p> <p><i>The message is deleted. An entry is recorded in the receiving Gateway's audit log, noting the date / time / sender / subject / error.</i></p> <p><i>The authenticated Sender is notified that the message could not be delivered.</i></p> <p><i>They are provided with original message information (date/time sent, TO:, FROM:, SUBJECT:).</i></p> <p><i>The failed delivery receipt wording MUST include: "Your message has NOT been delivered to the organisation responsible for handling the addressee's messages..."</i></p> <p><i>The receiving Gateway may also append additional information about the reason for the failure (e.g. no such mailbox, mailbox is full, mailbox is suspended, receiver has moved).</i></p>	<u>New</u>
75.	<p><u>The Gateway MAY provide a Delivery Report (DR), OR Non Delivery Report (NDR), when requested by an UNAUTHENTICATED sender</u></p> <p><u>Note: This is an agency-specific feature (NOT part of Secure Email).</u></p>	<u>New</u>
76.	<p><u>IF the message is verified, then the Gateway MUST deliver it.</u></p> <p><u>If the message is unverified but contains an:</u></p> <p><u>ELSE the message is unverified;</u></p> <ul style="list-style-type: none"> <u>• IF the X-HEADER field "X-NZ-Secure-email" exists then the Gateway MUST deliver the message with an UNVERIFIED warning;</u> <u>• ELSE the Gateway MAY deliver the message with an UNVERIFIED warning OR MAY delete the message, whilst logging the details of the deletion for an audit trail. This is an agency-specific decision.</u> <p><u>{B.Reg}</u></p>	<u>New</u>

Formatted: Bullets and Numbering

77.	<p><u>The Gateway MUST provide a meaningful notification capability for exceptions using the SecureMail Messages format (as defined in SecureMail Tests).</u></p> <p><u>Notifications MUST only contain the mail header information (TO:, FROM:, DATE:, and SUBJECT:), not repeat the entire message, and definitely not return the entire attachment.</u></p>	New
78.	<p>The Gateway MUST use the generic warnings. They are permitted to append additional information. e.g. "For further information on this error, click here, http://www.agency.govt.nz/seeinfo/warning5.html".</p>	
79.	<p>The Gateway MUST cease processing of further S.E.E. Mail rules IF a S.E.E. Mail rule triggers a warning. There should only ever be one message i.e. multiple warning messages should not be created, based upon a single original message.</p>	
80.	<p>The Gateway MUST handle messages that cannot be decrypted, the receiving agency should treat the message as per their policy for unknown encrypted messages. This may mean the original message is NOT attached to the SEEMail warning for the recipient.</p>	
S/MIME Receiving Requirements		
81.	<p>The Gateway MUST use the public key certificate sent with a signed email to verify the signature on that email. {RFC}</p> <p><i>As per RFC2632, Section 2.3, CertificateSet -</i></p> <p><i>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.</i></p>	
82.	<p>The Gateway SHOULD be able to handle received email without certificates by retrieving the relevant certificates using a database or directory lookup scheme {RFC}</p> <p><i>As per RFC2632, Section 2.3, CertificateSet -</i></p> <p><i>Receiving S/MIME agents SHOULD be able to handle messages without certificates using a database or directory lookup scheme.</i></p>	
83.	<p>The Gateway 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</p>	

	<p>local store. {RFC}</p> <p><i>As per RFC2633, Section 4.2, Incoming - ...certificates and CRLs SHOULD be cached for use in chain validation and optionally stored for later use...</i></p>	
84.	<p>The Gateway SHOULD cache S/MIME capabilities from received email for future use. {RFC}</p> <p><i>As per RFC2633, Section 2.7.1 - The list of capabilities SHOULD be stored for future use in creating messages...</i></p>	
85.	<p>The Gateway SHOULD automatically determine the highest available encryption algorithm and key length from a received email using the S/MIME capability attribute. {B Req}</p>	
86.	<p>The Gateway MUST handle email encrypted or signed with expired or revoked key pairs. {B Req}</p>	
87.	<p>The Gateway MUST accept email (including unsigned email), encrypted with its DCA-public key, from an unknown source. {B Req}</p>	
88.	<p>The Gateway MUST be able to strip DSA certificates from incoming email where CN=domain-signing-authority. {B Req}</p>	
89.	<p>The Gateway MUST be able to strip DCA certificates from incoming email where CN=domain-confidentiality-authority. {B Req}</p>	
Timekeeping Requirements		
90.	<p><u>The Gateway MUST maintain an accurate clock synchronised with UTC (MSL) time.</u></p> <p><u>Note: Possible methods include GPS, or Network Time Protocol (NTP) to the NZ Time Source (msltime.irl.cri.nz).</u></p>	<u>New</u>
Agency-Specific Requirements		
91.	<p>The Gateway MAY support an agency-specific EXCEPTION list of domains that can communicate using S/MIME, but are not a member of Secure Email, specified by the System's Administrator. {B Req}</p>	

