X.509 Certificate Policy
for the
New Zealand Government PKI
ECC SEEMail Certificates

Version 1.1
Mar-21

Notice to all parties seeking to rely

Reliance on a Certificate issued under this Certificate Policy, identified by subarcs of the object identifier **2.16.554.101.8.1.1.6.1** is only permitted as set forth in this document. Use of this document constitutes acceptance of the terms and conditions set out in this document. The acceptance of a Certificate by a Relying Party for a prohibited purpose is at the Relying Party's risk. Engaging in a prohibited Certificate use is a breach of this Certificate Policy and the New Zealand Government disclaims any and all liability in such circumstances. The conditions applicable to each type of New Zealand Government PKI Certificate will vary.

Document Management

This document is controlled by:	Cogito Group
Changes are authorised by:	Lead Agency

Change History

Version	Issue Date	Description/ Amendment	Changed by
0.1 Draft	Jul 2020	Initial draft derived from SEEMail v3.1 CP and CPS	BF
0.2	Sep 2020	Update after review	BF
0.3	Nov 2020	Minor update	BF
0.4	Mar 2021	Update after Review	BF
1.0	Mar 2021	Release	BF
1.1	Mar 2021	Update based on feedback received	BF

Signatures

Appointment	Organisation	Signature
Operations Manager	Cogito Group	
Lead Agency	DIA	

Contents

List of Tables

1. INTRODUCTION

Certificate Policies (CPs) are, in the X.509 version 3 digital certificate standard, the named set of rules regarding the applicability of a *Certificate* to a particular community and/or class of applications with common security requirements. A CP may be used by a *Relying Party* to help in deciding whether a certificate, and the binding therein, are sufficiently trustworthy and otherwise appropriate for a particular application.

This CP identifies the rules to manage the New Zealand Government PKI **SEEMail** *Resource Certificates* that are used to establish secure message signing and encryption using *Secure/Multipurpose Internet Mail Extensions (S/MIME)*. It includes the obligations of the *Public Key Infrastructure* (PKI) entities, and how the parties, indicated below, use them. It does not describe how to implement these rules as that information is in the New Zealand Government PKI SEEMail *Certification Practice Statement* (CPS), or documents referenced by the CPS. In general, the rules in this CP identify the minimum standards in terms of performance, security and/or quality.

The headings in this CP follow the framework set out in Internet Engineering Task Force Request for Comment (RFC) 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

A document hierarchy applies: the provisions of any applicable contract such as a *Subscriber Agreement*, *Deed of Agreement* or other relevant contract override the provisions of this CP. The provisions of this CP prevail over the provisions of CPS to the extent of any direct inconsistency. The provisions of CPS govern any matter on which this CP is silent. (Note: where sub titled sections of the framework provide no additional information to detail provided in the CPS they have not been further extrapolated in this document.)

This section identifies and introduces the set of provisions, and indicates the types of entities and applications applicable for this CP.

1.1 Overview

This CP only applies to certificates issued to *New Zealand Government resources* for the establishment of secure message signing and encryption using S/MIME, and does not apply to other non-individuals (organisations, resources or devices) or any individuals.

No authority, or privilege, applies to a resource by becoming an approved Secure Communications Resource Certificate holder, other than confirming ownership by the New Zealand Government.

The principal documents referenced by this CP are shown in Appendix A. The contents of a referenced document may be classified.

The SEEMail Technical Specification v3.1 is referenced for the creation of the SEEMail End Entity certificate profile

1.2 Document name and identification

The title for this CP is "X.509 Certificate Policy for New Zealand Government PKI SEEMail Certificates". The *Object Identifier* (OID) for this CP is 2.16.554.101.8.1.1.6.1

{joint-iso-itu-t (2) member-body (16)NZ(554) Govt (101) pki (8) certificate policy (1) resource (1) SEEMail (6) version (1)}

Extensions of this OID represent the certificate variants governed by this CP. They are identified in Appendix B.

1.3 PKI participants

1.3.1 Certification authorities

The *Certification Authorities* (CAs) that issue certificates under this CP are New Zealand Government - accredited. For further information, see CPS.

1.3.2 Registration authorities

The *Registration Authorities* (RAs) that perform the registration function under this CP are New Zealand Government - accredited RAs.

