

# Secure Electronic Environment Project



## S.E.E. PKI Certificate Policy

Security Requirements for Public Key Certificates  
Used to Access SENSITIVE Computer Systems

**Version 2.0**

Franz Ombler – The Treasury

Mike Pearson – State Services Commission

# 1 INTRODUCTION

## 1.1 Overview

1. This Policy defines the requirements for the management of cryptographic public key pairs and X.509 public key certificates used by the New Zealand Government to

- Access computer systems classified up to SENSITIVE;
- Authenticate individuals and devices;
- Provide authentication of roles and proof of membership;
- Provide authentication by proxy.

2. This policy defines security practices and mechanisms appropriate for certificates and keys used to identify and authenticate entities passing, holding, processing or accessing information classified up to and including SENSITIVE or RESTRICTED. It is not suitable for use with information classified CONFIDENTIAL and above, without additional measures.

3. This Policy is intended to support applications such as single sign-on, virtual private networks and remote access. It does not specifically consider the requirements for certificates and keys used for encryption (privacy and confidentiality services) or for digital signatures (i.e., proof after the fact or by a third person). It does not exclude the use of certificates and keys for such purposes.

4. This Policy is a deliverable of the State Services Commission's E-government initiative, associated with the Secure Electronic Environment (S.E.E.) project, [www.see.govt.nz](http://www.see.govt.nz). The management authority for the S.E.E project is the S.E.E. Steering Group. As such, the S.E.E. Steering Group is the controlling authority for this document.

5. This Policy is written to comply with Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527), <http://www.ietf.org/rfc/rfc2527.txt>. The terms “must”, “should” and “may” are interpreted as set out in RFC 2119, <http://www.ietf.org/rfc/rfc2119.txt>.

## 1.2 Identification

6. The alphanumeric Object Identifier (OID) of this Policy is **SEEKEY\_1\_0**.

7. The full numeric OID is **2.16.554.101.2.1.1**.

8. Certificates issued under this policy will be termed “SEEKEY Certificates”.

9. This policy will be referred to as the “S.E.E. Key Certificate Policy” or “S.E.E. Key CP”.

## 1.3 Community and Applicability

### 1.3.1 Certification authorities

10. The definition of a Certification Authority (CA) under this Policy is a party that **will**

- create and sign digital certificates binding Subscribers with the public component of their asymmetric cryptographic key pairs;
- promulgate certificate status through Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP); and
- enforce the requirements of the Certificate Policy within the entities it has issued certificates for (i.e., CA staff, Registration Authorities, Sponsors and Subscribers).

11. The CA is responsible for either supplying or confirming an individual's requirement for, and the attribute details in, a PASSPORT certificate, as specified in the [SEEKEY Certificate Table](#).

### 1.3.2 Registration Agents

12. A Registration Agent (RA) is responsible for administration of Subscribers on behalf of a CA. The RA is an agent of the CA.

13. An RA **may** act as an agent for more than one CA or public key infrastructure.

### 1.3.3 End entities

14. **Sponsor** – This policy introduces the concept of a Sponsor. The Sponsor is responsible for either supplying or confirming an individual's requirement for, and the attribute details in, a BUSINESS CARD, ASSOCIATE or ANONYMOUS certificate, as specified in the [SEEKEY Certificate Table](#).

15. The Sponsor will typically be a department or public servant that has nominated an individual or organisation to be issued.

16. The Sponsor is responsible for informing the CA or RA if the department's relationship with the Subscriber is terminated or changed such that the certificate should be revoked or updated.

17. The same person or group as the RA role may perform the Sponsor role.

18. **End users** - This policy is for the authentication of employees of government departments and agencies, and device authentication, within the New Zealand Government, not the general public or private business.

### 1.3.4 Applicability

19. Certificates can be characterised into **Certificate Types**, by combining three specific but extensible sets of attributes. Square brackets indicate an optional attribute

- 1. Certificate class, (cATTRIBUTE): PASSPORT or BUSINESS CARD or ASSOCIATE or ANONYMOUS
- 2. Certificate storage (sATTRIBUTE): SMART-TOKEN, PROXY
- 3. Certificate purpose (pATTRIBUTE): ACCESS or (ID, [SIGN,] ENCRYPT)

20. This Policy allows several Certificate Types, as specified in the [SEEKEY Certificate Table](#), typically used for ACCESS or ID. An ID certificate may also include SIGN and/or ENCRYPT functionality.

21. Note that in the context of this document, the term Certificate Types is used to differentiate among certificates used for slightly different purposes and which have different rules around their use, issuance and reliance; they are thus formally different certificates and will have different Policy OIDs, but are governed by the same Certificate Policy.

22. The S.E.E. Steering Group **may** accredit a CA for one or more of these Certificate Types.

23. **Identity certificates**, have several sub-uses, which provide proof of identity for

- Individual (person)
- Device (machine)
- Role (person(s) in a role)
- Membership (person has eligibility)
- Proxy (machine acting for a person)

24. **Access** certificates act similar to a physical key. They also have several sub-types

- Access to a resource
- Anonymous access

25. Possession of an "access to a resource" certificate, acts like a physical key, the user can access a resource, such as an encrypted laptop.

26. An “anonymous access” certificate is similar to “access to a resource”, but has little or no identifying information – the equivalent of an unlabelled key – it provides access, but anyone finding it, must know where to present it, to be given access.

27. The [SEEKEY Certificate Table](#) defines the variations differentiated by the Certificate Alphanumeric OID, the Certificate Numeric OID and the Certificate `subjectName` Distinguished Name (DN) conventions.

## 1.4 Contact Details

28. The contact person is the S.E.E. Project Manager, who can be contacted at [pki@security.govt.nz](mailto:pki@security.govt.nz).

# 2 GENERAL PROVISIONS

## 2.1 Obligations

### CA and RA Obligations

29. CAs and RAs **must** operate in accordance with their Certification Practice Statement (CPS), the current version of this Policy, and the laws of New Zealand when issuing and managing the certificates and keys provided to S.E.E Key RAs and Subscribers.

### CA Obligations

30. The Certification Authority **must**

- Ensure that RAs, Sponsors, Subscribers are aware of their rights and obligations with respect to the operation and management of keys, certificates and cryptographic modules.
- Ensure any CA public key approved for S.E.E. PKI use is only used to issue certificates compliant with the certificate policies approved for S.E.E. PKI (i.e. the CA must not issue lower assurance certificates with that particular CA key)
- Verify in writing that they comply with this Policy and from time to time conduct compliance audits if requested to do so by the S.E.E. Steering Group. Such compliance audits will be conducted at the CA’s cost;
- Have mechanisms and procedures to ensure that their RAs, Sponsors or End-users, issued with a SEEKEY, have also agreed to abide with this Policy;
- Have at least one CRL repository associated with them;
- Make the CRLs and OCSP services they manage available to Subscribers and Relying Parties in accordance with [Operational Requirements \(Section 4\)](#).
- Provide a web site for Subscriber and Relying Party access to the documents that define their rights and responsibilities.
- Provide any Sponsor with a list of all certificates issued using its name within one working day of request, including the status of each certificate, the certificate’s `subjectName`, and its expiry date.
- Ensure that the procedures for the expiration, revocation and re-issuance of their certificates conform to this Policy and are expressly stated in their CPSs and any Subscriber agreements or policies.
- Ensure that when they revoke a certificate all relevant CRL and OCSP servers are updated and published within one working day of notification.