Gateway Administrator Notification		
<p>Principles:</p> <ul style="list-style-type: none"> Implement notifications in such a way as to minimize the impact on service / performance e.g. don't send an error email 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. 		
92.	The Gateway MUST ensure exception / notification messages are addressed "from" a valid "postmaster@domainname" account. {B Req}	
93.	The Gateway MUST ensure a rule for inbound email, where the message is "from" postmaster, does not send an exception message (to avoid loops). {B Req}	
94.	The Gateway SHOULD allow the system administrator to specify audit log and/or email notifications, and their frequency, as some failures could cause a log/mail notification storm. {B Req}	
95.	The Gateway MUST ensure rules for inbound email do not send exception messages to postmaster of the sending agency. {B Req}	

Diagnostics		
96.	The Gateway MUST support an automated email responder for diagnostic purposes, ("ping function") {B Req}	
97.	The Gateway MUST operate the ping function before any other Secure Email business rules and not invoke them. {B Req}	
98.	The Gateway's ping function MUST auto-respond with a signed/encrypted reply to a message that is signed (and/or encrypted) with a domain certificate issued by a Secure Email CA {B Req}	
99.	The Gateway's ping function MUST respond with the Secure Email environment (SecureMail or SEEMail) version number, gateway software name/version number and SHOULD respond with the list of SEEMail agencies it knows about {B Req}	

Record Keeping Requirements		
100.	The Gateway MUST be able to record information relating to when the relevant Gateway sent and received the SecureMail message in the message header.	

SEEMail Requirements

SEEMail Participating Agency Requirements

1 These requirements override the generic Participating Agency requirements.

Security Requirements		
101.	The Participating Agency MUST comply with the minimum security standards for IN-CONFIDENCE, SENSITIVE and RESTRICTED information, dictated by the Security In the Government Sector (SIGS) manual and New Zealand Security of Information Technology (NZSIT) publications.	
102.	The Participating Agency MUST <ul style="list-style-type: none"> • 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 	
103.	The Participating Agency SHOULD have real time access to the logging and analysis of faults, alerts and intrusions.	amended
104.	The Participating Agency SHOULD have processes in place for when a Gateway fails.	
105.	The 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). {S Req}	
106.	The Participating Agency MUST protect Gateway private keys at all times, from any unauthorised access, disclosure or tampering. {S Req}	
107.	The Participating Agency MUST ensure all media used for the storage of Gateway private keys is sanitised by overwriting or degaussing as described in GCSB Security Notice 02/04, 'Declassification of Storage Media', or destroyed before it is released from the Participating Agency's control. {S Req}	

Deleted: SENSITIVE

Exception Requirements		
108.	The Participating Agency SHOULD support a “WORKSPACE” ruleset, and use this as the basis to downgrade UNVERIFIED messages to NO warning. The “WORKSPACE” rule set will apply to all domains obtained on a regular basis from the LDAP workspace list. {B Req}	

SEEMail Gateway Requirements

2 These requirements override the generic Gateway requirements.

SEEMail Trigger Words		
109.	The Gateway MUST recognise SIGS specific trigger word(s): IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, when in UPPER CASE and bounded by square brackets. {B Req}	
110.	When sending, the Gateway SHOULD quarantine TOP SECRET, SECRET or CONFIDENTIAL messages and notify the System Administrator. {B Req}	
111.	The Gateway MUST ensure emails containing SENSITIVE and/or RESTRICTED trigger word(s) are only sent to a SEEMAIL gateway domain or an agency-specific exception list {B Req}.	
112.	The Gateway MUST ensure emails containing the IN-CONFIDENCE trigger word are only sent to a SEEMAIL gateway domain, a SECUREMAIL gateway domain or an agency-specific exception list {B Req}.	
<u>113.</u>	<u>The Gateway SHOULD log breaches of SIGS trigger words and MAY notify the System Administrator. {B Req}</u>	<u>New</u>