Registration (or enrolment) for certificates for issued for use with SEEMail will be the responsibility of the CCCPG, who may elect to delegate performance of the specified activities to an Approved PKI Service Provider

For further information, see CPS.

1.3.3 Subscribers

SEEMail Certificates are only issued to non-person entities (NPE), not individuals.

In this document - and as allowed by the definition of Subscriber in the CPS - the Subscriber of a New Zealand Government PKI SEEMail Certificate may, depending on the context, refer to the NPE whose name appears as the subject in the certificate, or to the person or legal entity that applied for that Certificate.

In some instances, certain responsibilities of the Subscriber (person or legal entity) may be delegated to a Key Custodian. The Subscriber person or legal entity is fully responsible and accountable for the acts or omissions of its delegate.

Participating agencies will be limited to those agencies that have been accepted as members of the SEEMail community by the Common Communications Capability Planning Group (CCCPG).

Participating agency subscribers will receive root, gateway and agency SEEMail certificates from the SEEMail Gateway CA. The Chief Executive (CE) of an approved agency may delegate the task of enrolling for a SEEMail Gateway certificate and managing the issued certificate to a member of their agency.

Participating Trusted Partner organisation subscribers will receive root, gateway and agency SEEMail certificates from the SEEMail Gateway CA. The CE of an approved agency may delegate the task of enrolling for a SEEMail Gateway certificate and managing the issued certificate to a member of their agency

1.3.4 Relying parties

SEEMail Participating Agencies (the definitive list of Participating Agencies is maintained by the SEEMail Product Manager), SEEMail Trusted Partner Participating Organisations (the approved list of Trusted Partner Organisation is maintained by the SEEMail Product Manager), the two SEEMail Gateway CAs and SEEMail Gateway RA

See CPS.

1.3.5 Other participants

See CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The appropriate use for a certificate issued under this CP, in conjunction with its associated private key, are detailed below:

- SEEMail Gateway certificates are issued for restricted use which is limited to either:
    - message signing and message encryption at a domain level using the S/MIME protocol for SEEMail between agencies participating in the SEEMail community
    - the operations of the SEEMail RA such as certificate request submission to the two SEEMail Gateway CAs.
- SEEMail Gateway Certificates are issued for the purpose of domain confidentiality and domain authority. They may be used to sign and encrypt emails using the S/MIME protocol (RFC 3183).
- A SEEMail Gateway Certificate used by a properly configured agency or trusted partner mail gateway will provide assurance to the sending and receiving agencies that it is infeasible to:
    - read the message content (body text) of emails sent between Gateways (confidentiality)
    - alter message content (body text) without detection between Gateways (integrity)
    - pretend to be a SEEMail Gateway when sending (authentication of sending agency).

1.4.2 Prohibited certificate uses

The prohibited uses for certificates issued under this CP are:

- SEEMail Gateway Certificates may NOT be used to secure emails to or from an individual.
- SEEMail Gateway Certificates may NOT be used for securing SSL/TLS connections.
- SEEMail Gateway Certificates may NOT be used for securing information stored in a repository or archive.

Engaging in prohibited certificate use is a breach of the responsibilities and obligations agreed to by the *Registration Officer* (RO).

1.5 Policy administration

1.5.1 Organisation administering the document

See CPS.

1.5.2 Contact person

See CPS.

1.5.3 Authority determining CPS suitability for the policy

See CPS.

1.5.4 CPS approval procedures

See CPS.

1.6 Definitions, acronyms and interpretation

Acronyms and terms used in this CP are defined in the CPS. Note that defined terms in this CP appear in italics the first time they are used and otherwise are not identified in this manner when appearing later throughout the CP. Defined terms may be upper or lower case.

The interpretation clause in Part 3 of Appendix B (B.3) of the CPS also applies to this CP.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

See CPS.

2.2 Publication of certificate information

The New Zealand Government publishes the issuing CA certificate, and the issuing CA's latest CRL in its repository. This information is available to Subscribers and Relying.

The New Zealand Government provides for Subscribers and Relying Parties the URL of a website which the New Zealand Government uses to publish:

i. this CP;
ii. the CP for any end entity certificates; and
iii. the CPS.

2.3 Time or frequency of publication

SEEMail Gateway certificates will be issued to requesting agencies on demand, following successful enrolment by the RA.