31. The Certification Authority **should** provide an OCSP service.

32. The Certification Authority **may**

- Create Subscriber key pairs.
- Issue, recognise or support any number of certificate policies as long as the requirements of

one do not affect compliance to the requirements of another, i.e. a CA issuing certificates under this Policy is not limited to only this Policy.

### Sponsor Obligations

#### 33. The Sponsor **must**

- Ensure that any information submitted to a CA/RA when applying, updating or requesting revocation of a certificate is complete and accurate.
- Only request BUSINESS CARD and ASSOCIATE certificates with organisation names for which they are authorised to act.
- Only request BUSINESS CARD certificates with internet domain names (e.g. in email addresses and urls) that are in the control of the organisation name requested.
- Notify the CA / RA when an End-entity certificate is no longer required or if they suspect private key compromise.

### Subscriber Obligations

#### 34. The Subscriber **must**

- Ensure that any information submitted to a CA / RA / Sponsor when applying, updating or requesting revocation of a certificate is complete and accurate.
- Protect their private keys and key tokens (if applicable) in accordance with [Section 6](#), and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorised use.
- Notify their Sponsor as soon as possible, if they suspect private key compromise.

## 2.2 Liability

35. Accreditation of or the issue of certificates by a CA in relation to S.E.E. Key **does not** permit or authorise under any circumstances the CA to conduct business transactions or otherwise act on behalf of the organisation using the certificates or the New Zealand government.

36. A Relying Party **must not** assume that a subscriber has any authority to conduct business transactions or otherwise act on behalf of the subscriber's organisation based solely on the fact that the subscriber has a certificate.

37. A Relying Party **must** consider the differences among Certificate Types, as specified in the [SEEKEY Certificate Table](#), and assign a level of trust consistent with business purpose.

## 2.3 Financial Responsibility.

38. No stipulation.

## 2.4 Interpretation and Enforcement

39. New Zealand law **must** govern certificates issued under this policy.

### Dispute Resolution – Escalation, Arbitration

#### Principles

40. The parties **must** use their best efforts to resolve any dispute that may arise under the Accreditation Process through good faith negotiations.

41. The parties acknowledge their desire that any irreconcilable dispute or difference shall be resolved by mediation. This is without prejudice to any other right or entitlement that they may have. The rules governing any mediation shall be agreed between the Parties. The Parties agree to the assistance of LEADR (Lawyers involved in Alternative Dispute Resolution) to set the terms of reference for any such

mediation and/or to procure mediation at equal cost to the parties or on such other terms as the Parties agree.

### Process

42. If an irreconcilable dispute or difference arises between any two parties, either party may seek request that the dispute be submitted for mediation within 14 days by way of written notice by one party to the other.

43. However where an irreconcilable dispute or difference arises between the Applicant and the S.E.E. Manager as a result of an application for Accreditation by a supplier, or from the Accreditation Process, the dispute shall first be referred to the S.E.E. Steering Group for discussion and resolution.

44. If an irreconcilable dispute or difference is not submitted for mediation within 14 days of written notice by one party to the other, or resolved by mediation, either party may by way of 14 days written notice to the other require the matter to be determined by the arbitration of a single arbitrator in accordance with the provisions of the Arbitration Act 1996 (as amended by this Agreement).

The arbitrator shall be appointed by the parties or, failing agreement within five Working Days of such notice, appointed as soon as possible by the President of the New Zealand Law Society at the request of either party. The arbitration shall be conducted as soon as possible at Wellington.

The parties shall continue to perform their obligations as far as possible as if no dispute had arisen pending the final settlement of any matter referred to mediation or arbitration.

Nothing in this section shall preclude either party from taking immediate steps to seek urgent interlocutory relief before a New Zealand Court.

## 2.5 Fees

45. No stipulation.

## 2.6 Publication & Repository

46. The Certification Authority **must**

- Ensure that all NZ Government Relying Parties have access to current CRLs and OCSP services from the locations and via the protocols specified in its certificates' `cRLDistributionPoint` and `authorityInfoAccess` fields
- Ensure that the CRLs and OCSP services specified in the `cRLDistributionPoint` and `authorityInfoAccess` fields in the certificates must specify locations accessible via the Internet over LDAP and/or HTTP.
- Publish a copy of this Policy and a public version of its CPS on its web site

## 2.7 Compliance Audit

47. The CA **will** be required to

- Provide resource to the accreditation/audit process
- Pay for all costs incurred in their accreditation/audit

48. The Certification Authority **must**

- Notify the S.E.E. Steering Group prior to making any substantive change to their operations that could affect the likelihood of being successfully re-accredited;
- Provide a full CPS when necessary for the purposes of any audit or accreditation;

### Periods of Notice

49. The following periods of notice **will** apply to the Accreditation/Audit Process.

- (a) The S.E.E. Steering Group will give Applicants five (5) working days notice of termination of the Accreditation/Audit Process.

- (b) Applicants will give the S.E.E. Steering Group five (5) working days notice of their intention to withdraw from the Accreditation/Audit Process.
- (c) The S.E.E. Steering Group will give Applicants and Accredited Suppliers
  - Fourteen (14) days notice of changes or variations to the Accreditation/Audit process
  - Fourteen (14) days notice of changes or variations to its requirements.
- (d) Applicants or Accredited Suppliers will give notice by e-mail, to the S.E.E. Steering Group. The period of notice will commence from the time of acceptance of that notice by the S.E.E. Steering Group. Acceptance will be notified by return e-mail to the person(s) who is authorised by the Applicant or Accredited Supplier to act on behalf of their organisation for the purposes of the Accreditation Process.
- (e) The S.E.E. Steering Group will give notice by e-mail to the person(s) who is authorised by the Applicant or Accredited Supplier to act on behalf of their organisation for the purposes of the Accreditation Process. The period of notice will commence at the time of dispatch of the e-mail.

The S.E.E. Steering Group reserves the right to amend the Accreditation or Audit Process, its requirements and/or this Document and to make any changes whatsoever, including cancelling the Accreditation Process and the S.E.E project itself. Applicants and Accredited Suppliers will be notified of any changes to the requirements in accordance with the notice provisions detailed in this document.