SecureMail Requirements

SecureMail Gateway Requirements

3 These requirements override the generic Gateway requirements.

SecureMail Trigger Words		
114.	The Gateway MUST recognise the SIGS specific trigger word IN-CONFIDENCE when in UPPER CASE and bounded by square brackets. {B Req}	
115.	The Gateway MUST ensure emails containing the IN-CONFIDENCE trigger word are only sent to a SEEMAIL gateway domain, a SECUREMAIL gateway domain or an agency-specific exception list {B Req}.	

SecureMail – Generic Service Provider Requirements

4 A SecureMail Service Provider handles information classified IN-CONFIDENCE, in accordance with the Security in the Government Sector (SIGS) manual.

5 A Service Provider is any provider of any aspect of the SecureMail service such as:

- Gateway Service Provider
- Mail Service Provider

6 These requirements override the generic Participating Agency requirements.

Sovereignty Requirements		
116.	<u>The Service Provider MUST ensure there is no uncertainty that New Zealand law applies and that any information stored or created as part of this system will remain sovereign to this country - both in a legal and physical sense.</u>	<u>New</u>
117.	The Service Provider MUST retain such information obtained by that organisation as enables the identification of: (i) the origin of the SecureMail message; and (ii) the destination of the SecureMail message; and (iii) the time when the SecureMail message was sent and the time when it was received; and	

	The information referred to above must be readily accessible so as to be usable for subsequent reference.	
118.	The Service Provider MUST comply with the law	
Accreditation Requirements		
119.	The Service Provider MUST comply with the SecureMail interoperability and security requirements, at all times, and at its own cost.	
120.	The Service Provider MUST verify in writing that they comply with these Requirements and conduct regular compliance audits as specified by the Secure Email Administrator.	
121.	The Service Provider WILL have to abide by the Secure Email process (including time frames) for making technical changes to the Secure Email environment and resolving disputes between parties.	
Security Requirements		
122.	The Service Provider MUST comply with the IN-CONFIDENCE standards dictated by the Security In the Government Sector (SIGS) manual and New Zealand Security of Information Technology (NZSIT) publications.	
123.	The Service Provider MUST ensure their system is configured to comply with the Minimum Standards for Internet Security in the New Zealand Government: http://www.security.govt.nz/sigs/html/chapter8.html#Ref9668810 .	
124.	The Service Provider MUST <ul style="list-style-type: none"> • 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 	
125.	The Service Provider MUST ensure Secure Mail messages, whether encrypted or unencrypted, are not sent outside of the New Zealand portion of the Internet.	
126.	The Service Provider MUST ensure messages are stored/communicated in a	

	secure manner.	
127.	The Service Provider MUST have real time access to the logging and analysis of faults, alerts and intrusions.	
128.	The Service Provider MUST have processes in place for when the System fails or is compromised.	
129.	The Service Provider MUST demonstrate that they have an effective disaster recovery procedure and business continuity plan.	
130.	The Service Provider MUST have protocols in place which outline responsibilities and accountabilities of all parties, when the service is to be externally tested for security.	
131.	The Service Provider 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). {S Req}	
132.	The Service Provider MUST protect private keys at all times, from any unauthorised access, disclosure or tampering. {S Req}	
133.	The Service Provider MUST ensure any service information; private keys or messages are disposed of in a secure manner.	
134.	The Service Provider MUST ensure all media used for the storage of private keys is sanitised by overwriting or degaussing as described in GCSB Security Notice 02/04 dated 24 February 2004, or destroyed before it is released from the Service Provider's control. {S Req}	
User Authentication Requirements		
135.	The Service Provider MUST ensure the organisation applying for the service is verified as the owner of the domain address	
Duty of Care Requirements		
136.	The Service Provider MUST ensure no spoofing of customers within the Service Provider's system.	
137.	The Service Provider MUST inform customers of good practise e.g. ensuring no	