SEEMail Gateway certificates issued under this policy will be published once the new certificate and private key has been installed by the agency, it is anticipated this would normally occur within 48 hours.

See 4.9.7 for CRL issuance frequency. For further information, see CPS.

A CRL may be issued at times other than these on demand when a certificate has been revoked following a request from the SEEMail Manager.

2.4 Access controls on repositories

See CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

A clear distinguishable and unique Distinguished Name (DN) must be present in the certificate Subject field.

3.1.2 Need for names to be meaningful

The Lead Agency shall ensure that the DN in subjectName field used to identify the Subject of a certificate is:

iv. Meaningful; and
v. Relates directly to an attribute or identifier of the Resource.

All certificates issued by either SEEMail Gateway CA must include an alternate name for the subject (subjectAltName) consisting of the same RFC 822 email address used in the distinguished name (ie "domain-confidentiality-authority@<agency domain>")

3.1.3 Anonymity of pseudonymity of Subscribers

SEEMail Gateway certificates may NOT be issued to anonymous subscribers. All certificates must be issued to verified agencies entitled to participate in the SEEMail community.

3.1.4 Rules for interpreting various name forms

Not applicable.

3.1.5 Uniqueness of names

Names are unique within the PKI name space.

3.1.6 Recognition, authentication, and role of trademarks

See CPS.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Certificate requests submitted to the CA must be PKCS#10 formatted requests where proof of possession of the Private Key is ensured and that the Key Pair is generated at the time the certificate request is created.

An agency requesting a SEEMail Gateway certificate will demonstrate possession of the private key associated with the certificate request by signing the request to the SEEMail Gateway CA.

A trusted partner organisation requesting a SEEMail Trusted Partner Gateway certificate will demonstrate possession of the private key associated with the certificate request by signing the request to the SEEMail Trusted Partner Gateway CA.

Certificate requests that have not been signed by the associated private key will be rejected by the associated SEEMail Gateway CA.

The SEEMail Gateway CAs will not provide any facility to generate a private key on behalf of the requesting agency.

3.2.2 Authentication of organisation identity

Initial identity validation of agencies applying for a SEEMail Gateway certificate will be performed according the procedures specified in the SEEMail Gateway RA Policy and Operations Manual.

3.2.3 Authentication of individual identity

This CP is for a non-human resource, and not an individual. The identifying characteristics of the resource will be resource specific. The RO authenticates the identity of the resource during the approval of the certification request after checking that the information in the request is correct.

3.2.4 Non-verified subscriber information

All Subscriber information included in the certificate request is verified by the RO.

3.2.5 Validation of authority

Prior to the issue of a certificate, *affiliation* with the New Zealand Government or subscriber organisation is validated by the RO.

3.2.6 Criteria for interoperation

Not Applicable.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and authentication for routine re-key

The SEEMail Gateway RA Policy and Operations Manual specifies the procedures to be followed when authenticating the identity of an agency or trusted partner requesting a replacement SEEMail Gateway certificate approaching expiration of a current SEEMail Gateway certificate.

3.3.2 Identification and authentication for re-key after revocation

See 3.2.2 (Authentication of organisation identity) and 3.2.3 (Authentication of individual identity).

3.4 Identification and Authentication for Revocation Requests

Dual authentication is required for all requests to *revoke* (either two ROs or one RO and a PKI Operator). Prior to revocation, the request is verified and the requestor and reasons documented.

Revocation requests, from sources other than a RO, should be digitally signed. If that is not possible, then a signed letter should be sent by post or fax.

Revocation requests, from sources other than a RO, are authenticated by verifying that the request is signed by the person making the request, validating that the sender is affiliated with the New Zealand Government, and checking that the request contains all the correct and required information.

Only in extraordinary (emergency) circumstances can a revocation request be submitted verbally.

See 4.9 (Certificate revocation and suspension) for more information on revocation.

4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

Application by an agency entitled to participate in the SEEMail community for a SEEMail Gateway certificate must be made in the first instance to the SEEMail RA via the SEEMail RA Portal..

The SEEMail RA will then submit the certificate request to the SEEMail Gateway CA for issuing of the SEEMail Gateway certificate.

Detail on the SEEMail RA Portal including URL will be provided to the Participating Agency by the SEEMail Product Manager upon acceptance as a Participating Agency.