### Accreditation

50. The Certification Authority **must** have been accredited by the S.E.E. Steering Group, BEFORE they can issue any S.E.E. PKI certificate.

51. The Certification Authority is eligible for accreditation if they provide a statement of compliance with this Certificate Policy and has either

- (a) undergone an independent audit (evidence of audit) deemed acceptable by the S.E.E. Steering Group; or
- (b) been accredited to another scheme approved by the S.E.E. Steering Group (third party accreditation); or
- (c) been accredited to another scheme approved by the S.E.E. Steering Group, and the differences between that scheme's CP and the S.E.E. CP has undergone an independent audit (audit to S.E.E. PKI CP)

52. At the time of application for accreditation, the Certificate Authority **must** provide the S.E.E. Steering group

- A copy of the CA's most recent audited annual report
- The CA's proposed Certificate Practice Statement (CPS)
- A formal comparison of the CPS with the S.E.E. Key CP (this document)
- A letter indicating whether the proposed CA matches the requirements of the S.E.E. Key CP, indicating any potentially controversial areas of compliance
- Any certificate of accreditation from another body
- Access to relevant audit reports of CA operations
- Access to CA operations centres where requested

53. The S.E.E. Steering Group reserves the right to accept or decline any application for accreditation received.

54. The formal comparison of the CPS with the S.E.E. Key CP **must**

- Compare the documents on a paragraph-by-paragraph basis
- Mark each paragraph with either "Pass" or "Fail" in each case.

- For each paragraph where your proposal satisfies S.E.E. Key needs but there is not an accurate match of policies between the CP and CPS, complete the sentence "Meets because..."
- Mark each paragraph as to whether compliance has been audited by an independent auditor.

55. During the accreditation process the Certificate Authority **must** make available on request CRL, OCSP services and FOUR (4) digital certificates, to each of up to FIVE (5) S.E.E. application owners selected by the S.E.E. Steering Group to test the proposed certificates with their applications.

56. The S.E.E. Steering Group may accredit the CA, on completion of the accreditation process, and verification that the CA satisfies other local conditions. Accreditation will be at the discretion of the S.E.E. Steering Group and may be withdrawn at any time.

### **Withdrawal of accreditation**

57. In the event that the S.E.E. Manager is considering withdrawal of S.E.E. Key accreditation, the following process will be used.

58. The S.E.E. Manager will send the Certification Authority an email notice that they intend to recommend withdrawal of S.E.E. Key accreditation.

59. The e-mail will include

- The reason for the withdrawal of accreditation;
- The withdrawal of accreditation process;
- The contact details of the S.E.E. Steering Group chair;
- The contact details of the S.E.E. Manager.

60. The Certification Authority will have 14 days to resolve the matter to the satisfaction of the S.E.E. Manager.

61. If after 14 days, the S.E.E. Manager still considers withdrawal of S.E.E. Key accreditation necessary, the S.E.E. Manager will recommend to the S.E.E. Steering Group that accreditation should be withdrawn.

62. The S.E.E. Manager will invite the Certification Authority to present any counter argument to the S.E.E. Steering Group. The CA will be required to present its case in writing within 7 days of the invitation. The CA may also request to be heard orally by the S.E.E. Steering Group.

63. The S.E.E. Steering Group's decision will be final.

64. In the event that accreditation is withdrawn

- The Certification Authority **must** offer Sponsors, or in the case of PASSPORT certificates, the Individual, the choice of either the destruction or the return of all backed up or escrowed private keys managed by the CA. All costs associated with return or destruction of private keys will be met by the CA.
- The Certification Authority **must** continue to provide certificate status checking, and certificate revocation services as per this document, for a period of one year unless agreed otherwise between the S.E.E. Manager and the CA.
- The Certification Authority **must not** continue to sell or issue S.E.E. branded certificates.

### **Audit**

65. The Certification Authority **must** demonstrate a commitment to ongoing audit of CA operations.

66. The results of the audit **must** be provided to the S.E.E. Steering Group as soon as practicable and at no cost.

67. The S.E.E. Steering Group **may** require that the Certification Authority be audited

- Prior to initial approval by the S.E.E. Steering Group;

- Upon breach of any part of the S.E.E. Certificate Policy

## 2.8 Confidentiality of Information

68. Private keys **must** be protected in accordance with [Technical Security Controls \(Section 6\)](#)

69. The Subscriber **must** protect his or her private key from disclosure to any other party, unless required by law.

70. No party **shall** make backups of a Subscriber or Sponsor's private keys without the prior consent of the Subscriber or Sponsor. Backups of private keys **shall not** be made available to any party other than the Subscriber or Sponsor without the prior consent of the Subscriber or Sponsor, unless required by law.

71. The Certification Authority **must** ensure

- Information collected is only be used for digital certificate management purposes;
- It complies with the Privacy Act of New Zealand 1993.

## 2.9 Intellectual Property Rights

72. No stipulation.

# 3 IDENTIFICATION & AUTHENTICATION

## 3.1 Initial Registration

### 3.1.1 Types of names

No stipulation.

### 3.1.2 Need for names to be meaningful

No stipulation.

### 3.1.3 Rules for interpreting various name forms

No stipulation.

### 3.1.4 Uniqueness of names

73. The Certification Authority processes must be such that the existence of the keyword SEEKEY in the CN is proof that the certificate was issued under the S.E.E. Key Certificate Policy. Note this gives the CA flexibility to produce other certificates using the same CA root key.

### 3.1.5 Name claim dispute resolution procedure

No stipulation.

### 3.1.6 Recognition, authentication and role of trademarks

No stipulation.

### 3.1.7 Method to prove possession of private key

No stipulation.

### 3.1.8 Authentication of organization identity

74. The CA **must** get authorisation from the organisation to produce each certificate it produces with that organisation's name in the Distinguished Name. Authorisation **shall** be from the chief executive or a company director, or a Sponsor explicitly delegated by them for the management of digital certificates issued under the organisation's name.

### 3.1.9 Authentication of individual identity

75. Respective identities **must** be confirmed prior to the exchange of a public or private key or the issuance of a certificate.

- For PASSPORT certificates, the Certification Authority or RA and the Subscriber **must** confirm their respective identities
- For BUSINESS CARD and ASSOCIATE certificates, the Certification Authority or RA and the Sponsor **must** confirm their respective identities.

76. The appropriate mechanisms for confirming respective identities are either

- In person,
- Through the use of a shared secret (e.g., secret key or password), or
- Through the use of pre-positioned asymmetric key pairs,

77. The key transfer protocol described in the PKIX Certificate Management Protocol is suitable for the above tasks.

## 3.2 Authentication for Routine Rekey

78. The Certification Authority or RA **must** authenticate all requests by Subscribers and Sponsors for issuance of new certificates and key pairs, and subsequent responses.