	spoofing of employees within organisations or by persons associated with people.	
138.	The Service Provider MUST manage a robust internal authentication and identity management model that meets the Authentication for e-Government: Best Practice Framework for Authentication.	
139.	The Service Provider SHOULD manage a robust internal authentication and identity management model that can eventually integrate with the All-of-Government On-Line Authentication initiative as it matures.	
140.	The Service Provider MUST ensure their employment agreement requires employees to return all access keys on ceasing employment and not to misuse their computer access	
Timekeeping Requirements		
141.	<p><u>The Gateway MUST maintain an accurate clock synchronised with UTC (MSL) time.</u></p> <p><u>Note: Possible methods include GPS, or Network Time Protocol (NTP) to the NZ Time Source (msltime.irl.cri.nz).</u></p>	<u>New</u>
Minimum Customer Service Requirements		
142.	<p>The Service Provider's Customer Service Contract MUST contain clauses that are equal or equivalent to those listed in this section. Compliance with these clauses shall form part of the Service Provider accreditation process.</p> <ul style="list-style-type: none"> The Service Provider MUST ensure the Service is contracted under New Zealand law. The Service Provider MUST contract to provide a secure service (protecting the confidentiality, integrity, authenticity and availability of the Customer's messages) and system information The Service Provider MUST ensure messages can be exchanged with other Secure EMail participants. The Service Provider MUST provide a web site for Customers to access the documents that define their rights and responsibilities. The Service Provider MUST have provision to cancel the Service provided to a Customer, who abuses the SecureMail system. The Service Provider MUST guarantee levels of availability (including connectivity). Availability guarantees should, in any, case exceed 99.5%. 	

Contact Information Requirements		
143.	The Service Provider MUST provide up-to-date contact information to the Secure EMail administrator. This information should not contain any personally identifiable information. For example, a generic email address such as securemailadmin@domainname, and a phone number.	
Reporting Requirements		
144.	The Service Provider MUST report any security breaches and their resolution to the SecureMail Administrator on a monthly basis.	
Lawful Interception Requirements		
145.	The Service Provider MUST ensure that public telecommunications networks and telecommunications services that they own, control or operate have interception capability {Law}.	
146.	The Service Provider MUST assist with the interception of telecommunications subject to an interception warrant. (Law)	
147.	<p>The Service Provider MUST ensure an original copy of the message (as received by the Service Provider) is held in New Zealand, to ensure the message is obtainable by a search warrant and ensure New Zealand sovereignty/jurisdiction is maintained over the message. (Law)</p> <p>Note: This means that a Service Provider offering an off-shore storage or encryption facility will not be eligible for accreditation.</p>	

SecureMail – Mail Service Provider Requirements

7 These requirements are in addition to the Service Provider requirements.

Authentication Requirements		
148.	<p>The Mail Service Provider MUST ensure:</p> <ul style="list-style-type: none"> • each customer's/employee's authorisation is verified before allowing them to access a SecureMail mailbox (eg username/password); • an audit trail that shows whose authorisation was used to access the relevant SecureMail mailbox must be kept for as long as required; and • their customers are not able to spoof one another. 	
149.	<p>The Mail Service Provider MUST authenticate SecureMail customers requiring access to IN-CONFIDENCE information with a means of authentication such as username/password complying with NZSIT 204, para 220, http://www.gcsb.govt.nz/nzsit/204/204chap2.htm</p>	
Mail Service Provision Requirements		
150.	<p>The Mail Service Provider MUST ensure that information is protected, by reasonable safeguards, against loss, unauthorised access, and misuse. In meeting this requirement, service providers should note that no particular technology or combination of technologies is prescribed.</p>	
151.	<p>The Mail Service Provider MAY provide one or more of the following services:</p> <ul style="list-style-type: none"> • WebMail • Pop3/SMTP/IMAP4 • Server-Server 	
152.	<p>The Mail Service Provider providing WebMail MUST use SSL (transmission security) and authentication (username/password)</p>	
153.	<p>The Mail Service Provider providing POP3/SMTP/IMAP4 SHOULD provide SSL (transmission security) and authentication (username/password)</p>	
154.	<p>The Mail Service Provider providing Server-Server MUST provide a secure means of transmission (VPN or leased line) and authentication (depends on technology)</p>	