4.1.1 Who can submit a certificate application

The SEEMail RA is the only entity entitled to submit a certificate application to the SEEMail Gateway CAs.

4.1.2 Enrolment process and responsibilities

Using the resource's security functionality, the resource's administrator generates a key pair and submits a certificate request. The RO verifies the information in the request and then approves it for registration. The RA validates and signs the request, and sends it to the CA.

The resource's administrator is responsible for providing accurate information in an application for the correct certificate type. The RO is responsible for checking the accuracy of that information and verifying that the application is for a New Zealand Government resource prior to approval for registration.

The enrolment process used by the SEEMail RA for agencies applying for a SEEMail Gateway certificate is specified in the SEEMail Gateway RA Policy and Operations Manual.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA signs and forwards the certificate request to the CA after receiving registration approval from an RO and validating the request. The CA only certifies certificate requests that are signed by an accredited New Zealand Government PKI RA.

Refer to the SEEMail Gateway RA Policy and Operations Manual

4.2.2 Approval or rejection of certificate applications

A RO may reject or approve a certificate application. Reasons for rejection may include invalid application, insufficient affiliation with the New Zealand Government or subscriber organisation, or the provision of incorrect or insufficient identification details.

For further details refer to the SEEMail Gateway RA Policy and Operations Manual

4.2.3 Time to process certificate applications

See Subscriber Agreement, but if not stipulated then processing of certificate applications will occur in a timely manner.

For further details refer to the SEEMail Gateway RA Policy and Operations Manual

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The SEEMail Gateway CA will verify the certificate request presented by the RA to ensure that all required attributes are present. If required attributers are not present, they will be added. If attributes are present but have unacceptable values, then they will be replaced.

The validated certificate request will then be signed by the SEEMail Gateway CA private key to create the SEEMail Gateway certificate. The signed certificate will be returned to the SEEMail Gateway RA.

For additional information see CPS.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The SEEMail Gateway CA will not notify the subscriber (SEEMail Agency or Trusted Partner) of the certificate issuance. It will instead notify the RA which is responsible for managing the notification to the subscriber. Refer to the SEEMail RA Policy and Operations Manual.

For additional information see CPS.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The agency or trusted partner requesting the certificate will be notified when the certificate is issued, and unless they file a notice of rejection of the issued certificate in accordance with the SEEMail Gateway RA Policy and Operations Manual, the certificate will be deemed to have been accepted.

4.4.2 Publication of the certificate by the CA

The RA will publish SEEMail Gateway certificates on the SEE website where they can be accessed by the requesting agency and other interested parties.

Once a SEEMail Gateway certificate has been accepted by the requesting agency (including deemed acceptance), it will be published on the SEE LDAP directory by the SEEMail RA

See CPS.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Agencies issued with a SEEMail Gateway certificate must use it only for securing messages to/from another SEEMail email gateway with domain signing and domain encryption

4.5.2 Relying party public key and certificate usage

An agency relying on a SEEMail Gateway certificate may only rely on it when it has been used for domain signing or domain encryption to or from another SEEMail email gateway associated with the subject agency.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal is specifically not allowed under this CP, that is SEEMail Gateway RA certificates or SEEMail Gateway certificates may NOT be renewed with the same key pair as a previously issued certificate. Replacement SEEMail RA and Gateway certificates must be issued with new a new key pairs.

The process for obtaining a new certificate to replace an expired or revoked certificate is described above in sections 4.1 through to 4.4.

4.6.2 Who may request renewal

Not stipulated.

4.6.3 Processing certificate renewal requests

Not stipulated.

4.6.4 Notification of new certificate issuance to subscriber

Not stipulated.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not stipulated.

4.6.6 Publication of the renewal certificate by the CA

Not stipulated.

4.6.7 Notification of certificate issuance by the CA to other entities

LDAP is the formal repository and list for members and their certificates. No notification is necessary as each gateway is required to retrieve member/certs periodically.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

SEEMail Gateway certificates may not be re-keyed. If a SEEMail Gateway Certificate expires or is revoked, then any replacement must contain a new key pair which is different from any previously issued SEEMail Gateway certificates.

4.7.2 Who may request certification of a new public key?

Not stipulated.

4.7.3 Processing certificate re-keying requests

Not stipulated.