79. This authentication **may** be done by an online method in accordance with the PKIX Certificate Management Protocol where the Entity is authenticated using its current key pair.

## 3.3 Rekey after Revocation

The Certification Authority or RA **must** re-authenticate the entity in the same manner as for initial registration when there is a known or suspected compromise of an entity's private key.

80. The Certification Authority or RA **must** verify any change in the information contained in a certificate – via the Sponsor where applicable - before an updated certificate is issued.

## 3.4 Revocation Request

81. No stipulation.

# 4 OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

## 4.2 Certificate Issuance

82. The CA **must** ensure any public key approved for S.E.E. PKI use is only used to issue certificates under the certificate policies approved for S.E.E. PKI (i.e. the CA must not issue lower assurance certificates with that particular CA key).

83. The CA's registration process **must** be sufficiently rigorous that for **PASSPORT certificates**

- It is at least as rigorous as the Australian GateKeeper Project 100 point system
- The email address is reliable and approved by the individual, e.g. this should be tested by sending an email to the address, and requesting a reply confirming the validity of the application.
- It, or one of its RAs has verified the identity and authorisation of the Subscriber in accordance with [Identification & Authentication \(Section 3\)](#)
- The details in the certificate must match the Subscriber's details,

84. The CA's registration process **must** be sufficiently rigorous that for **BUSINESS CARD certificates**

- The Sponsor delegated from CE of organisation has approved certificate request;
- The S.E.E. Key may only be stamped with the name of the organisation which employs or manages the End-entity identified in the certificate; and
- The email address in the certificate uses an Internet domain registered to the organisation.
- An individual can be issued with a S.E.E. Key only in the name by which they are usually called within the Sponsor's organisation;
- For devices, the certificate must include the name of the device administrator, the business unit, or the primary business function the device is used for;
- The S.E.E. Key may only be stamped with the name of the organisation which employs or manages the End-entity identified in the certificate; and
- The email address in the certificate uses an Internet domain registered to the organisation.
- Ensure that it has appropriately verified the identity and authorisation of the Sponsor in accordance with [Identification & Authentication \(Section 3\)](#)
- Ensure that the organisation name and email address / Internet domain details in the certificate match the Sponsor's organisation details.
- Only request BUSINESS CARD certificate with Internet domain names (e.g. in email addresses and urls) that are in the control of the organisation name requested.

85. The CA's registration process **must** be sufficiently rigorous that for **ASSOCIATE certificates**

- It has appropriately verified the identity and authorisation of the Sponsor in accordance with [Identification & Authentication \(Section 3\)](#);
- An individual can be issued with a S.E.E. Key only in the name by which they are known to the Sponsor's organisation.
- For devices, the certificate must include the name of the device administrator, the business unit, or the primary business function the device is used for;
- The organisation name details in the certificate match the Sponsor's organisation details
- The email address is reliable and approved by the individual, e.g. this should be testing by sending an email to the address, and requesting a reply confirming the validity of the application.

86. The CA's registration process **must** be sufficiently rigorous that for **ANONYMOUS certificates**

- The DN's uniqueness is assured.
- If a private key is lost together with its certificate, the details of the certificate will give no clue to what it may unlock.

87. The CA's registration process **must** be sufficiently rigorous that for **SMART-TOKEN certificates**

- The private key associated with the certificate is stored in a non-exportable form on a hardware token as per Certificate Policy.

88. The CA's registration process **must** be sufficiently rigorous that for **PROXY certificates**
- The private key is stored on a gateway server acting on behalf of the individual, e.g. email gateway signing or proxy authentication to a server.
89. The CA's registration process **must** be sufficiently rigorous that for **ACCESS certificates**
- The "non-repudiation" key usage flag should NOT be set.
90. The CA's registration process must be sufficiently rigorous that for **ID certificates**
- The "digital signature" key usage flag should be set.
91. The CA's registration process **must** be sufficiently rigorous that for **SIGN certificates**
- The "non-repudiation" key usage flag should be set.
92. The CA's registration process **must** be sufficiently rigorous that for **ENCRYPTION certificates**
- The "digital signature" key usage flag should be set.

### 4.3 Certificate Acceptance

93. The Certification Authority **must** ensure that all procedures and requirements with respect to an application for a certificate are set out in its CPS.
94. Only authorised Sponsors (i.e. such persons authorised by both the organisation and the CA) **may** make bulk applications on behalf of prospective Subscribers.
95. CAs, or RAs on their behalf, **must** ensure that each application for a certificate is accompanied by:
- Sponsor authorisation for the certificate to be issued. This will include any use of a departmental identifier in the name or alternate name fields, and authorisation for any requested certificate attributes; and
  - In the case of a PASSPORT certificate, an acknowledgement by the Subscriber of the terms and conditions governing their use of the keys and certificate.

### 4.4 Certificate Suspension & Revocation

96. The Subscriber, the Sponsor or the CA **may** initiate a Certificate revocation.
97. A certificate **should** be revoked:
- If any of the information in the certificate is no longer true; or
  - If the Subscriber is no longer associated with their Sponsor; or
  - If the private key or the media holding the private key is lost, stolen or compromised; or
  - If the Subscriber disregards any of the obligations set out in their agreement with the CA; or
  - At the request of the Sponsor;
98. The Certification Authority **must**:
- Publish the revocation in the appropriate CRL and make it available via OCSP until after the certificate's expiry date.
  - Ensure an up-to-date CRL is issued at least every eight (8) hours every day of the year (including public holidays)
  - Ensure the validity period for OCSP responses does not exceed eight (8) hours
  - Have the capability to update and issue an appropriate CRL immediately, for instance in the case of suspected compromise of a Subscriber's private key

99. The subscriber **must** notify their CA as soon as possible, if a Subscriber's private key is lost or possibly compromised.

100. The Certification Authority **must** notify the S.E.E. Steering Group immediately, if a CA certificate-signing key is compromised or possibly compromised.

101. A Relying Party **must** check all the certificates in the validation chain for authenticity and integrity (by checking the digital signature) and validity (against the CAs OCSP service or the applicable CRLs) BEFORE relying on the certificate. The digital signature of each CRL or OCSP response **must** be checked as part of this process.

102. The Certification Authority **should** ensure that all procedures and requirements with respect to the revocation of a certificate are set out in their CPS.

#### 4.5 System Security Audit Procedures

103. The Certification Authority **must** perform periodic vulnerability assessments, where their system is connected to a shared or public network, to ensure resilience to network attack.

104. The vulnerability assessment **should** take into account any alerts or irregularities in network traffic noticed in the audit logs.