Minimum Customer Service Requirements		
155.	<p>The Mail Service Provider's Customer Service Contract MUST contain clauses that are equal or equivalent to those listed in this section. Compliance with these clauses shall form part of the Service Provider accreditation process.</p> <ul style="list-style-type: none"> The Mail Service Provider MUST specify that the Customer owns the messages and associated information in the Message Store, while the Service Provider is merely the custodian. The Mail Service Provider MUST guarantee that the contents of a message store can be recovered within 1-business day. The Mail Service Provider MUST require all clients that have their own domain name to authorise using that domain name for SecureMail. The Mail Service Provider MUST obtain the Customer's written acknowledgement that the mailbox may be shared, and the Customer then accepts that other users may access emails addressed to the individual. 	
Value-Added Service Requirements		
156.	<p>The Mail Service Provider is free to provide value-added extensions and services to their clients, but these extensions MUST not:</p> <ul style="list-style-type: none"> impact the interoperability or security of SecureMail; impact the performance and service delivery of other Service Providers or Participating Agencies; and/or lock-in customers. 	
Minimum Customer Training Requirements		
157.	<p>The Mail Service Provider MUST provide training/information that is equal or equivalent to those listed in this section. Compliance with these clauses shall form part of the Service Provider accreditation process.</p> <ul style="list-style-type: none"> The Mail Service Provider MUST ensure a Customer acknowledges his/her understanding that where a mailbox is shared, there are risks such as that messages can be opened by the wrong person.; The Mail Service Provider MUST ensure a Customer acknowledges his/her understanding that messages can still be sent to the wrong addressee; 	

TABLE 3: Secure Email Warning Codes

Code	GENERIC ERROR / Description
001	SECURE DELIVERY FAILURE: The sender is trying to send a secure message (indicated by a trigger word) to an agency that does not have the appropriate Secure Email capability.
002	UNVERIFIED MESSAGE: This message did not come directly from the apparent sender's agency. The From: field shows a Participating agency address, i.e. nothing to indicate an external sender. Possible causes of this warning include: <ul style="list-style-type: none"> a. The mail may have been forwarded by a distribution (List serve) service b. The sender is working away from their agency, and using an ISP mail account c. Someone other than the sender may have sent the message and falsified the email address
003	UNVERIFIED MESSAGE: This message was altered en-route. Possible causes of this warning include: <ul style="list-style-type: none"> a. The message was garbled in-transit due to communications problems b. The message was intercepted and altered while in transit
004	UNVERIFIED MESSAGE: A message containing a trigger word has arrived from a non-Participating Agency. The confidentiality, integrity or authenticity of the message cannot be guaranteed.
005	UNVERIFIED MESSAGE: A message has arrived which appears to be from the <u>sender's</u> agency. Possible causes of this warning include: <ul style="list-style-type: none"> a. The mail may have been forwarded by a distribution (List serve) service b. The sender is working away from our agency, and using an ISP mail account c. Someone other than the sender may have sent the message and falsified the email address
006	No longer used.
007	No longer used.

008	UNVERIFIED MESSAGE: The message was sent from a Participating Agency but only signed, not encrypted.
009	SYSTEM FAILURE MESSAGE: A message has got through the rule set.
	INCOMING - Certificate Warning Messages
101	UNVERIFIED MESSAGE: The sender's certificate has been revoked / suspended for some reason.
102	UNVERIFIED MESSAGE: The sender's certificate is untrusted / unknown for some reason.
103	UNVERIFIED MESSAGE: The sender's certificate has expired. The Secure Email system could not retrieve a new one.
104	UNVERIFIED MESSAGE: The sender's certificate status could not be verified against the Certificate Revocation List.
105	UNVERIFIED MESSAGE: The sender's certificate is not yet valid.
111	UNVERIFIED MESSAGE: The recipient's certificate has been revoked / suspended for some reason.
112	UNVERIFIED MESSAGE: The recipient's certificate is associated with an untrusted / unknown CA.
113	UNVERIFIED MESSAGE: The recipient's certificate has expired. The Secure Email system could not retrieve a new one.
114	UNVERIFIED MESSAGE: The recipient's certificate status could not be verified against the Certificate Revocation List.
115	UNVERIFIED MESSAGE: The recipient's certificate is not yet valid.
	OUTGOING - Certificate Warning Messages
201	SECURE DELIVERY DELAYED: The sender's Secure Email system does not have a valid certificate for the recipient agency, and cannot auto-discover a valid certificate. The message has been held for future delivery.