4.7.4 Notification of new certificate issuance to subscriber

Not stipulated.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not stipulated.

4.7.6 Publication of the re-keyed certificate by the CA

Not stipulated.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificate modification is specifically not allowed under this CP for any certificates issued by the SEEMail Gateway CA. Changes in any certificate, that is SEEMail gateway RA or SEEMail gateway certificates, must entail a certificate re-issuance process.

Specifically, if agency information changes to the extent that a SEEMail Gateway Certificate requires modification, then the agency must request revocation of the old certificate and apply for a replacement certificate with the new information.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

SEEMail Gateway certificates and SEEMail Gateway RA certificates may not be suspended, but must be revoked and re-issued if required.

4.9.1 Circumstances for revocation

See CPS.

4.9.2 Who can request revocation

See CPS.

4.9.3 Procedure for revocation request

Refer to the SEEMail Gateway RA Policy and Procedures Manual.

4.9.4 Revocation request grace period

Not applicable.

4.9.5 Time within which CA must process the revocation request

The CA will process the revocation request as soon as practicable and within two hours during normal business hours, or eight hours outside this period.

4.9.6 Revocation checking requirement for relying parties

Participating Agencies and Trusted Partners are required to check the status of a SEEMail Gateway certificate, all SEEMail Intermediate CA certificates and SEEMail Gateway RA certificate before they may rely on it by confirming that it does not appear on the most recent CRL issued by the respective SEEMail issuing CA.

For practical purposes and to avoid excessive network traffic and processing delays, relying parties may cache a retrieved CRL for a period not exceeding one hour. If no CRL is available, then relying parties may use a cached CRL for a period not exceeding seven days.

See CPS for any further revocation checking requirements.

4.9.7 CRL issuance frequency (if applicable)

CRLs for the SEEMail Gateway CA are published on each certificate revocation or at intervals no longer than 24 hours, if there are no other updates in that period.

The CRL lifespan for the SEEMail Gateway CA is 10 days.

4.9.8 Maximum latency for CRLs (if applicable)

4.9.9 The maximum latency between the generation and publication of CRLs is 3 days.On-line revocation/status checking availability

Online Certificate Status Protocol service (OCSP) is available at:

http://ocsp.pki.govt.nz/

Refer to the relevant Certificate Profile in Appendix B - if the certificate is issued with an OCSP access location reference (Authority Information Access extension), OCSP is available to the Relying Party as a certificate status checking method.

The latest CRL is available from the published repositories; refer to 2.1 (Repositories) and the certificates CRL Distribution Point for further information.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

See CPS.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

Certificate suspension is not supported under this CP.

4.9.14 Who can request suspension

Certificate suspension is not supported under this CP.

4.9.15 Procedure for suspension request

Certificate suspension is not supported under this CP.

4.9.16 Limits on suspension period

Certificate suspension is not supported under this CP.

4.10 Certificate status services

4.10.1 Operational characteristics

See CPS.

4.10.2 Service availability

See CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

If a SEEMail Agency ceases to be eligible for participation in the SEEMail community, the Product Manager will request revocation of any SEEMail Gateway Certificates currently issued to that agency.

For further details see CPS.

4.12 Key escrow and recovery

Keys will not be escrowed, key recovery is not supported.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

See CPS.

5.2 Procedural controls

See CPS.

5.3 Personnel controls

See CPS.

5.4 Audit logging procedures

See CPS.

5.5 Records archival

5.5.1 Types of records archived

See CPS.

5.5.2 Retention period for archive

See CPS.

5.5.3 Protection of archive

See CPS.

5.5.4 Archive backup procedures

See CPS.

5.5.5 Requirements for time-stamping of records

See CPS.

5.5.6 Archive collection system (internal or external)

No Stipulation.

5.5.7 Procedures to obtain and verify archive information

See CPS.

5.6 Key changeover

See CPS.

5.7 Compromise and disaster recovery

See CPS.

5.8 CA or RA termination

See CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Keys are primarily generated locally within the gateway during the requesting process. Where a key pair is generated on behalf of the gateway, the generation occurs centrally by a *trusted* role and following the placement of the keys in the custody of the resource the copy of the key pair is destroyed.