105. The Certification Authority **should**:

- Record all events relating to their security in audit log files
- Ensure all logs, whether electronic or manual, contain the date and time of the event, and the identity of the entity which caused the event
- Review their audit logs at least once every working day

#### 4.6 Records Archival

106. No stipulation.

#### 4.7 Key Changeover

107. S.E.E. Key certificates **must** have an expiry date of no longer than THIRTEEN months after the issue date.

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

#### 4.8 Compromise and Disaster Recovery

109. The Certification Authority **must**

- Ensure that their CPS, and any Subscriber agreements, contain provisions outlining the means they will use to provide notice of compromise or suspected compromise
- Have business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data

110. The Certification Authority **should** have a disaster recovery plan that outlines the steps to be taken to re-establish a secure facility and CA services in the event of a natural or other type of disaster.

#### 4.9 CA Termination

111. The Certification Authority **must**

- Notify its Subscribers and the S.E.E. Steering Group immediately in the event that a CA ceases operation or changes ownership .
- Ensure arrangements are in place to ensure the CA's and Subscriber's keys are protected and available in accordance with this Policy

## 5 PHYSICAL, PROCEDURAL & PERSONNEL SECURITY

### 5.1 Physical Security Controls

112. Any site housing a CA system or administration terminal **must**

- Satisfy at least the requirements for a Grade 2 site (as per Security In Government Departments) i.e.:
  - Structural barriers are used to deter the entry of unauthorised persons outside normal working hours; and
  - An approved security guard patrols outside normal working hours in the vicinity of the site and within the perimeter security barrier are irregular intervals at least once every two hours, with random patrols inside the site at least once every four hours; or
  - An approved intruder detection system is installed and maintained by technically qualified and security cleared personnel.
- Have restricted access to the CA area. All people not on the authorised access list **must** be escorted and supervised whenever in the area; and
- Ensure all removable media and paper containing sensitive plaintext information is stored in at least Group IIIA containers (as per [Security in the Government Sector](#)).

113. Where CA, RA or Subscriber private keys are stored on a computer or removable media they **must** be protected at all times from any unauthorised access.

114. All media used for the storage of information such as keys, activation data or CA files is to be sanitised by overwriting or degaussing as described in *NZSIT207: Declassification of Storage Media*, or destroyed before it is released from a CA's control. When no longer required, paper documents containing operational information should be disposed of or destroyed in a way that makes reconstruction highly unlikely.

115. The Certification Authority **must** ensure that any facilities used for off-site backup of data or services have the same level of physical access control and monitoring as the primary CA site.

### 5.2 Procedural Security Controls

116. The Certification Authority **must** comply with *AS/NZS4444 Information Security Management* or another approved quality control standard.

### 5.3 Personnel Security Controls

117. The Certification Authority **must**

- Ensure that all CA personnel in operational roles (i.e. those with login or physical access to the CA system and/or database) have achieved an NZ Government CONFIDENTIAL, or equivalent, vetting level. This may be arranged through the S.E.E. Steering Group.
- Enforce their obligations on staff in regard to Subscriber privacy and service expectations.
- Ensure that all personnel performing CA or RA duties have received appropriate training in
  - PKI security principles and mechanisms
  - The operation of the CA and/or RA hardware and software
  - All relevant procedures and requirements in this Policy and their Certification Practice Statement

118. The Certification Authority manager **must**:

- Authorise any contractors or non-CA personnel requiring access to the CA site
- Ensure such visitors are escorted during their visit.

- Ensure such visitors are not permitted physical access to the CA workstation unless required for CA operation and only under supervision

## 6 TECHNICAL SECURITY CONTROLS

### 6.1 Key Pair Generation and Installation

119. Subscriber key pairs **must** be 1024 bit RSA. CAs' keys may be 1024-bit or 2048-bit RSA.

120. Each key pair **should** be generated using a S.E.E. Steering Group approved key generation algorithm or system. Any keys passed between the CA and the Subscriber at this time **must** be either delivered in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner.

121. Keys **may** be used for authentication, message integrity and session key establishment. Only CA signing keys must be permitted for signing certificates and CRLs.

122. The certificate `keyUsage` field **must** be used in accordance with PKIX-1 Certificate and CRL Profile.

123. The `digitalSignature` key usage value **must** be present in all certificates.

124. `keyCertSign` and `cRLSign` values **must** only be present in CA certificate-signing certificates.

### 6.2 Private Key Protection

125. Each Entity **must** physically protect their private keys from disclosure and tampering.

126. Subscriber private keys for PASSPORT and BUSINESS CARD certificates **must** be stored and processed in hardware cryptomodules (e.g. a smartcard, PC card, USB token, etc)

127. Subscriber private keys for ASSOCIATE certificates **may** be software based or stored and processed in hardware cryptomodules.

128. The cryptomodule **must** be protected from theft or misuse to a similar level to a driver's licence or credit card.

129. Private keys for server and other devices **may** be software based or stored and processed in hardware cryptomodules.

130. Subscriber's private keys may be backed up by the Subscriber, the CA, or a third party on behalf of the Sponsor on the proviso that the back-up keys are not stored on-line, never reside outside New Zealand, and are protected from physical harm and compromise. They **should** be stored in an encrypted and password protected form (using Triple DES, AES or equivalent).

131. Subscribers **must** be authenticated to their cryptographic modules before their private keys are activated (e.g. by a PIN, password or biometrics comparison).

132. Whenever private keys are inactive they **must** be available only in an encrypted form.

133. The cryptomodule and/or computer **should** also include mechanisms to prevent extraction of the private key(s) by an unauthorised user or malicious software.

134. All keys (including CA keys) **must** have validity periods of no more than FIVE years, except for 2048 bit CA keys which **may** have a validity period of up to TWENTY years.

135. The S.E.E. Steering Group reserves the right to make such changes as are required, if in their opinion, any deficiency in the security of the PKI is suspected.

### 6.3 Other Aspects of Key Pair Management

136. No stipulation.

## 6.4 Activation Data

137. Any activation data such as passwords and shared secrets (e.g. between a subscriber and their CA) **must** be unpredictable and unrelated to other user's activation data.

138. Subscribers **must** have the capability to change their passwords at any time.

139. The cryptographic token **should** include a facility to temporarily lock the token after a predetermined number of login attempts, if a reusable password scheme is used.

## 6.5 Computer Security Controls

140. The Certification Authority **must** include the following system security functionality:

- Unique identification and authentication of CA operators;
- System controlled access to the CA functions;
- Use of cryptography for session communication and database security;
- Archival of CA and Subscriber history and audit data; and
- Self-test of security related CA services and audit of security related events.

This functionality may be provided by the operating system, or through a combination of operating system, CA software, and physical safeguards.

141. The Certification Authority operating system and application software **should** be evaluated to an assurance level of at least ITSEC-E2 or Common Criteria EAL3 (refer to the AISEP area on [www.dsd.gov.au/infosec](http://www.dsd.gov.au/infosec) or [www.commoncriteria.org](http://www.commoncriteria.org)). Only the services required for the CA tasks – including CA management and protection – **should** be active on the CA server.