202	SECURE DELIVERY DELAYED: The sender's Secure Email system has (or has auto-discovered) a valid certificate for the recipient agency, but cannot determine its status (no CRL, etc) The message has been held for future delivery.
211	SECURE DELIVERY DELAYED: The sender's Secure Email system does not have a valid certificate for itself and cannot auto-discover a valid certificate. The message has been held for future delivery.
212	SECURE DELIVERY DELAYED: The sender's Secure Email system has (or has auto-discovered) a valid certificate for itself, but cannot determine its status (no CRL, etc). The message has been held for future delivery.

TABLE 4: Secure Email Delivery Messages

	The following text must be displayed as part of any Secure Email Delivery message. And as the first line.
Receiving (back to sender)	DELIVERY RECEIPT – Your message has been successfully delivered to the organisation responsible for handling the addressee's messages. This is not a read receipt.
Receiving (back to sender)	NON DELIVERY REPORT – Your message was NOT delivered to the organisation responsible for handling the addressee's messages.

Certification Authority (CA) Requirements

8 The Secure Email Manager will accredit each Certificate Authority (CA) to ensure their certificates are interoperable within the Secure Email environment.

9 Wider issues for discussion, that will have implications on the following requirements:

- Should the Secure Email Manager act as a CA with the CAs in effect, being ICAs?
- Should there be a single directory, or should each CA run their own directory?

Formatted: Bullets and Numbering

Security Requirements		
158.	The CA MUST include a CRL distribution point extension in the Secure Email certificate. {RFC} As per RFC2459, Section 4.2.1.14, CRL Distribution Points - <i>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.</i>	
159.	The CA MUST support an automatic process for retrieving certificates, via LDAP query. The query SHOULD retrieve the certificate by setting a 'search base' to "C=NZ", filtering on the unique gateway email address, domain-confidentiality-authority@domainname and requesting the 'usercertificate' attribute to the entry that is found.	
160.	The CA MUST generate certificates with an expiry date of no longer than THIRTEEN months after the issue date. {CP Req}	Or replace key every thirteen months
161.	The CA MUST generate a new key pair 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). {CP Req}	
162.	The CA SHOULD provide a public key pair created with a hardware key pair or seed generator. {S Req}	
Certificate Requirements		
163.	<ul style="list-style-type: none"> • The CA MUST provide one DCA certificate (for encryption and signing) for each unique domain 	Amended

Deleted: F

Deleted: , the CA MUST provide either {RFC}; ¶ one DCA certificate (for encryption and signing); OR ¶ separate DCA certificates (one for encryption and one for signing)

164.	<p>The CA MUST provide a certificate complying with RFC3183, Section 4.1 Domain Confidentiality Naming Conventions. {RFC}</p> <p><i>As per RFC3183, Section 4.1, Domain Confidentiality Naming Conventions</i></p> <p><i>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.</i></p> <p><i>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.</i></p>	Amended
165.		Deleted
166.	<p>The CA MUST ensure that the domain part of an email MUST be the same as either the SubjectAltName.rfc822Name or PKCS#9 emailAddress in the signer's certificate. {RFC}</p> <p><i>As per RFC2632, Section 4.4.3, Subject Alternative Name Extension -</i></p> <p><i>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.</i></p> <p><i>As per RFC2632, Section 3, Using Distinguished Names for Internet Mail -</i></p> <p><i>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.</i></p> <p><i>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.</i></p>	Deleted
167.		Deleted
LDAP updates		
168.	<p>The CA MUST provide and maintain a certificate or certificate URL to the LDAP server. {B Req}</p>	
169.	<p>The CA MUST remove any revoked certificates from the LDAP list. {B Req}</p>	

Deleted: IF a single DCA certificate is used for both signing and encrypting,

Deleted: IF a CA provides separate certificates for signing and encryption, then the signing certificate MUST comply with RFC3183, Section 4.1 Domain Confidentiality Naming Conventions. {RFC}

Deleted: or an ascendant of,

Deleted: IF a CA provides separate certificates for signing and encryption, then the encryption certificate MUST comply with RFC3183, Section 3.1.1 Naming Conventions. {RFC}

As per RFC3183, Section 3.1.1 - ¶

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

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.