6.1.2 Private key delivery to subscriber

Generally the key generation is performed within the gateway so no delivery is required. Where keys are generated externally the private key is delivered to the subscriber within a protected container known as a PKCS#12 file. The PKCS#12 format ensures the private key data is encrypted, and is only accessible with the provision of an unlocking password.

Where gateways are working in a failover configuration, cloning of the key pair and certificate is permitted. It is the Gateway administrator's responsibility to ensure that they are installed in the correct location(s).

6.1.3 Public key delivery to certificate issuer

Where keys are generated within the Gateway, its public key is provided to the CA in a PKCS#10 certificate request file signed with the corresponding private key.

6.1.4 CA public key delivery to relying parties

See CPS.

6.1.5 Key sizes

Key sizes will be a minimum of 384 bit ECC secp384r1.

6.1.6 Public key parameters generation and quality checking

See CPS.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Keys issued under this CP allow a Subscriber to encrypt data for email transmission between gateways. See Appendix B and CPS for further information.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

See CPS.

6.2.2 Private key (n out of m) multi-person control

See CPS.

6.2.3 Private key escrow

Escrow of keys does not occur.

6.2.4 Private key backup

See CPS.

6.2.5 Private key archival

See CPS.

6.2.6 Private key transfer into or from a cryptographic module

See CPS.

6.2.7 Private key storage on cryptographic module

See CPS.

6.2.8 Method of activating private key

Activating private keys occurs by the Gateway authenticating to the cryptographic module.

6.2.9 Method of deactivating private key

Deactivation can be achieved via:

i. shut down or restart of the system; or
ii. shut down of the service that exercises the private key.

6.2.10 Method of destroying private key

See CPS.

6.2.11 Cryptographic Module Rating

See CPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See CPS.

6.3.2 Certificate operational periods and key pair usage periods

The Subscriber certificate has a maximum validity period of 2 years to limit the key lifetime. For further information, see CPS.

6.4 Activation data

6.4.1 Activation data generation and installation

No Stipulation.

6.4.2 Activation data protection

See CPS.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

See CPS.

6.6 Life cycle technical controls

See CPS.

6.7 Network security controls

See CPS.

6.8 Time-stamping

See CPS.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates are X.509 Version 3 certificates.

7.1.2 Certificate extensions

See Appendix B.

7.1.3 Algorithm object identifiers

Certificates under this CP will use one of the following OIDs for signatures.

ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

Table 1 - Signature OIDs

Certificates under this CP will use one of the following OIDs for identifying the algorithm for which the subject key was generated.

id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12) }
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Table 2 - Algorithm OIDs

7.1.4 Name forms

All SEEMail Gateway certificates issued by the SEEMail Gateway CAs will contain a distinguished name with the following name components:

- E – email address (“domain-confidentiality-authority@<organisation domain>”)
- CN – common name (“domain-confidentiality-authority”)
- OU – organisation unit (“SEEMail”)
- O – organisation (“Organisation Full Name”)
- C – country (“NZ”)

The SEEMail Gateway certificates issuer field will contain the following name components:

- CN – common name (SEEMail Intermediate CA Name), Intermediate CA Name can be:
  - “SEEMail V3.1 Intermediate CA”
  - “SEEMail V3.1 Trusted Partners CA”
- OU – organisational unit (“Government Technology Services”)
- O – organisation (“Department of Internal Affairs”)

- C – country (“NZ”)

All SEEMail Gateway certificates issued by the SEEMail Gateway CAs will have a common name (“CN”) of “domain-confidentiality-authority”.

See CPS and Appendix B for further information.

7.1.5 Name constraints

Name constraints are not present.

7.1.6 Certificate policy object identifier

Certificates issued under this CP shall assert this CPs OID (or an extension of it – See Appendix B for variants):

{2.16.554.101.8.1.1.6.1)

Certificates issued under this policy shall also assert the following LoA OID:

{2.16.554.101.8.2.2.2.1} Level of Assurance – Medium (Resource)

In addition; to enable the use of the certificate at lower Levels of Assurance, this policy also asserts the following OID:

{2.16.554.101.8.2.2.1.1} Level of Assurance – Low (Resource).

See also Appendix B.

7.1.7 Usage of policy constraints extension

See Appendix B.

7.1.8 Policy qualifiers syntax and semantics

See Appendix B.