142. The Certification Authority system **should** include a virus detection system that is kept up to date.

## 6.6 Life Cycle Technical Controls

143. The Certification Authority **must** ensure

- That a documented configuration management procedure is used for installation and ongoing maintenance of the CA system.
- The CA personnel verify the CA software during installation, to confirm it:
  - Originated from the software developer;
  - Has not been modified prior to installation; and
  - Is the version intended for use.

144. The Certification Authority **should** ensure the integrity of the software and configuration is verified at regular intervals.

## 6.7 Network Security Controls

145. The Certification Authority server **must** be protected from attack through any open or general-purpose network it is connected to. Such protection **must** include the use of a firewall certified to EAL3 or better and configured to allow only the protocols and commands required for the operation of the CA.

146. The Certification Authority subnet **should** be protected against all AusCERT-published vulnerabilities.

147. A network intrusion detection system **should** be in place with appropriate procedures and responsibilities defined to manage any alerts appropriately.

148. The RA **must** satisfy all the physical, personnel and network security controls required for a CA site, in situations where an RA has Subscriber administration access on the CA server. Certificate-based authentication and encryption **must** be used to secure the connection.

## 6.8 Cryptographic Module Engineering Controls

149. All CA, RA and End-entity cryptographic functions **must** be performed in cryptographic modules that have been evaluated to a minimum of either FIPS140 Level 2, ITSEC level E2, or common Criteria EAL3.

150. The cryptographic application software used by RAs and End-entities **should**:

- Establish, transfer and use the public and private keys correctly and in a secure fashion;
- Be capable of performing the appropriate certificate validity and verification checking; and
- Report appropriate information and warnings to the user.

151. The Certification Authority, RA and Subscriber crypto-modules **must** support RSA 1024 and 2048 (as per PKCS#1) and SHA-1 (as per FIPS PUB 180-1 / ANSI X9.30).

## 7 CERTIFICATE & CRL PROFILES

### 7.1 Certificate Profile

#### 7.1.1 Version number(s)

152. The Certification Authority **must** ensure

- All certificates are X.509 Version 3 in accordance with the PKIX Certificate and CRL Profile.

#### 7.1.2 Certificate extensions

153. The PKI End-Entity software **must** support all the base (non-extension) X.509 fields as well as the certificate extensions identified in section 4.2.2 of the PKIX certificate profile.

#### 7.1.3 Algorithm object identifiers

154. No stipulation.

#### 7.1.4 Name forms

155. The Certification Authority **must** ensure

- Each PKI Entity (e.g. CA, RA, Subscriber or device) has a clearly distinguishable and unique Distinguished Name (DN) in the certificate `subjectName` field as defined in the IETF PKIX Certificate and CRL Profile.
- End-entity `distinguishedName`'s
  - are in the form of an X.501 or UTF-8 printableString.
  - either have an association with the authenticated name of the Subscriber or reflect the organisation or organisational unit
  - are unique for all End-Entities of the CA.

156. The Certification Authority **must not** mandatorily require any additional fields.

157. The Certification Authority and the Sponsor **may**

- Include additional fields in the DN, at their joint discretion.
- Use the `subjectAlternateName` field where an alternative type of name form is required in the certificate. This usage **must** be in accordance with PKIX Part 1.

158. The Sponsor **should** determine the structure of the `distinguishedName`.

### 7.1.5 Name constraints

159. The DN structure for a certificate **shall** be:

- C=country
- S=state
- L=location
- O=organisation
- OU=optional organisation unit
- CN=common name
- E=e-mail address

160. The Certification Authority **must** ensure

- For the `distinguishedName`
  - The Organisation (O=) field **should** reflect the proper relevant legal name of the organisation name e.g. O=Ministry of Water, not O=minwtr.govt.nz.
  - The State (S=) field **must** be set to "-", however applications should not require the presence or otherwise of the S= field in the DN.
  - The Organisational Unit (OU=) field **should** be used to provide additional information, such as liability disclaimers.
  - The Common Name (CN=) field **must** be used to differentiate certificate types, using the generic format "**CN = Commonname [SEEKEY name]**".
  - The Common Name (CN=) field **must not** be used in conflict with the labels defined in this Policy
  - The Common Name (CN=) field **should** reflect the subscriber's preferred name e.g., Les Battersby, rather than Lesley Battersby or, in the case of a server certificate, its DNS address, rather than IP address.
- For PASSPORT certificates
  - The `distinguishedName` Organisation field **may** be blank, or **may** contain the name of the CA organisation prefixed with a string such as "Identity authenticated by". An appropriate example is "Identity authenticated by ACME-CA Associates".
- For BUSINESS CARD certificates
  - The `distinguishedName` Organisation (O=) field **must** contain the Sponsor's name.
- For ASSOCIATE certificates
  - The `distinguishedName` Organisation (O=) field **must** contain the Sponsor's name prefixed with a mutually agreed string, such as "Associate registered by ". An appropriate example is "Associate of The Treasury".
  - The `distinguishedName` Organisation Unit (OU=) field **should** contain a disclaimer to differentiate it significantly from a BUSINESS-CARD style certificate.
- For ANONYMOUS certificate

- The distinguishedName Organisation (O= ) field **must** contain “-“ or the Sponsor’s name.
- The distinguishedName Common Name (CN= ) field **must** be set to “ANONYMOUS arbitraryString” , where arbitraryString is a unique value.

161. The Certification Authority **may** ensure the distinguishedName’s uniqueness by appending additional numbers or letters to the commonName.

#### 7.1.6 Certificate Policy Object Identifier (OID)

162. The [SEEKEY Certificate Table](#) lists the SEEKEY Certificate Types. Each Certificate Type has a corresponding Alphanumeric OID and Numeric OID.

163. The Certificate Type Numeric OID is specified by adding a unique numeric suffix (.1, .2, etc) to the SEEKEY Certificate Policy OID (2.16.554.101.2.1.1).

164. The Certificate Type Alphanumeric OID is a unique label, prefixed by the label “SEEKEY”, used to describe the purpose of the Certificate Type, e.g. “SEEKEY BUSINESS-CARD”

165. These OIDs are not formally registered.

166. The Certification Authority **must** ensure

- For each certificate issued under this Policy, that the Certificate Policies extension specifies the appropriate
  - Certificate Type Numeric OID (e.g. 2.16.554.101.2.1.1.6), and
  - a userNotice of the certificate type as it appears in the CN (e.g. [SEEKEY ASSOCIATE-ROLE], and
  - a cpsUri of http://see.govt.nz/pki/cp/seekey/#/ where # is the certificate type e.g. http://see.govt.nz/pki/cp/seekey/associate-role/

#### 7.1.7 Usage of Policy Constraints extension

#### 7.1.8 Policy qualifiers syntax and semantics

#### 7.1.9 Processing semantics for the critical certificate policy extension

167. The Certification Authority **must** ensure

- The CRL Distribution Point (CDP) defined in each SEEKEY certificate specifies the location of the CRL and the protocol used to address and obtain it (either HTTP or LDAP).
- The Authority Information Access extension should specify an OCSP service, and if specified, must specify HTTP or HTTPS as the protocol.