Deleted: current

Participating Agency Requirements

Principles

- 10 Each Secure Email Agency must be confident that:
- All Secure Email is secured;
 - An email with a Secure Email trigger word will only ever be sent securely;
 - All email between Secure Email Agencies authenticates the sending agency;
 - Incoming and outgoing email must be automatically suspended when the Gateway is not operational.
- 11 The Recipient in a Secure Email Agency must be confident that:
- The email is from the sending Secure Email Agency as claimed;
 - No one outside the sending Secure Email Agency has read the email;
 - No one outside the sending Secure Email Agency has altered the email.
- 12 The Sender in a Secure Email Agency must be confident that:
- The email can only be read by the receiving Secure Email Agency;
 - No one outside the receiving Secure Email Agency can read the email in transit;
 - No one outside the receiving Secure Email Agency can alter the email.

Lawful Requirements		
170.	The Participating Agency MUST comply with the law	
Interoperability Requirements		
171.	The Participating Agency MUST ensure at all times that it is able to pass Site Certification tests.	
Security Requirements		
172.	The Participating Agency MUST ensure the security of messages within their organisation. Note: SecureMail can only be used in the New Zealand portion of the Internet.	
173.	The Participating Agency must ensure that any SecureMail message it sends has an authenticated rfc2822.FROM: address. I.e. the address can be linked to an individual. The SecureMail minimum standards for authentication are username/password.	

174.	<p><u>IF a Participating Agency suspects their message security has been compromised, as soon as practicable it MUST:</u></p> <ul style="list-style-type: none"> • <u>obtain a new public/private key pair;</u> • <u>issue/install the new certificate; and</u> • <u>revoke any certificate relating to the compromised key pair.</u> 	New
175.	The Participating Agency MUST have real time access to the logging and analysis of faults, alerts and intrusions.	
176.	The Participating Agency SHOULD have processes in place for when a Gateway fails.	
177.	The Participating Agency MUST ensure their employment agreement requires employees to return all access keys on ceasing employment and not to misuse their computer access	
Certificate Requirements		
178.	The Participating Agency MUST use a certificate issued by an accredited Secure Email Certificate Authority (CA). Self-signed certificates are not acceptable.	
179.	The Participating Agency MUST maintain a Secure Email Manager list of trusted CA root-keys. {B Req}	
180.	The Participating Agency MAY add other CA root-keys if they require. {B Req}	
Documentation and Training Recommendations		
181.	The Participating Agency SHOULD provide user education material and publicise the Secure Email service on a regular basis. {B Req}	
Postmaster Configuration		
182.	The Participating Agency MUST have a valid postmaster account, e.g. postmaster@domainname, to send exception messages and accept notifications. {B Req}	
Notification Requirements		
183.	The Participating Agency MUST send notification messages to authenticated	New

Formatted: Bullets and Numbering

	<p>senders.</p> <p>NOTE: A Participating Agency SHOULD send notification messages to all senders, but due to spam/etc, this is not current practice.</p>	
184.	<p>The Participating Agency SHOULD to the extent possible, notify the sending agency if the Secure Email message is not immediately available to the relevant individual at the receiving agency.</p>	New
ETA Requirements		
185.	<p>The Participating Agency MUST obtain the receiving organisation/person's consent to the use of SecureMail messages, if consent to the use of electronic communications has not already been obtained, WHEN the ETA applies. {Legal}</p>	New
186.	<p>The Participating Agency MUST obtain the sender's electronic signature (being a method used to identify the sender (a person) and to indicate the sender's approval of information), in addition to the sending agency's SecureMail digital signature, WHEN the ETA applies, AND where there is a legal requirement for a signature. {Legal}</p>	New
187.	<p>The Participating Agency MUST ensure that the integrity of the information is maintained outside of the SecureMail environment, WHEN the ETA applies, AND when the agency is subject to a legal requirement to retain, provide or produce, or provide access to information. {Legal}</p>	New
188.	<p>The Participating Agency MUST be satisfied with the email address details of the person they are dealing with and verify their identity, where appropriate (ie depending on the nature of the transaction), before sending SecureMail messages to that email address or acting on messages from them, as SecureMail does not authenticate the person sending or receiving the message. {Legal}</p>	New
189.	<p>The Participating Agency MUST retain all relevant Public/Private Keys (and decryption technology) where encrypted/signed messages are retained by the agency, so that future access to the message is maintained {Legal}</p>	New