7.1.9 Processing semantics for the critical certificate policies extension

This CP does not require the certificate policies extension to be critical. Relying Parties whose client software does not process this extension do so at their own risk.

7.2 CRL profile

7.2.1 Version number(s)

CRLs issued shall be X.509 version 2.

7.2.2 CRL and CRL entry extensions

See Appendix C.

7.3 OCSP profile

7.3.1 Version Numbers

OSCP is implemented using version 1 as specified under RFC 6960.

7.3.2 OCSP Extensions

Refer to CPS and Validation Authority (VA) CP for full OCSP profile.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

See CPS.

8.2 Identity/qualifications of assessor

See CPS.

8.3 Assessor's relationship to assessed entity

See CPS.

8.4 Topics covered by assessment

See CPS.

8.5 Actions taken as a result of deficiency

See CPS.

8.6 Communication of results

See CPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

There is no fee for accessing Certificates from approved repositories.

9.1.3 Revocation or status information access fees

There is no fee for accessing the CRL from approved repositories.

9.1.4 Fees for other services

See CPS regarding fees for access to this CP. No fee has been stipulated for other services.

9.1.5 Refund policy

See CPS.

9.2 Financial responsibility

9.2.1 Insurance

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

See CPS.

9.3.1 Scope of confidential information

SEEMail Gateway certificates are approved for use in securing messages between Participating Agencies that contain information with a government security classification of RESTRICTED/SENSITIVE or below.

See CPS for further information.

9.3.2 Information not within the scope of confidential information

Government information with a security classification of greater than "Restricted" or information which must be limited to specific individuals MUST not be protected by SEEMail Gateway Certificates.

9.3.3 Responsibility to protect confidential information

The agencies participating in the SEEMail community are responsible for protecting information properly secured by SEEMail Gateway Certificates within their own borders.

For further information see CPS.

9.4 Privacy of personal information

SEEMail Gateway Certificates pertain to non-person entities, not individuals, and do not contain any personal information (as defined in the Privacy Act 1993).

9.5 Intellectual property rights

See CPS.

9.6 Representations and warranties

See CPS.

9.6.1 CA representations and warranties

See CPS.

9.6.2 RA representations and warranties

See CPS.

9.6.3 Subscriber representations and warranties

As the trusted role responsible for the private keys, the relevant Key custodian warrants to:

i. only use Keys and digital certificates within the limits specified in the CP;
ii. take all reasonable measures to protect the Private Key(s) in their custody from compromise and take all necessary precautions to prevent loss, disclosure, modification, or unauthorised use of the Private Key(s); and
iii. promptly notify the RA in the event that they consider or suspect there has been a compromise of the Private Key(s).

Each participating SEEMail agency subscribing to a SEEMail Gateway Certificate undertakes to use the certificate only for securing SEEMail messages between participating agencies as specified in this document.

9.6.4 Relying party representations and warranties

Relying parties undertake to rely on a SEEMail Gateway Certificate only when it has been used to secure SEEMail between participating agencies as specified in this document.

Certificates issued under this CP do not contain, or imply, any authority, access or privilege. Relying Parties assume responsibility for any financial limit they may wish to apply for transactions authenticated using certificates issued under this CP.

For further information see CPS

9.6.5 Representations and warranties of other participants

Other participants may NOT use or rely on SEEMail Gateway Certificates except as expressly specified in this document.

9.7 Disclaimer of warranties

See CPS.

9.8 Limitations of liability

See CPS.

9.9 Indemnities

See CPS.

9.10 Term and termination

9.10.1 Term

This CP and any amendments shall become effective upon publication in the Repository and shall remain in effect until the notice of its termination is communicated by the New Zealand Government PKI on its web site or Repository.

9.10.2 Termination

See CPS.

9.10.3 Effect of termination and survival

See CPS.

9.11 Individual notices and communications with participants

See CPS.

9.12 Amendments

See CPS.

9.13 Dispute resolution provisions

See CPS.

9.14 Governing Law

See CPS.

9.15 Compliance with Applicable Law

See CPS.

9.16 Miscellaneous provisions

See CPS.

9.17 Other provisions

See CPS.