### 7.2 CRL Profile

168. The Certification Authority **must** ensure

- All CRLs are X.509 Version 2 in accordance with the PKIX Certificate and CRL Profile.

## 8 SPECIFICATION ADMINISTRATION

### 8.1 Specification Change Procedures

169. The S.E.E. Steering Group **will** notify all approved CAs in writing of any non-minor changes to this Policy.

170. The S.E.E. Steering Group **may** assign a new OID for the modified Policy, in some circumstances.

## **8.2 Publication and Notification Policy**

171. An electronic copy of this document is available via an e-mail request to [pki@security.govt.nz](mailto:pki@security.govt.nz) or from the Government Security Web site, URL [www.security.govt.nz](http://www.security.govt.nz). Any changes to the Policy will be posted to the Web site.

## **8.3 CPS Approval Procedures**

172. Refer Section 2.7 *Compliance Audit*.

## GLOSSARY

**CA (Certification Authority)** – A person that establishes practices for all authorities and users within its domain. An entity authorised to issue and manage X.509 public key certificates and CRLs.

**CN (Common Name)** – This is the X.500 commonName attribute, which contains a name of an object. If the object corresponds to a person, it is typically the person's full name.

**CP (Certificate Policy)** – a standard by which public key certificates and keys are issued and managed. The CP that a specific certificate is issued under **should** be referenced in the certificate's certificatePolicy field.

**CPS (Certification Practice Statement)** – a Certification Authority's security plan and standard operating procedures.

**CRL (Certificate Revocation List)** – an electronically signed list of certificates that **should** no longer be trusted but have not yet expired. Each CA will issue one or more CRLs. The location of the relevant CRL for a specific certificate will be defined in the certificate's CRL Distribution Point (CDP) field.

**DN (Distinguished Name)** – an ISO X.500 term defining a standard for unique identifiers for people, devices or other objects.

**EAL (Evaluation Assurance Level)** – international Common Criteria IT product security testing evaluation level. EAL1 is the lowest level of testing; EAL7 is the highest.

**End-entity** – The users of the certificates and keys, for instance, Subscribers, Webservers, S.E.E. Mail gateways, etc.

**FIPS (Federal Information Processing Standards)** – a set of IT security standards promulgated by the US National Institute of Standards and Technology.

**HTTP (Hypertext Transfer Protocol)** – the primary application-level communications protocol of the World Wide Web.

**IETF PKIX (Internet Engineering Task Force PKI X.509)** – references the Internet Working Group on PKI and their resulting standards.

**IN-CONFIDENCE** – Compromise of such information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand, or affect adversely the privacy of its citizens.

**ITSEC (IT Security Evaluation Criteria)** – UK Government IT product security testing criteria. Evaluations go from E1 (lowest assurance = EAL2) to E6 (mathematically proven = EAL7)

**LDAP (Lightweight Directory Access Protocol)** – an Internet protocol for communicating with directories.

**NZSIT (NZ Security of IT)** – a set of IT security publications promulgated by the Government Communications Security Bureau.

**OCSP (Online Certificate Status Protocol)** - An Internet protocol used by a client to obtain from a server the validity status and other information concerning a digital certificate. OCSP provides more up-to-date status than is possible with CRLs at the expense of increased network traffic, latency and dependence on the OCSP service. The location of the relevant OCSP service for a specific certificate will be defined in the certificate's Authority Information Access field.

**OID (Object Identifier)** – the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. Certificate policies and cryptographic algorithms are two such classes.

**PKCS (Public Key Cryptographic Standard)** – cryptographic guidelines promulgated by RSA Inc.

**RA (Registration Agent/Authority)** – also called a Local Registration Authority (LRA) or Organisation RA (ORA) – an entity that is responsible for the identification and authentication of Subscribers before certificate issuance, but does not actually create or issue the certificates. The RA is a delegated agent of the CA.

**Reliance** – To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective.

**Relying Party** – A recipient who acts in reliance on a certificate and digital signature.

**S.E.E. (Secure Electronic Environment)** – NZ Government initiative to provide secure interaction and collaboration between Government departments and agencies across the Internet.

**SENSITIVE** – Compromise of such information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens.

**SIGD** – Security in Government Departments manual available at <http://www.security.govt.nz/sigd/>

**Sponsor** – the department or public servant that has nominated an individual or organisation to be issued a certificate. The Sponsor is responsible for either supplying or confirming an individual's requirement for a certificate and the attribute details in the certificate. The Sponsor is also responsible for informing the CA or RA if the department's relationship with the Subscriber is terminated or changed such that the certificate **should** be revoked or updated. Some organisations may combine the Sponsor and Registration Agent roles.

**Steering Group (SG)** – the body responsible for setting, implementing and administering this Certificate Policy statement and overseeing the CA's issuing certificates under it. The S.E.E. Steering Group is the Policy Management Authority (PMA) for S.E.E. PKI.

**Subscriber** – An individual or organisation whose public key is certified in a public key certificate. In the Government context this could be a public servant, a citizen, or a Government client or supplier.

**URL (Universal Resource Locator)** – World Wide Web address of a computer or file.

## SEEKEY Certificate Table

Alphanumeric OID / numeric OID / Attributes	Description of characteristics	CN Example
SEEKEY PASSPORT 2.16.554.101.2.1.1.1  PASSPORT, SMART-TOKEN, ID, [SIGN,] [ENCRYPT]	Personal certificate. Individual is identified using Gatekeeper 100 point system and certificate is not tied to a particular organisation – The DN O field is left blank. MUST be on a hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT.	O= CN=Joe Bloggs [SEEKEY PASSPORT] E=joe.bloggs@ssc.govt.nz
SEEKEY BUSINESS-CARD 2.16.554.101.2.1.1.2  BUSINESS CARD, SMART-TOKEN, ID, [SIGN,] [ENCRYPT]	Employer issued certificate. MUST be on hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT.	O=State Services Commission CN=Joe Bloggs [SEEKEY BUSINESS-CARD] E=joe.bloggs@ssc.govt.nz
SEEKEY ASSOCIATE 2.16.554.101.2.1.1.3  ASSOCIATE, ID, [SIGN,] [ENCRYPT]	Organisation issued associate certificate. OPTIONAL hardware token. Typically ID. Optionally SIGN. Optionally ENCRYPT. SHOULD have an OU= liability statement.	O= State Services Commission OU= For internal use only. We disclaim any liability from third parties accepting this certificate for their own purposes. CN=Mary Smith [SEEKEY ASSOCIATE] E=mary.smith@someplace.co.nz
SEEKEY DEVICE 2.16.554.101.2.1.1.4  PASSPORT, ID, ENCRYPT or  BUSINESS CARD, ID, ENCRYPT or  ASSOCIATE, ID, ENCRYPT	Device certificate. OPTIONAL hardware token. Typically ID and ENCRYPT. Optionally SIGN. NB: Web server certificates cannot use the CN qualifiers as common practice is for the DNS name to match the CN	O=State Services Commission CN=webserver.ssc.govt.nz E=webmaster@ssc.govt.nz
SEEKEY BUSINESS-ROLE 2.16.554.101.2.1.1.5	Employer issued role certificate. MUST be on a hardware token. Typically ID.	O=State Services Commission CN=Helpdesk [SEEKEY BUSINESS-ROLE] E=helpdesk@ssc.govt.nz