Centralised Infrastructure Requirements

13. The Secure Email Manager will be responsible for centralised infrastructure essential to the operation of the Secure Email environment. This includes:

- SMARTS – the Secure Email Automated Reference Test Server
- LDAP – the LDAP directory

Formatted: Bullets and Numbering

LDAP Server Requirements		
190.	<p>The LDAP server WILL have several lists controlled by the SEEMail Manager {B Req}:</p> <ul style="list-style-type: none"> • <u>Operational Environments – Each Gateway will need to have a list of accredited agencies to trust. For reasons of transition, it is intended the lists will include a version number.</u> • SEEMAIL2 – A list of Accredited Participating Agencies as *@domainname • SECUREMAIL1 – A list of Accredited Participating Agencies as *@domainname <p><u>Test Environments – SMARTS will require each Gateway Domain/Version to have a list of agencies able to run the relevant tests. The current lists are</u></p> <ul style="list-style-type: none"> • SEEMAIL2TEST • SECUREMAIL1TEST 	<p><u>Note: Gateways should automatically sign/encrypt if they receive a signed/encrypted email, therefore the following lists will be dropped “EGU certs” and “VENDOR”.</u></p>
191.	The LDAP server MUST support LDAP v3.0. {RFC}	
192.	The LDAP server MUST support a request to retrieve a certificate by setting a ‘search base’ to “C=NZ”, filtering on the unique gateway email address, domain-confidentiality-authority@domainname and requesting the ‘usercertificate’ attribute to the entry that is found.	
LDAP Service Provision Requirements		
193.	The LDAP Service Provider MUST ensure that the Directory is reliable and has a high degree of availability.	
194.	The LDAP Service Provider MUST ensure that no personal information is recorded in the Directory, so that that no privacy issues arise.	

Deleted: ¶ WORKSPACE – A list of Trusted Listserves as *@domainname. An email from this address will not generate a “spoofed” warning

Deleted: <#>VENDOR – A list of Participating Vendors as *@domain¶

Formatted: Bullets and Numbering

Deleted: .

<u>SMARTS Server Requirements</u>		
<u>195.</u>	<u>The SMARTS service MUST allow any agency in the Test Environment LDAP groups to perform SMARTS tests.</u>	

Deleted requirements

- 14 The Gateway SHOULD operate on multiple platforms, such as Windows NT and Unix.
- 15 {B Req} Participating Agencies MUST implement S.E.E. Key server certificates, when they become available, on the next renewal of their key.
- 16 {RFC} Agencies MUST use one DCA certificate (for encryption and signing) for one unique domain
- 17 one or more DCA certificate(s) (for encryption and signing) with multiple RFC822 DCA email addresses for every unique domain in the Subject Alternative Name Extension of the certificate

Listserve Requirements		
196.	The Gateway MUST permit the exchange of non-secure email among list-serve groups of individuals; some of whom are members of Participating Agencies and some of whom are members of non-Participating Agencies.	
197.	The Gateway MUST allow the exchange of secure email among list-serve groups of individuals; who are all members of Participating Agencies.	
198.	The Gateway MUST function with list-serves that do not support Secure Email.	
199.	<p>The Gateway SHOULD support a "LISTSERVE" rule, and use this as the basis to downgrade Warning 2 (unverified external sender) or Warning 5 (unverified internal sender) from a HARD warning, to a SOFT warning. The test to detect a message from a Listserve is the presence of one or more of the following headers in the message {B Req}:</p> <ul style="list-style-type: none"> • errors-to: • list-archive: • list-help: • list-id: • list-name: • list-post: • list-subscribe: • list-unsubscribe: • mailing list: • precedence: bulk • x-beenthere: • x-mailman: 	

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