APPENDIX A. REFERENCES

The following documents are referenced in this CP:

[CPS]	X.509 Certification Practice Statement for the New Zealand Government, available at http://www.pki.govt.nz/policy/
[6960]	RFC6960 Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol (ocsp), Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6960.txt
[3647]	RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc3647.txt
[6818]	RFC6818 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet Engineering Task Force, available at http://www.ietf.org/rfc/rfc6818.txt
[KMP]	New Zealand Government Public Key Infrastructure Key Management Plan (classified)
[LOA]	New Zealand Government Public Key Infrastructure Assurance Level Requirements document, available at http://www.pki.govt.nz/policy/
[RCA CP]	X.509 Certificate Policy New Zealand Government Root Certification Authority and Subordinate Certificate Authorities, available at http://www.pki.govt.nz/policy
[VA CP]	X.509 Certificate Policy for New Zealand Government Validation Authority Certificates, available at http://www.pki.govt.nz/policy
[Privacy Act]	New Zealand Privacy Act 1993 http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

Table 3 - References

APPENDIX B. CERTIFICATE PROFILES

NB. Variations associated with this Annex will occur over time due to technical implementations. As such variations will be marginal and not materially affect the certificates issued under this CP they will not be reviewed by the Accreditation Authority.

B.1 SEEMail End Entity Certificate

Field	Critical	Value	Notes
Version		V3 (2)	
Serial		<*octet string*>	Must be unique within the New Zealand Government namespace
Issuer signature algorithm		ecdsa-with-SHA384	
Issuer distinguished name		CN= NZGovtCA<serial> OU= CAs OU= PKI O= Govt C= NZ	Encoded as printable string. <Serial> denotes the number after "NZGovtCA" that represents the issuing CA. and is expected to start at "301".
Validity period		Not before <UTCtime> Not after <UTCtime>	2 years from date of issue
Subject distinguished name		E=domain-confidentiality-authority@<email domain> CN= <Agency email domain> OU=SEEMail O=<Subscribing Agency> C=NZ	Note: This is an example only, actual distinguished names will describe the subscriber organisation
Subject public key information		ecdsa-with-SHA384	ECDH_P384
Issuer unique identifier		-	Not Present
Subject unique identifier		-	Not Present
X.509 v3 extensions			
Authority key identifier	No	<*octet string*>	384 bit SHA384 hash of binary DER encoding of signing CA's public key
Subject key identifier	No	<*octet string*>	384 bit SHA384 hash of binary DER encoding of subject's public key
Key usage	Yes	digitalSignature Non-Repudiation keyEncipherment	
Extended key usage			
Private key usage period		-	Not Present
Certificate policies	No	[1] Policy Id: {2.16.554.101.8.1.1.6.1} Policy qualifier – CPS pointer: https://www.pki.govt.nz/policy/	The OID of this CP
Policy mapping		-	Not Present
Subject Alternative Name		RFC822 Name=domain-confidentiality-authority@<email domain>	Not Present

Field	Critical	Value	Notes
Issuer alternative name		-	Not Present
Subject directory attributes		-	Not Present
Basic constraints		Subject Type=End Entity Path Length Constraint=None	Not Present
Name constraints		-	Not Present
Policy constraints		-	Not Present
Authority information access	No	[1] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/Certificates/NZGovtCA<serial>.crt [2] Access method: CAIssuer{1.3.6.1.5.5.7.48.2} Access location: http://cert.pki.govt.nz/pki/Certificates/NZGovtCA<serial>.p7b [3] Access method: OCSP {1.3.6.1.5.5.7.48.1} Access location: http://ocsp.pki.govt.nz	
CRL Distribution Point	No	[1] Distribution Point Name (http): http://crl.pki.govt.nz/crl/NZGovtCA<Serial>.crl [2] Distribution Point Name (ldap): ldap://dir.pki.govt.nz/cn=NZGovtCA<serial>,ou=CAs,ou=PKI,o=Govt,c=NZ?certificateRevocationList	The CRL distribution point extension shall only populate the distributionPoint field. The field shall only contain the URI name form. The reasons and cRLIssuer fields shall not be populated. The CRL shall point to a full and complete CRL only (i.e., a CRL that does NOT contain the issuer distribution point extension).

Table 4 – Certificate Profile – Variation 1 – SEEMail End Entity Certificate

APPENDIX C. CRL FORMAT

Please refer to the issuing CA's Certificate Policy.