Alphanumeric OID / numeric OID / Attributes	Description of characteristics	CN Example
BUSINESS CARD, SMART-TOKEN, ID, [SIGN,] [ENCRYPT]	<p>Optionally SIGN.</p> <p>Optionally ENCRYPT.</p> <p>MUST be issued on a limited basis, to a group of users.</p> <p>SHOULD have a unique number for each token.</p> <p>SHOULD have a register showing user / token unique number.</p> <p>TOKEN may be shared among group of users.</p>	
SEEKEY ASSOCIATE-ROLE 2.16.554.101.2.1.1.6  ASSOCIATE, SMART-TOKEN, ID, [SIGN,] [ENCRYPT]	<p>Organisation issued role certificate.</p> <p>MUST be on a hardware token.</p> <p>Typically ID.</p> <p>Optionally SIGN.</p> <p>Optionally ENCRYPT.</p> <p>MUST be issued on a limited basis, to a group of users.</p> <p>SHOULD have a unique number for each token.</p> <p>SHOULD have a register showing user / token unique number.</p> <p>SHOULD have an OU= liability statement.</p>	<p>O=State Services Commission</p> <p>OU= For internal use only. We disclaim any liability from third parties accepting this certificate for their own purposes.</p> <p>CN=Helpdesk [SEEKEY ASSOCIATE-ROLE]</p> <p>E=helpdesk@someplace.co.nz</p>
SEEKEY MEMBERSHIP 2.16.554.101.2.1.1.7  PASSPORT, ID or  BUSINESS CARD, ID or  ASSOCIATE, ID	<p>The concept of Organisation can be covered by Role e.g. a role of "Common Seal of the Company" represents an organisation. The concept of Delegation can be covered by Role. For instance, a PA has the delegated authority to act on behalf of the CEO in certain areas. The PA would have the role of "PA to the CEO". The PA may sign on behalf of the CEO – typically there are other checks and balances to manage issues such as misrepresentation.</p> <p>The concept of Membership, Registration, Certification or similar capability can be covered by Membership. Typically several people will have the same Membership certificate.</p> <p>Membership certificate.</p> <p>Organisational name must match authority that approves membership.</p> <p>OPTIONAL hardware token.</p> <p>ID only.</p> <p>NO SIGN or ENCRYPT.</p> <p>MAY have duplicates.</p> <p>MUST be issued on a limited basis, to a group of users.</p>	<p>O= GOVIS</p> <p>OU= GOVIS warrants this certificate for the purposes of membership only</p> <p>CN=Joe Bloggs [SEEKEY MEMBERSHIP-GOVIS-ASSOCIATE]</p> <p>O= GOVIS</p> <p>OU= GOVIS warrants this certificate for the purposes of membership only</p> <p>CN=Joe Bloggs [SEEKEY MEMBERSHIP-GOVIS-FELLOW]</p>

Alphanumeric OID / numeric OID / Attributes	Description of characteristics	CN Example
	<p>MUST have a unique number for each token.</p> <p>MUST have a register showing user / token unique number.</p> <p>SHOULD have an OU= liability statement.</p> <p>Different types of membership can be achieved by adding a 3rd part to the name.</p>	
<p>SEEKEY PROXY 2.16.554.101.2.1.1.8</p> <p>PASSPORT, PROXY, SIGN, ENCRYPT or BUSINESS CARD, PROXY, SIGN, ENCRYPT</p>	<p>Organisation signing on behalf of an individual.</p> <p>OPTIONAL hardware token.</p> <p>Typically ID, SIGN, ENCRYPT.</p> <p>Typically used by mail gateways, to generate a certificate on the fly, for an individual, to sign an outgoing e-mail. This allows s/mime to individual e-mail clients to work without generating an error message.</p> <p>SHOULD have an OU= liability statement.</p>	<p>O= State Services Commission OU= Proxy certificate used by mail server CN=Joe Bloggs [SEEKEY PROXY] E=joe.bloggs@ssc.govt.nz</p>
<p>SEEKEY PROXY-ACCESS 2.16.554.101.2.1.1.9</p> <p>BUSINESS CARD, PROXY, ACCESS</p>	<p>Organisation access to a protected resource e.g. part of web server, through a proxy mechanism.</p> <p>Organisation confirms user identity through minimum of username/password.</p> <p>Organisation assigns unique username/password to each individual.</p> <p>NO ID, SIGN or ENCRYPT.</p> <p>SHOULD have an OU= liability statement.</p>	<p>O= State Services Commission OU= Proxy certificate used by web server CN=Joe Bloggs [SEEKEY PROXY-ACCESS] E=joe.bloggs@ssc.govt.nz</p>
<p>SEEKEY ACCESS-CARD 2.16.554.101.2.1.1.10</p> <p>BUSINESS CARD, SMART-TOKEN, ACCESS or</p> <p>ASSOCIATE, SMART-TOKEN, ACCESS</p>	<p>General purpose certificate.</p> <p>MUST be on a hardware token.</p> <p>NO ID, SIGN or ENCRYPT.</p> <p>MAY have duplicates.</p> <p>SHOULD have an OU= liability statement.</p>	<p>O= State Services Commission OU= No validity for signing CN=Laptop [SEEKEY ACCESS-CARD]</p>
<p>SEEKEY ANON-ACCESS-CARD 2.16.554.101.2.1.1.11</p> <p>ANONYMOUS, SMART-TOKEN, ACCESS</p>	<p>General purpose certificate.</p> <p>MUST be on a hardware token.</p> <p>NO ID, SIGN or ENCRYPT.</p> <p>MAY have duplicates.</p> <p>SHOULD have an OU= liability statement.</p>	<p>O= - OU=No validity for signing CN=12345678 [SEEKEY ANON-ACCESS-CARD]</p>